ETSI GS NGP 005 V1.1.1 (2017-04)

Next Generation Protocols (NGP);
Next Generation Protocol Requirements

Disclaimer

The present document has been produced and approved by the Next Generation Protocols (NGP) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGS/NGP-005

Keywords

core network, cyber security, IoT, mobility, network, QoE, reliability, security, service, use case

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Next Generation Protocols (NGP).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The scope of the present document is to specify the minimum set of key requirements for the Next Generation Protocols (NGP), Industry Specific Group (ISG).

The present document addresses requirements in the following areas:

- Business Case and Techno-Economics
- Migration
- General Technical Requirements
- Addressing
- Security
- Mobility
- Multi-Access Support (including FMC)
- Context Awareness
- Performance (including Content Enablement)
- Network Virtualisation
- IoT Support
- Energy Efficiency
- e-Commerce
- MEC
- Mission Critical Services
- Drones and Autonomous Vehicles and Connected Vehicles
- Ultra Reliable Low Latency Communications

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS NGP 001: "Next Generation Protocol (NGP); Scenario Definitions".

NOTE: ETSI NGP references are available at http://www.etsi.org/deliver/etsi_gs/NGP/.

[2] ETSI TS 122 280: "Technical Specification Group Services and System Aspects; Mission Critical Services Common Requirements (MCCoRe); Stage 1".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] 3GPP TR 23.799: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Architecture for Next Generation System".

[i.2] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.3] 3GPP TR 22.862: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers for Critical Communications; Stage 1".

NOTE: ETSI standards are available at http://www.etsi.org/standards.

[i.4] Recommendation ITU-R M.2083-0: "Framework and overall objectives of the future development of IMT for 2020 and beyond".

[i.5] ETSI GS NFV 001: "Network Functions Virtualisation (NFV); Use Cases".

[i.6] 3GPP TR 37.868: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on RAN Improvements for Machine-type Communications".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions applying to scenarios that include mobile network architectures given in ETSI GS NGP 001 [1], ETSI TR 121 905 [i.2] and 3GPP TR 23.799 [i.1] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NGP 001 [1], ETSI TR 121 905 [i.2] and the following apply.

AN	Access Network
FPGA	Field Programmable Gate Array
GGC	General Group Communications
IC	Integrated Circuit
IOC	Information Object Class
LTE	Long Term Evolution

NOTE: Cellular standard.

MCS	Mission Critical Services

MEC	Mobile Edge Computing

NOTE: ETSI, ISG specified.

MPS	Multimedia Priority Service
NFV	Network Function Virtualisation
NGP	Next Generation Protocol
NG-UE	Next Generation User Equipment

NOTE: Beyond LTE.

NIC	Network Interface Card
PGW	PDN Gateway

NOTE: In LTE system.

SDN	Software Defined Networking
SGSDS	Smart Grid System with Distributed Sensors
SGW	Serving Gateway

NOTE: In LTE system.

SPC	Substation Protection and Control
TFT	Traffic Flow Template

NOTE: E.g. as defined for 3GPP LTE.

UE	User Equipment for LTE
URLLC	Ultra Reliable Low Latency Communications
VM	Virtual Machine

4 Overview

The Next Generation Protocols (NGP), ISG aims to review the future landscape of Internet Protocols, identify and document future requirements and trigger follow up activities to drive a vision of a considerably more efficient Internet that is far more attentive to user demand and more responsive whether towards humans, machines or things.

ETSI GS NGP 001 [1], Scenarios Descriptions specification, lists the key agreed networking and internetworking issues for multi-access communications at present and provides examples of current scenarios where these issues are exemplified. ETSI GS NGP 001 [1] further provides recommendations, on a per issue basis, targeted at applicable next generation SDOs: ITU-T, IEEE, IETF and 3GPP in their consideration of future networking and internetworking protocol architecture definitions.

The present document progresses the requirements decomposition process one further stage to define key requirements for NGP.

The present document provides key general NGP requirements, in clause 5 and NGP issue specific requirements, in clause 6.

5 General Requirements

5.1 Business Case

[**Gen-BC-01**] The NGP architecture shall be 25 % more energy efficient across end-user devices, servers, fixed transmission and access technologies and wireless and/or cellular access technologies as compared to existing IPv4/v6 protocol based architectures.

NOTE 1: This performance measure should be based on network wide measurements and devices connecting with reference access technologies current at the time of specification as follows: LTE-A, Rel-12, Wi-Fi™ 802.11ac and Ethernet 100 Mbit/s FE.

[**Gen-BC-02**] The NGP architecture shall be 30 % more spectrally efficient when transporting NGP across the access technology as compared to transporting existing IPv4/v6 protocol based architectures and considering all over-air impacting facets.

[**Gen-BC-03**] The NGP architecture shall be at least 25 % more header efficient than existing IPv4/v6 protocol based architectures.

[**Gen-BC-04**] The NGP architecture shall be at least 10 % more bitwise efficient per packet than existing IPv4/v6 protocol based architectures for the same application transport.

