

Three Lines in the Standard

An ant leaves a trail. Not because it plans to. Because the environment is built that way - it remembers every step until the trail evaporates. This serverless memory is precisely what makes the colony resilient, adaptive, and open.

The three previous articles in this series explained why this principle applies to 6G, how it works technically, and for whom it changes everything. One question remains: what exactly needs to be written into the standard to make this a reality.

The answer fits into three elements.

What Is Wrong Now

The standards of previous communications generations addressed speed, latency, and throughput. They did not address network memory. Every device in a 5G network knows only what it has been told centrally. It does not accumulate knowledge about path quality. It does not leave a trail for the next device.

This is not a technical limitation - it is an architectural choice. A choice that can be changed. But only if it is made now, while the 6G standard is still open.

Three gaps that need to be closed:

The first - packets have no mechanism to leave a trail about path quality. The second - nodes have no common language for reading these trails. The third - tags have no verification mechanism without a central arbiter.

Each of them is closed by one specific technical solution.

Proposal One - A Path Quality Field in the Packet Header

Every data packet in 6G should contain a service field - a Path Quality Tag (PQT). This field, no larger than 16 bytes, includes three parameters: the measured latency on the last segment of the path in milliseconds, the packet loss rate on the last segment, and a measurement timestamp.

The obvious objection: adding 16 bytes to every packet increases overhead. The answer: PQT is implemented not as a separate protocol layer but as an optional extension of an existing header - following the same model by which optional fields already work in TCP and IPv6. The PDCP header in the 5G stack is itself 16 bytes - PQT fits within the already established logic of service fields.

The receiving node reads the PQT of the previous node, compares it with its own measurements, and writes an updated value before forwarding. The sending node uses the accumulated PQT values of its neighbors to choose the next hop.

The lifetime of the tag - TTL-Q - is set independently of the packet's own TTL. Proposed starting values for discussion in the working group: 30 seconds for latency metrics, 5 minutes for loss metrics. The reasoning: latency metrics change quickly and should expire quickly; loss metrics

reflect more stable channel characteristics. Specific values are subject to refinement based on measurements in real networks. An expired tag resets to zero automatically. The network does not get stuck in the past.

A precedent exists: the QUIC protocol already measures RTT in real time within a single connection. PQT extends this principle to the level of the entire network - memory about path quality becomes distributed rather than local.

Proposal Two - An Open Tag Format as a Mandatory Element of the Standard

The PQT field must be defined in the 6G standard as a mandatory protocol element with an open specification. Not recommended - mandatory.

Today every equipment manufacturer implements similar mechanisms in a proprietary format. A device from one manufacturer cannot read the tag of a device from another. A network assembled from heterogeneous equipment cannot form a unified distributed memory.

An open standard for the PQT format is the same as an open standard for the IP address format. Without it, the internet would not have been possible. Without open PQT, distributed network memory will not be possible.

The specific requirement for the standard: an RFC-compatible specification of the PQT format, mandatory for all devices seeking 6G certification. A manufacturer may add proprietary fields on top of the mandatory ones - but the three base parameters must be readable by any node in the network.

Proposal Three - Tag Verification Through a Trusted Hardware Module

An open format creates a vulnerability: if any node can write a tag, any node can write a false tag. Falsification of path quality data is an attack on the entire routing system.

An ant cannot lie about a pheromone trail - the chemical molecule is either there or it is not. A technical node can lie. The solution: the PQT tag must be signed by the device's trusted hardware module - a Trusted Execution Environment (TEE) or equivalent.

The signature does not reveal the user's identity. It confirms only one thing: the tag was formed on the basis of real measurements by a secure chip, not fabricated by a software layer. The receiving node verifies the signature locally, without querying a central verification server.

This is not new technology. TEE is already implemented in virtually every modern smartphone and tablet through ARM TrustZone. A solution to the interoperability problem between different manufacturers' implementations also exists - the GlobalPlatform TEE API, an open standard already in use across the mobile industry that provides a unified software interface for trusted applications on top of different hardware implementations. The IEEE IC25-009-01 document explicitly names open trusted hardware modules as a foundational element of the open 6G device

ecosystem. The proposal is to establish the use of TEE with a GlobalPlatform-compatible API for signing PQT as a standard requirement - not an option.

What Happens If These Three Elements Are Adopted

The 6G network acquires distributed memory about path quality. Every packet carries a verified trail of previous packets. Every node makes decisions based on current local knowledge rather than stale centralized tables.

The routing system becomes self-organizing. The failure of any node does not disrupt the network - flows reroute through neighboring nodes, following fresh tags. There is no single point of failure because there is no single point of memory.

The open device ecosystem architecture described in IEEE IC25-009-01 gains a technical foundation. A device with an open trusted chip, participating in the network through PQT, does not need an operator's permission to route traffic through neighbors. A neighbourhood hotspot - a device sharing connectivity with nearby devices - becomes technically possible without changing the operator's business model.

What Happens If They Are Not

The 6G standard will reproduce the architecture of previous generations - faster, with lower latency, with greater throughput. The center will remain. Memory about path quality will remain the property of whoever owns the infrastructure.

The doctor in the regional town will remain dependent on the operator's commercial decision about the profitability of a base station. The farmer, the manufacturer, the teacher - all of them will remain on the periphery of an architecture that was not designed for them.

The window is open now. The 6G standards are being shaped in these years. Three lines in the specification - a mandatory PQT field, an open format, a TEE signature - are not a revolution. They are an architectural choice that will define the next twenty years.

Closing the Series

Four articles form a single argument.

The first showed: a network with no owner is not a utopia - it is an architectural consequence. Nature proved this a hundred million years ago.

The second showed: the mechanism that implements it already partially exists in operating protocols. Three gaps remain.

The third showed: behind this stands a specific person - the one the center does not serve and never has.

This fourth article names three specific elements that close those gaps.

What follows is a decision for the standardization working groups.