Density as an Availability Condition for Environment-Dependent Trust Roots

The P-DENS and P-OBS Principles

Contribution to IEEE Industry Connections activity IC25-009-01 *A Technical Reference Architecture Framework for an Open 6G Device Ecosystem*

Version 2.0 | July 2026 | For IC Activity Review | Supersedes all v0.x and v1.x drafts

---

Abstract

The contributions of this series have specified how trust roots must be composed (P-AUTH), how accountability must be made visible (ACP), how roots must be independent by foundation (P-INDEP), and how authority may be delegated without moving trust (P-DELEG). Each specifies the *integrity* of a root: whether it can be forged, extracted, or reached by a single compromise. None specifies its *availability.*

Two of the four trust-root carriers that make the quorum affordable do not exist on the device. An off-device root verified by geometry requires consistent measurements from several independent nodes; a witness root requires witnesses from independent owners. Their readiness is a function of node density in the deployment area, and node density is a quantity no requirement in the framework declares.

This document states the missing condition and proposes what follows from it. **R12** requires that availability conditions for environment-dependent roots be declared and that correct degradation be verified. **P-DENS** requires that every device provide standalone utility at zero participating neighbours, that it measure local density and adapt autonomously, and that the architecture declare both a floor and a ceiling on density per environment. **P-OBS** answers the incentive question left open by the economics of witnessing: participation is sustained by the exchange of non-substitutable local observation rather than by payment. **R21** requires each normative requirement in this framework to be classified as demonstrable or merely attested, which is the question Part Eight of the accompanying series poses to this technical work by name.

The document also states plainly what it does not solve. Removing the centre from the carriage of data does nothing about the concentration of assembled knowledge, and the architecture currently under study in 3GPP routes sensing results to the core network for exposure to third-party applications. That is the concentration arriving by default rather than by decision, and this contribution names it without closing it.

Keywords: 6G device ecosystem, trust roots, availability, node density, percolation, standalone utility, integrated sensing and communication, cooperative perception, witnessing incentives, IEEE IC25-009-01

---

1. Introduction

P-INDEP established that the cost of attacking a quorum of trust roots is set by its cheapest shared foundation. The resolution document closed the three questions P-INDEP left open, introduced P-DELEG binding minimum quorum to action class, and named four carriers independent by foundation and already paid for: a dedicated secure element, a physically separate PUF, an off-device root based on physical-layer geometry, and a quorum of neighbouring witnesses.

Two of those four do not exist on the device. They exist in the space around it. That is precisely what makes them valuable, since a carrier the owner does not own cannot share a coupling factor with the device by construction. It is also what makes them conditional. A root that lives in the neighbourhood is available only where there is a neighbourhood.

The framework does not say how much of a neighbourhood, nor what a device should do where there is not one. This document supplies that, and follows the consequences further than the first question goes.

---

2. The availability of a trust root

2.1 Integrity and availability are distinct

Dependability practice distinguishes availability, defined as readiness for correct service, from integrity, defined as absence of improper state alteration. Both are first-class attributes; they fail for different reasons and are not interchangeable.

The independence analysis of P-INDEP is an integrity analysis throughout. The generative rule of R7 defines a coupling factor as a node of the dependency graph whose single compromise reaches more than one quorum root, and the compromise-injection testing of R8 verifies that definition experimentally. Both are correct. Both are silent on a second failure mode.

A root can fail without being attacked. It can simply not be there. No adversary is required, no coupling factor is involved, and no injection experiment will reveal it, because nothing has been compromised. The quorum degrades because the environment did not supply what the specification assumed.

This is not an idiosyncratic reading. A 2026 survey of roots of trust categorises them by function and evaluates them against confidentiality, integrity and authentication. Availability does not appear among the security goals. The omission is general to the field, and this framework inherited it.

2.2 Connectivity is a phase transition

The density on which environment-dependent roots rely is not a smooth parameter. Place nodes at random on a plane and connect any pair within radio range. Below a critical mean degree only finite clusters exist and spanning connectivity is impossible; above it a spanning cluster appears. Numerical work with rigorous confidence bounds places the critical mean degree of the two-dimensional disc model between 4.508 and 4.515, while the bounds that have been proved rigorously remain several times wider and no closed form is known.

The number is model-dependent and should not be treated as a design target. The structural fact is what matters: below the transition the network does not degrade gracefully, and neither do the roots that depend on it. There is no partial-credit region in which a geometric root is somewhat available.