NOTE 2: The scope of Gen-BC-02x requirements is from the UE or NG-UE to the edge of Operator Domain connecting to the Internet or other external PDN.

NOTE 3: Gen-BC-02(x) performance measures should be based on reference radio-based access technologies current at the time of specification as follows: LTE-A, Rel-12, Wi-Fi™ 802.11ac.

[**Gen-BC-05**] The NGP architecture shall be able to be cost effectively implemented into existing user device operating systems with no additional processor or memory requirements, as compared to IPv4/6 implementations.

NOTE 4: Current key user device, operating systems should include Android™, iOS® and Windows®.

[**Gen-BC-06**] The NGP architecture shall be able to be cost effectively implemented into existing user server operating systems with no additional processor or memory requirements, as compared to IPv4/6 implementations.

NOTE 5: Current key server operating systems should include Linux® variants and Windows®.

[**Gen-BC-07**] The NGP architecture shall be able to be cost effectively implemented into network interface software and hardware, with no additional processor or memory requirements. as compared to IPV4/6 implementations.

NOTE 6: Current implementations should include: Custom Integrated Circuits (IC), Field Programmable Gate Array (FPGA) technology solutions and software defined, Network Interface Cards (NIC).

5.2 Migration

[**Gen-Mig-01**] The NGP architecture shall be able to provide peer to peer communications between a next generation access communications device and the edge of that access network or networks with no increase in setup delay as compared to existing IPv4/v6 protocol based architectures, for the issues described in ETSI ETSI ETSI GS NFV 001 [i.5] and when operating over LTE-A, Rel-12 access technology.

NOTE 1: An access communications device may include an evolved 3GPP UE, server or IoT device and the access network may include millimetric radio, cellular, wireless and/or fixed connectivity.

NOTE 2: Access efficiency in this context may be: spectrum efficiency, bitwise efficiency, or byte efficiency of the protocol.

[**Gen-Mig-02**] The NGP architecture shall be able to interwork to the existing IPv4 and IPv6 protocol.

[**Gen-Mig-03**] The NGP architecture shall be able to support transmission of the 3GPP TR 23.799 [i.1] defined interfaces: NG1, NG2, NG3 NG4 and NG6, interfaces at layer 3.

5.3 Technical

[**Gen-Tech-01**] NGP shall support multi-level mutual authentication between peers.

NOTE 1: Authentication is operated between peer entities.

NOTE 2. Authentication among applications only involves the applications, not NGP.

NOTE 3: Authentication within NGP is among the entities supporting NGP itself.

NOTE 4: NGP should require the authentication of all members of a given layer.

[**Gen-Tech-02**] NGP shall not allow third parties (other than those authorized by law, such as national security agencies) to discover the identity of entities that are communicating with each other.

[**Gen-Tech-03**] NGP shall provide stakeholder based confidentiality for user data.

[**Gen-Tech-04**] NGP shall provide stakeholder based confidentiality for protocol control.

NOTE 5: For Gen-Tech-03x: A stakeholder would typically include N x communicating peers.

NOTE 6: For Gen-Tech-03x: A stakeholder agreement could optionally include an N+1 party as well as the peers (e.g. Operator and/or Lawful Intercept party.

6 Issue Specific Requirements

6.1 Addressing

[**Iss-Addr-01**] In a multi-access and multi-layer, context aware NGP environment future protocols should address ID and Addressing aspects separately.

NOTE 1: For example Network Communications Protocol Address, Usage IDs, Session/Service-IDs and Application Naming are distinctly operated.

[**Iss-Addr-02**] Application-ID shall not change during mobility and multi-homing link state changes.

NOTE 2: This requirement is essential in order to maintain application instances during mobility.

NOTE 3: See NGP definition of 'Application Process' and 'Identity' in ETSI GS NGP 001[1].

[**Iss-Addr-03**] NGP should minimize addressing updates in future protocols for mobility and multi-homing. During mobility events, addressing may change but should be minimized.

[**Iss-Addr-04**] NGP addressing should support at least the following communication models: client-client, client-server (push and/or pull) and server-server models and multi-protocol versions thereof.

[**Iss-Addr-05**] NGP should be designed to minimize multi-address mappings.

NOTE 4: For example the inefficiencies associated with extensive use of NAT today including: NFV implementations, Device-to-Device capabilities (D2D), etc.

[**Iss-Addr-06**] NGP shall minimize the use of "well-known" ports.

[**Iss-Addr-07**] NGP shall include an addressing strategy that scales.

NOTE 5: This means that an addressing scheme that includes every entity on the planet does not need to include the full address length in the packet header all of the time for local communication, but has to accommodate the case for an entity to address another entity on the other side of the world when required.

Table 1 captures a set of KPIs that can be used to compare the merits of different addressing schemes.