2.3 The density conditions already implicit in the framework

Two requirements in the resolution document carry density conditions stated as counts of nodes rather than as conditions on deployment. The off-device root is recognised only under geometric verification by consistent measurements from no fewer than three independent nodes. The witness root is recognised as equivalent for the higher agent classes given no fewer than three witnesses from independent owners.

Mapping those counts onto the quorum scale gives the following. This is not a criticism of the scale, which is correct as written; it is the deployment condition the scale implies and does not state.

Agent class	Minimum k	Roots available at very low density	Density condition
Executor	k = 1	Secure element (on device)	None. Operative at zero neighbours.
Adapter	k = 2	Secure element only	At least three independent nodes, or three independent-owner witnesses, in range
Strategist	k = 3	Secure element plus user presence	As Adapter, plus live presence

The consequence is bounded and specific. In a deployment area below the condition, devices remain fully conformant, but only the Executor class is operable and mandate width under P-DELEG narrows accordingly. Nothing is insecure. Something is unavailable, and the architecture should say which, where, and from what density onwards.

2.4 Proposed requirement

R12 (declared availability conditions). For every trust root whose recognition depends on entities outside the device, the reference architecture shall declare the environmental condition under which that root is recognised, expressed as a minimum count of qualifying independent entities within sensing or communication range, together with the device behaviour when the condition is not met. Conformance testing shall include verification of correct degradation: a device shall detect the absence of the condition, shall not report a quorum it did not obtain, and shall restrict its agent class accordingly.

Rationale: an independence audit verifies that roots do not fail together under attack; it does not verify that they are present. Both are required before a quorum can be relied upon.

---

3. P-DENS: threshold density, standalone utility, and a ceiling

3.1 The problem

Density is not a free parameter. It is the result of people choosing to own devices. If a device becomes valuable only once other people have bought one, the first purchase returns nothing, the

condition of clause 2.3 is never met, and the higher agent classes remain theoretical. The security model then rests on an adoption assumption that no part of the specification defends.

3.2 Standalone utility is available from existing hardware

The requirement that a device be useful at zero participating neighbours does not imply added components. The communication transceiver is already a sensing instrument.

This is settled rather than prospective. IEEE Std 802.11bf-2025 was published on 26 September 2025 as Amendment 4 to IEEE Std 802.11, defining WLAN sensing as the use of PHY and MAC features of stations to obtain measurements useful for estimating features of objects in an area of interest. Integrated sensing and communication is one of six usage scenarios of the IMT-2030 framework approved by the ITU Radiocommunication Assembly in November 2023.

In the cellular track the position is more precise and less comfortable, and clause 9.3 sets it out.

Propagation in the bands under consideration reinforces rather than obstructs the argument. Strong interaction with the medium, including absorption by H2O and O2 and heavy obstruction loss, degrades the communication link and simultaneously makes the same aperture a sensitive instrument for the state of the medium.

The physical mechanisms are mature and independently deployed: Doppler shift for motion and respiration, time of flight and reflection for ranging and occupancy, channel-state variation for presence, resonant absorption for composition of the medium. None is speculative and none requires hardware beyond what the quorum roots already assume.

3.3 The ceiling, and why a floor alone is wrong

Part Eight of the accompanying series supplies a correction this contribution must carry.

A signal that travels out to a body and back weakens twice over. Under the two-way law, received power falls as the fourth power of range, so doubling the distance costs about 12 dB. The margin by which a person reads their own body better than the surrounding infrastructure reads it is therefore a function of distance. Doubling areal node density shrinks mean spacing by the square root of two and spends about 6 dB of that margin; doubling density along a street, which is how relays are actually strung, halves the spacing and spends about 12 dB.

Density therefore buys availability of trust roots and sells privacy margin at a known rate. Three independent lines converge on the same conclusion: trust roots need density; privacy margin is spent by density; and the non-substitutability of observation, which clause 4 relies on for participation incentive, dissolves as density rises. A requirement stating only a floor is incomplete.

3.4 Acknowledgement of prior art

Standalone-first adoption is not a new observation. In platform economics it is a recognised bootstrapping strategy, commonly expressed as attracting users with a single-player tool and letting the network form afterwards. This contribution claims no novelty for the strategy. It claims that in this architecture the property is not a commercial option but a precondition for the availability of trust roots, and that properties on which security guarantees depend belong in the specification rather than in a market plan.

3.5 Normative principles

P-DENS-1 (standalone utility). No function on which a device's value to its owner depends shall require the presence of participating neighbours. Every conformant device shall provide measurable standalone utility to its owner at zero participating neighbours. Sensing performed by the communication transceiver is recognised as a first-class device capability for this purpose and shall not be specified as an optional extension of the communication function.