Table 1: KPIs for Assessment of Addressing Requirements

KPI Name	Description	Related to requirements	Measured feature	Units	Example Values for IPv4 (CIDR)
Scalability of address space	Measures how many different entities can be uniquely addressed	[**Iss-Addr-07**]	Address space size	Integer value	2^32
Address encoding efficiency	Measures how many bits on the wire are required to encode the address information	[**Iss-Addr-07**]	Header overhead due to addressing	Integer value	Always 32
Aggregation capabilities	Measures how well address assignment follows the underlying "network topology" in order to facilitate aggregation	[**Iss-Addr-07**]	Size of forwarding tables in routers as a function of addressed entities in the network	Order of magnitude O(f(x)), where x is # of addressed entities	Up to 32 levels of addressing hierarchy. Forwarding efficiency depends on allocation policy
Identity decoupled from addressing	Checks if applications can be assigned independent identifiers which are loosely coupled to network addresses (via directories/mapping systems).	[**Iss-Addr-01**] [**Iss-Addr-02**]	Application identity separated from network addressing	Binary value	False
Cost of mobility	Measures the overhead of supporting mobility as the extra state required in the network due to mobility events	[**Iss-Addr-03**]	Extra entries in forwarding tables per mobility event	Order of magnitude O(f(x)), where x is # of mobility events	Depends on mobility management protocol in use, usually requires setup of tunnels per mobility event

6.2 Security

[**Iss-Sec-01**] NGP should decouple data transfer and layer management (also known as control plane) protocols from security functions (authentication, key agreement, access control, integrity verification, encryption) except where this would defeat other NGP security requirements. NGP should provide clear integration points for each type of security function.

NOTE 1: It is anticipated that the decoupling described in Iss-Sec-01 will facilitate rather than defeat most other security requirements.

[**Iss-Sec-02**] NGP shall adopt data transfer protocols that decouple port-id from connection-endpoint-id.

[**Iss-Sec-03**] NGP shall not use well-known ports.

[**Iss-Sec-04**] Applications should protect the confidentiality and integrity of their communication.

NOTE 2: Most security experts agree that the best encryption architecture should operate between peer applications.

NOTE 3: Operating peer application encryption greatly reduces the security problem for the network to primarily authenticating members of some layers, and protecting against traffic analysis at higher communication layers.

[**Iss-Sec-05**] Each protocol layer should offer an API that allows the layer above to request the properties of the network service it wants (bound on packet loss and delay, in-order delivery of data, etc.).

NOTE 4: NGP assumes that each layer and/ or the protocols in each layer should take the necessary security measures to protect their data without relying on the lower layer.

NOTE 5: This is to avoid making network service requirements implicit (as today) and having the network layers have to do DPI or similar to infer application requirements (which becomes very hard or infeasible if the application uses end-to-end encryption).

[**Iss-Sec-06**] Protocol layers should have good layer management and administration that provides the statistics needed for security.

NOTE 6: It is important to use different Information Object Classes (IOC) for different protocols.

NOTE 7: NGP needs a control structure that enables a layer to select different IoCs to be presented per layer.

[**Iss-Sec-07**] NGP should provide Optimization meta-data that enables both of the following options for delivery outside of the secure user data transport part of each packet:

a) Can be based on a 'pull' meta-data system.

b) Can be provided as a separate Meta-Data mechanism for which entities can offer information to, 'push' meta-data.

NOTE 8: The Optimisation Meta-Data capability is a mechanism required for NGP that is specifically designed for shipping context information around for an operator or user to optimize their user QoE or Network performance outside of user data security mechanisms.

NOTE 9: It is acknowledged that 'pull' mechanisms are simple to realise but may be slow to respond, which is why a 'push' mechanism is included as well.

NOTE 10: Despite the Optimization Meta-Data scheme being outside the User Data Payload security mechanisms, it may optionally have its own dedicated security mechanism.

[**Iss-Sec-08**] Coordination of meta-data across virtualised components in "network slices" should be supported by NGP to meet the goal of information being available where needed and only where needed.

NOTE 11: Next Generation solutions will be operating over heterogeneous networks and with varying network requirements. This creates a drive towards building network functions as slices, created out of a number of sub-components or sub-functions.

[**Iss-Sec-09**] Security monitoring should be a built-in part of NGP.

NOTE 12: Security assessments and standards often include references to security monitoring (frequent checking on security-related/impacting functions).

[**Iss-Sec-10**] NGPs shall support situations where location meta-data is a part of network audit or where it is required to be delivered for business purposes.

NOTE 13: To operate these audit cases, NGP functional implementations should be able to make a clear assessment of the situations where location meta-data needs to be propagated and where it should remain private or be obscured.

NOTE 14: Location based data can contain considerable personal or sensitive information. Location based information should not be transferred or made available without a proper assessment of the privacy implications.

[**Iss-Sec-11**] NGP should support an Identity Service mechanism.

NOTE 15: Currently there are identity security vulnerabilities in IPv4/6.

NOTE 16: An NGP Identity Service should include identity logging/checking/validation and ongoing management.

NOTE 17: Consideration is needed for NGP in the setup of ID servers for Users operating NGP and/or Resource Registration (RR) for logical entities operating NGP.

NOTE 18: Examples of ID based entities include ID servers for entities such as VNFs from the NFV space, or a register of Certified IoT devices or IoT Gateways.

[**Iss-Sec-12**] IoT Gateways shall be investigated as part of the secure Identity services provided in NGP.

NOTE 19: As latency requirements get tighter, the pressure for edge-based decision-making will increase.

NOTE 20: Gateways can have an important role in facilitating secure edge-based computing, potentially enabling better security and/or more effective use of meta-data.

[**Iss-Sec-13**] The NGP ID Service mechanism(s), should add Identity security but not be prohibitively expensive, be scalable and provide failsafe mechanisms according to potential threat level and scope.

NOTE 21: NGP needs to address a range of scalable ID capabilities and recommend according failsafe mechanisms per threat level.

NOTE 22: There is a balance of security versus cost and complexity to be considered in satisfying this recommendation, so it is recommended that the NGP evolves to scalable security and ID system where cheap and large scale edge devices have some level of ID check.

[**Iss-Sec-14**] Efficient extensions for MANO and SDN controller protocols should be provided to administer them across Tenant and Multi-Tenant environments in a secure manner including the following security mechanisms:

a) mandatory two-way authentication by traceable ID;

b) SW event logging;

c) Resource management monitoring at the memory, processing, VM, Flow and VNF levels.

It is critical that these are built-in controls that are mandatory rather than optional bolt-on controls.

[**Iss-Sec-15**] Confidence in components should be tied to the use of hardware root-of-trust attestation.

[**Iss-Sec-16**] Separation of sensitive components: an architecture with separate trust domains for key sensitive functions should be incorporated.

NOTE 23: This requirement ensures that, for example, fraud management, authentication/crypto credentials, cyber defence, lawful enforcement functions (Lawful Intercept) are all managed independently and that access to one does not grant access to all information.

[**Iss-Sec-17**] When NFV incorporates open source software; there should be procedures in place to ensure that basic security practices keep pace and are reflected in open source software.

[**Iss-Sec-18**] It is important that MEC meta-data should be handled securely with access when required and only when required.

6.3 Mobility

[**Iss-Mob-01**] The users identity shall be preserved during mobility operations.

NOTE 1: It is assumed that mobility operations include: cell selection/reselection, access point selection, connection of a device to a physical connector, handover between cells or access points, soft-handover or relocation.

[**Iss-Mob-02**] The communications device identity presented to an N-Concurrent Access communications network shall be preserved during mobility operations.

[**Iss-Mob-03**] Each access point shall be able to be identified by its address, location and name.

[**Iss-Mob-04**] Location for NGP access points should be accurate to ±1 m per update.

NOTE 2: It is assumed that access points include at least: cellular base station, wireless access point and physical connection.

[**Iss-Mob-05**] All handover control mechanisms shall be able to identify the available access technologies type in use from the list:

i) Cellular-RF;

ii) Cellular-mm-Wave;

iii) Wi-Fi™;

iv) Fixed access points providing access to each technology.

[**Iss-Mob-06**] There shall be a logical naming structure of access points in Next Generation Networks, that enables NGPs, to address:

i) a single access point;

ii) a grouping of Access-Points as a logical 'Cluster' of Access-Points and other Network_Entity_Aggregation groupings, such as an Operator grouping.

NOTE 3: Today a common Cellular Network Entity Aggregation example would be an LTE, SGW or an LTE PGW.

[**Iss-Mob-07**] Multiple access bearers shall be able to be supported at the same time over the same compound access connection whilst addressing different external PDNs during a handover.

NOTE 4: This is potentially a completion of the extensions defined for 3GPP LWA/eLWA for RF Cellular and Wi-Fi™ aggregation in both directions, but to include all of the envisaged access technologies for next generation systems:

i) Cellular-RF;

ii) Cellular-mm-Wave;

iii) Wi-Fi™;

iv) Fixed access.

[**Iss-Mob-08**] Bearer QoS and TFTs shall be exposed at the user equipment to support user mobility decision options.

NOTE 5: It is assumed that exposure of QoS/ TFT parameters may be to the user and/ or the operating system and/or the application and may be negotiated by one of these entities at the user device dynamically or according to subscribed or user defined profile according to the mobility procedure.

[**Iss-Mob-09**] NGP mobility shall be scalable, so as to support devices that are static as well as devices that operate at speeds increasing through walking speed, car speed to High Speed Trains (HST) over the same N-concurrent access network eco-system.

[**Iss-Mob-10**] NGP mobility shall be context aware so that mobility mechanisms can respond to the current and evolving mobility context of the user device in terms of: user entropy, location, speed and heading for all single or compound connections towards the N-concurrent access network eco-system.

[**Iss-Mob-11**] NGP mobility support shall retain the ability of a user device to provide radio measurement report summaries as context information to the network that reflect basic wireless and/or cellular mobility information including signal strength, signal quality and hierarchical level for the top N access points and/or cells within range.

NOTE 6: Used for mobility optimization when GPS or similar N x metre location references are unavailable, such as proximity to cell centre and quadrant or sub-quadrant of the coverage area.

[**Iss-Mob-12**] NGP mobility mechanisms shall be able to support user devices able to report a 2D location reference estimate within a cell or access point coverage scope, when more accurate location references are unavailable at the user device.

NOTE 7: Used for mobility optimization when GPS or similar N x metre location references are unavailable, such as proximity to cell centre and quadrant or sub-quadrant of the coverage area.

[**Iss-Mob-13**] NGP shall support a mobility data model that is common across multiple access technologies.

6.4 Multi-Access Support, (including FMC)

[**Iss-MA-01**] NGP should be able to deliver the aggregate throughput and speed of the FTTx/xDSL and multiple radio access technologies in both UL and DL directions to all traffic types and 3rd party applications.

[**Iss-MA-02**] The NGP should support mechanisms to ensure that combined traffic flows are delivered in sequence (to the end application) despite use of multiple radio access technologies and fixed broadband access being operated in combination.

[**Iss-MA-03**] The NGP should support a suitable addressing scheme to enable the combined use of multiple radio access technologies and fixed broadband, potentially provided access across different networks.

[**Iss-MA-04**] The NGP should support the use of common user equipment (e.g. router hub at customer premises) that support multiple radio access technologies and fixed broadband Access.

[**Iss-MA-05**] The NGP shall support dynamic and static address allocation to the common user equipment over multiple radio access technologies and fixed broadband access.

[**Iss-MA-06**] The NGP should support all traffic types over the combined use of multiple radio access technologies and fixed broadband access.

[**Iss-MA-07**] The NGP should support multi-access deployment scenarios with data rates of 10's of Gbps.

[**Iss-MA-08**] The NGP should support multi-access deployment scenarios with ultra-low latency to enable real-time applications.

[**Iss-MA-09**] The NGP should support the option for Operators to provide the same level of security over the FTTx/xDSL link as is provided over the multiple radio access technology links.

[**Iss-MA-10**] For customer premises multi-access support, the NGP should provide a generic protocol between the multi-access aggregation point in the customer premises (e.g. router hub) and the aggregation point in the multi-access converged core that has a minimum overhead that can handle per packet or per flow scenarios.

[**Iss-MA-11**] The NGP should support a flexible (programmable) geographical distribution of the functional elements in the converged multi-access core and the operator services platforms, allowing for the FMC/Multi-access scenarios described in ETSI GS NGP 001 [1] to be supported on any geographical deployment.

[**Iss-MA-12**] NGP shall be able to allocate an NGP address per user, per access technology.

[**Iss-MA-13**] NGP shall be able to allocate an NGP address that accesses multiple technologies.

[**Iss-MA-14**] NGP shall be able to support at least the following concurrent access technologies for next generation systems:

i) Cellular-RF;

ii) Cellular-mm-Wave;

iii) Wi-Fi™;

iv) Fixed access.

6.5 Context Awareness

[**Iss-CA-01**] The NGP architecture shall include protocol support for the explicit transfer of a standard extensible data structure of meta-data Information Object Classes (IoC) that can be readily interpreted by devices and functional network entities specifically for the purposes of optimizing and organizing the network and optimizing user QoE.

NOTE 1: Examples of Context IoCs to be included are as follows: Access_Context(Access Type=x), Mobility_Context, Device_Capabilities, Environment_Context, Social_Context, etc.

[**Iss-CA-02**] The NGP architecture shall include support for context information exchange.

[**Iss-CA-03**] The meta-data protocol support for the NGP architecture shall include a simple fixed information element IoC, TV coded data structure per release version and a defined dynamic extension TLV coding per release version.

NOTE 2: It is assumed that release updates are anticipated as to be made on a similar cycle to the Cellular generations of 5-10 years and would be approved by whichever SDO authors a future NGP standard. This is in-line with Cellular protocols as a need to minimize overair IE content efficiency through the adoption of TV coding for common fields.

NOTE 3: NGP would expect that each data class included in a context aware field is efficiently coded.

[**Iss-CA-04**] The meta-data protocol support for the NGP architecture shall include support for extensibility enabling the addition within release of proprietary IoC IEs and/or IEs proposed for next release consideration indicated as a contiguous group by a TLV field.

[**Iss-CA-05**] The meta-data protocol support for the NGP architecture shall include the ability to evolve with each new version according to common IoC usage such that as the usage of common IoCs grows proposed new TLV coded fields may be migrated into TV format depend.

NOTE 4: It is expected that over time previously common TV coded IEs should be able to be downgraded per version back to TLV coding as usage declines.

NOTE 5: It is expected that protocol revision version for context IoCs are updated in accordance with changing usage trends, typically every few years as is similar for current UE OS upgrades.

[**Iss-CA-06**]: The following typical set of pre-defined and common conditional contextual meta-data IoCs shall be included in the next generation meta-data protocol for the NGP architecture, supporting efficient and timely meta-data/ context information transport:

User Originated

What: Equipment Capabilities, Access Capabilities, Content history
Where: Address[Locale, Current Location(Cell/AP/Connection point, Latitude/Longitude, TAC)], Entropy history, Mobility history, Speed, Heading
When: Current Access opportunities, Recent Access performance assessments per access type
Why: Recent Access Failures
Who: Name of Equipment, Name of User Communication, Transaction History, Type of User

Network Originated

What: Network Function Type
Where: Address[Locale, Current Location(Cell, Latitude/Longitude, TAC)]
When: Current Performance, load statistics, Collective Access Network performance/History per type of user
Current Alarms
Why: Recent Access Failures/History per type of user
Who: Name of Function

[**Iss-CA-07**] Meta-data protocol support, for the NGP architecture shall include a method for a consumer to discover a meta-data supplier, setup a stakeholder relationship with them and be able to agree which IoCs they are going to provide on an ongoing or periodically.

[**Iss-CA-08**] Meta-data protocol support, for the NGP architecture shall include procedures between network entities generating, consuming and trading meta-data for mutual authentication of involved parties in the establishment of each stakeholder relationship.

[**Iss-CA-09**] Meta-data protocol support, for the NGP architecture shall include procedure(s) between network entities involved in a stakeholder relationship that allow scalable secure meta-data information exchange, including multiple selectable levels of data security.

6.6 Performance (including Content Enablement)

[**Iss-Perf-01**] For all situations that require feedback mechanisms, NGP should adopt protocols that explicitly bound Maximum Packet Lifetime, the time to wait before Ack, and the time to exhaust retries in all protocols with feedback.

[**Iss-Perf-02**] Improved forms of congestion, latency and PER feedback within known bounds that limit the variance of response time, time to notify and variance in time to notify, should be considered for NGP.

[**Iss-Perf-03**] Explicit Congestion Notification (ECN) should be used for congestion notification with each layer that does congestion management.

NOTE 1: It is likely that any layer that relays will require congestion management over the scope of the relay.

[**Iss-Perf-04**] NGP protocols should consider transmission protocols that can be configured dynamically for a variety of access technologies according to policy.

[**Iss-Perf-05**] Congestion management should occur in the same layer where QoS is enforced for that layer so that congestion management policy and QoS policy can be coordinated.

[**Iss-Perf-06**] For retrieval of static or pre-recorded content, NGP should introduce smart content handling mechanisms to reduce transmission latency through localization.

NOTE 2: This requirement applies only to static content (e.g. not 2 or more party conversations)
(Caching of content at the edge should surely be useful whatever layer 4 protocol is used.)

NOTE 3: For example, the access network edge may pre-fetch and/or cache content beforehand. Such features may be realized through a dedicated network function/entity at the network edge, which further enables the option of embedding context-aware intelligence at the access network.

[**Iss-Perf-07**] NGP should introduce new policy based networking protocols, that are able to apply flexible congestion handling techniques according to specific contexts, such as congestion avoidance or congestion control.

NOTE 4: Such new protocols operating policy based networking may be deployed as a network function at the access network edge.

[**Iss-Perf-08**] While providing E2E encrypted user traffic, key transmission control fields should be exposed to optimization algorithms along the E2E path.

[**Iss-Perf-09**] A trusted authenticating network function should be operated at the access network edge to facilitate compliance with Iss-Perf-10 by securely managing the E2E encrypted communication.

[**Iss-Perf-10**] NGP should enable the access network operator to be able to embed intelligence to enable smart content management.

[**Iss-Perf-11**] If TCP is operated in Next Generation networks, then network transmission latency should be reduced to mitigate the performance impact caused by slow-start.

NOTE 5: For example, the access network edge may prefetch and/or cache content before access transmission in the DL direction.

[**Iss-Perf-12**] NGP should introduce a new transmission protocol that can support multiple different policies that enables selective inclusion of transmission control mechanisms according to the underlying layers employed and the types of services to be supported.

[**Iss-Perf-13**] NGP shall support bounded latency for real-time streams.

6.7 Network Virtualisation

[**Iss-NV-01**] Virtualisation: (Multi-Tenancy in Mobile Networks) will drive new service models by sharing physical infrastructure to support the efficient use of resources to realise new dynamic and virtualised network architectures. NGP shall support management and operation of such dynamic and virtualised architectures and provide elastic and dynamic resource assignment as well as ETE network isolation of a particular slice of the network infrastructure.

NOTE 1: As mobile networks become service and context aware, end-to-end network isolation will need to be supported. Tunnel IDs themselves are not sufficient to support this operation as additional information may be required to exchange service specifications.

[**Iss-NV-02**] Network Slicing: Next Generation Protocol operation over virtualised infrastructure shall support generalized mechanisms to support both multi-tenant and service specific slicing, including the following capabilities:

a) Slicing with end to end predetermined coordinated QoS per network segment (including access, transport and core parts).

b) A flexible network abstraction model of a slice shall be provided so that a top level logical virtualised network infrastructure can be realised within which several other services can be organized/offered.

c) NGP virtualisation shall provide support of isolated orchestration on a per instance basis as defined in the ETSI NFV/SDN/MANO ISGs.

[**Iss-NV-03**] Scale: NGP based virtualisation shall provide simple routing schemes to support dynamic discovery, distribution and simplified management scheme without requiring large address mappings in the routing systems.

NOTE 2: As the mobile network infrastructure becomes virtualised, the scale of VNFs and mobile subscribers/mobile devices will increase significantly over time with their own address, isolation and reachability requirements.

[**Iss-NV-04**] Security: In virtualised networks, as the same network infrastructure is shared across multiple instances of different groups of 'network services', NGP shall ensure that each virtualised network service remains unaware of each other's presence by operating the following functionality:

a) The trusted domain concept shall be adopted and provide encryption and authentication capabilities that are enhanced as compared to 3GPP LTE Rel-12.

b) There shall be strict pre-deployment verification checks and certificate checks before a network function is added into service chain.

[**Iss-NV-05**] Management and Orchestration: NGP based virtualisation shall minimise MANO complexity through a balance between centralized and autonomic control for better resource coordination across different network segments to reduce dependency on application logic.

NOTE 3: MANO has evolved into a complex centralized multi-layer service architecture. While this is necessary, the method of allocating and managing resources within the service architecture is operator driven (manual), complex and centralized. The right balance between Autonomic and Centralized controls is essential for Next Generation Networks.

[**Iss-NV-06**] Programmability efficiency for NFV/SDN: NGP southbound control information protocols for NFV/SDN operation shall be efficient and provide reliable transmission in order to achieve the benefits of network abstraction through SDN/NFV.

NOTE 4: Often, such control protocol messaging does not require high throughput or congestion control (CC) mechanisms so protocol design for simplicity, efficiency and robustness is required in this instance.

[**Iss-NV-07**] NAT processing load and delay: NGP protocols shall avoid NAT operation throughout in favour of a more efficient solution which is simpler, agile and has scalable addressing and reachability.

NOTE 5: There is a notable reliance on the use of NAT in early implementations of virtualisation since NAT helps reuse IP addresses space between Virtualised infrastructure endpoints and real-world IP endpoints. Also NAT, in this instance provides an extra layer of security, and hides the internal network topology of the virtualised network from the real world. However, NAT has several drawbacks and limitations in respect of latency and processing load.

NOTE 6: Net Neutrality Legislation and Network slice adoption: NGP should be aware of Net Neutrality and Network slicing implications. However, neutrality is not an issue that NGP needs to resolve.

6.8 IoT Support

[**Iss-IoT-01**] NGP shall support multiple priority levels, with higher-priority users being able to be allocated, in emergency situations, resources that have been allocated to lower-priority users.

[**Iss-IoT-02**] NGP shall support different levels of security, selectable per device and/or per service.

NOTE 1: Lower levels will be appropriate for simple devices where adequate security can be assured by other aspects of the system design. Higher levels can be implemented by more complex devices.

[**Iss-IoT-03**] NGP addressing shall be able to support connection of at least 130 000 directly connected devices per access network type, per access point.

NOTE 2: Direct connection means in this context, without IoT relay via a gateway or adaptor.

NOTE 3: The number of IoT end-user devices connected per single cell access point is estimated in 3GPP TR 37.868 [i.6], "Study on RAN Improvements for Machine-Type Communications", Release 11.

NOTE 4: The demographics to cell size model is derived from a typical city e.g. 2011 Government Census Data, http://data.london.gov.uk/census/data/.

NOTE 5: The NGP addressing model would need to accommodate and map to the 3GPP 5G Cellular Addressing limit which is currently 64 000 for LTE and likely to increase an estimated x2 for 5G.

[**Iss-IoT-04**] NGP shall support Ultra-Reliable Communications (URC) for low-bitrate applications.

NOTE 6: Recommendation ITU-R M.2083-0 [i.4] defines the terms URLLC and URC.

[**Iss-IoT-05**] NGP shall support delay-tolerant networking, and in particular devices that are asleep (to save battery) for much of the time.

[**Iss-IoT-06**] For devices that are asleep (to save battery) for much of the time, NGP shall minimize the amount of power required to transmit when they wake up.

[**Iss-IoT-07**] NGP shall provide an efficient means to notify a user when communication with a specified device is lost.

NOTE 7: This allows an alarm to be raised in the event of failure without needing to continually poll the remote device.

[**Iss-IoT-08**] NGP shall allow an application to specify latency requirements for a flow and, for flows that are defined by the application to be latency-critical, shall report to the application the maximum and minimum latency each flow will experience.

6.9 Energy Efficiency

[**Iss-EE -01**] NGP shall minimize the need for complex address, header, compression and tunnelling processing in handling network protocols.

6.10 MEC

[**Iss-MEC-01**] NGP should provide protocol support that enables edge cloud platform capabilities that can offer such capabilities as caching, pre-fetching and other edge hosted capabilities for such services as video, application and VR optimization.

[**Iss-MEC-02**] NGP should provide access agnostic capabilities that enhance next generation wireline and wireless edge nodes for supporting the Edge computing, storage and optimization. Such features to be considered in NGP are:

1) edge-cloud capabilities; and

2) differentiating conventional traffic from traffic related to cloud applications, e.g. computation offloading and storage.

6.11 Mission Critical Services

[Iss-MCS -01] In the context of Substation Protection and Control (SPC), Mission Critical Services (MCS), NGP shall support the following:

- Latency: as low as 1 ms end-to-end
- Packet loss rate: as low as 10-4
- Transmission frequency: 80 samples/cycle for protection applications. 256 samples/cycle for quality analysis and recording
- Data rate: ~12,5 Mbps per MU at 256 samples/cycle
- Range: provide coverage to the substation

NOTE 1: Further information relating to SPC-MCS can be found in the reference 3GPP TR 22.862 [i.3].

[Iss-MCS -02] In the context of Smart Grid System with Distributed Sensors and Management (SGSDS), MCS, NGP shall support the following:

- Throughput: from 200 to 1 521 bytes reliably (99,999 %) delivered in 8 ms.
- One trip time latency between any two communicating points should be less than 8 ms for event-triggered message that may occur anytime.
- Device density:
  - dense urban hundreds of UEs per km^2
  - urban around 15 UEs per km^2
  - populated rural max 1 UE per km^2

NOTE 2: Further information relating to SGSDS-MCS can be found in the reference 3GPP TR 22.862 [i.3].

[Iss-MCS -03] In the context of Public Safety (PS) PS, MCS, NGP shall support:

- preferential handling of its traffic
- dynamic allocation of quality of service, priority and pre-emption parameters including:
  - Access Class (AC)
  - Quality of Service Class Identifier (QCI)
  - Allocation and Retention Priority (ARP)
  - Guaranteed Bit Rate (GBR)

- Aggregate Maximum Bit Rate (AMBR)
- Differentiated Services Code Point (DSCP)

NOTE 3: Further information relating to PS-MCS can be found in the reference 3GPP TR 22.862 [i.3].

[Iss-MCS -04] In the context of Multimedia Priority Service (MPS), MCS, NGP shall support preferential handling, and priority treatment.

NOTE 4: Further information relating to PS-MCS can be found in the reference 3GPP TR 22.862 [i.3].

[Iss-MCS -05] In the context of General Group Communications (GGC), MCS, NGP shall support one-to-many or many-to-many communications.

NOTE 5: Further information relating to GGC-MCS can be found in the reference ETSI TS 122 280 [2].

6.12 Drones and Autonomous Vehicles and Connected Vehicles

[**Iss-UAV-01**] In order to meet any requirement resulting from the specification of 3GPP TR 22.862 [i.3], potential requirement [PR 5.1.3-024], "*Continuous wireless coverage for UAV (Unmanned Aerial Vehicles) flying at low altitude of [10-1 000] meters with maximum speed of [200 km/h]*", the NGP architecture shall support persistent data communication for UAVs.

6.13 Ultra Reliable Low Latency Communications

[**Iss-URLLC-01**] NGP should support 'make before handover' so that a User Equipment connects to a target Access Network (AN) before disconnecting from the source AN.

[**Iss-URLLC-02**] NGP should support enhanced coordination between application and mobile network in order to maintain seamless service continuity when migrating application instances (e.g. Virtual Machine based) or application-specific user-related information between different edge nodes.

[**Iss-URLLC-03**] NGP Should support deterministic processing delay of the URLLC data stream in network nodes.

[**Iss-URLLC-04**] NGP should support transmission control that accommodates ultra-low latency requirements for both transport and handover between access technologies and within the same access technology at the NGP architectural level.

Annex A (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Mr Gerry Foster, University of Surrey (Institute of Communications Systems), g.foster@surrey.ac.uk

Other key contributors (lead scenario authors):

Addressing Requirements	Mr Lin Han, Huawei, lin.han@huawei.com
	Dr John Day, Boston University, jeanjour@comcast.net
	Eduard Gras, i2cat, eduard.grasa@i2cat.net
Security Requirements	Mr Mark Shepherd, Tencastle Limited, mark@tencastle.com
Mobility Requirements	Mr Gerry Foster
Context Awareness Requirements	Mr Gerry Foster
Multi-Access Requirements	Mr Andy Sutton, BT, andy.sutton@ee.com
Performance Requirements	Dr Chang Ge, University of Surrey, ICS, c.ge@surrey.ac.uk
	Dr John Day, Boston University, jeanjour@comcast.net
Network Virtualisation Requirements	Ms Kiran Makhijani, Huawei, kiran.makhijani@huawei.com
IoT Requirements	John Grant, Nine Tiles, j@ninetiles.com
Energy Efficiency Requirements	David Lake, dlake@CISCO.COM
MEC Requirements	Georgios Karagiannis, Huawei, georgios.karagiannis@huawei.com

History

Document history		
V1.1.1	April 2017	Publication