Rationale: density is produced by individual purchase decisions taken before the network exists; a device whose value begins after adoption cannot generate the density its own security model requires.

P-DENS-2 (local measurement and autonomous adaptation). The device shall measure the number of qualifying participating nodes within range locally, using its own transceiver, and shall transition between end-device behaviour and relaying and witnessing behaviour autonomously on the basis of that measurement. The threshold and the transition shall be fixed by the standard and shall not be subject to operator or vendor authorisation. The behaviour of the device as shipped forms part of that specification and is not a vendor prerogative. The measured density and the resulting agent class shall be reported in the accountability chain.

Rationale: a transition requiring permission recreates a permitting party; a transition fixed by the vendor recreates the silent quorum-reduction scenario of the P-INDEP diversion analysis at the level of the environment instead of the level of k. Behaviourally, the shipped state determines the outcome for the overwhelming majority of devices, since almost no owner ever changes it; the argument of clause 4 justifies a default and does not describe a decision that owners make.

P-DENS-3 (declared floor and ceiling). The reference architecture shall state, per device class and per environment class, both the node density at which each distributed function and each environment-dependent trust root becomes operative, and the density above which the deployment shall not be driven, together with the measurement method and the averaging window. Where a function is not operative, the device shall report unavailability rather than degraded operation.

Rationale: an undeclared threshold cannot be tested and will be assumed satisfied by every implementer. A floor without a ceiling instructs the ecosystem to maximise a quantity that has a known privacy cost per doubling.

---

4. P-OBS: observation as a second exchange layer

4.1 The problem created by clause 3

P-DENS solves the first purchase and creates the second problem. A device genuinely sufficient on its own gives its owner no reason to relay a stranger's traffic or witness a stranger's events. Relaying costs energy, witnessing costs energy and attention, and both expand exposure. The rational outcome is a landscape of self-sufficient islands: fully conformant, and delivering none of the density on which the higher agent classes depend.

This is the question left open in the resolution document under the economics of witnessing, where the incentive model was deferred to a separate specification. The answer proposed here adds no

incentive layer. It observes that the incentive is already present in the exchange, and was overlooked because the exchange was assumed to concern one commodity.

4.2 Substitutable and non-substitutable goods

Traffic is substitutable. A neighbour can obtain carriage from an operator, and so can the device owner. Exchange of a substitutable good approaches a zero-sum negotiation, which is why relaying has to be priced, policed and incentivised from outside.

Local observation is not. A device measures the volume it occupies and no other. The state of a location two hundred metres away cannot be obtained by any route other than a device that is there. Each participant holds something the others cannot generate, and the exchange is positive-sum by construction.

Witnessing, as specified for the witness root, is a special case of this with a single predicate: the continued presence and normal behaviour of a neighbouring node. Generalising the predicate set from node presence to environmental conditions converts a one-directional service into a reciprocal exchange, and supplies the missing incentive.

4.3 Three bounds on that argument

Overlap. Two devices whose sensing volumes coincide exchange identical views and gain nothing. Two devices whose volumes are disjoint gain information but cannot verify one another. Useful exchange requires partial overlap: a shared region sufficient for cross-checking, and a disjoint region sufficient for information gain.

The overlap requirement therefore has two distinct senses, and the earlier drafts of this contribution conflated them. Agreement between publishers *about the same predicate* is redundancy: it enables verification and, being redundant, adds little to the joint information published about the volume. Coverage of the same space *from different vantage points* enables triangulation: it adds information about the position of a subject that neither publisher holds alone. The first is what verification needs. The second is what privacy must bound. A single scalar defined as intersection volume over the smaller volume measures the second, not the first, and clause 4.5 corrects it.

Density. Non-substitutability is not a property of the good but of a density regime. Where fifty devices observe the same street each is replaceable and observation becomes as substitutable as traffic. The incentive argument holds in the sparse-to-medium regime and dissolves in the regime P-DENS is designed to produce. This is a second reason for the ceiling of P-DENS-3.

Defaults. The argument is not a description of owner choice. Owners do not weigh substitutability; almost none will ever change a setting. What the argument establishes is that a standard may reasonably require participation as the shipped state, and may justify that requirement in terms of the owner's own interest rather than by appeal to solidarity. The mechanism that determines outcomes is P-DENS-2.

4.4 Precedent, and the limit of that precedent

Exchange of locally perceived environment between independently owned devices is standardised for road vehicles. ETSI TS 103 324 specifies a collective perception service in which a station broadcasts what its sensors perceive of the environment rather than its own state; SAE J3224

defines a sensor-sharing service for the same purpose. The messages carry interpreted object descriptions rather than raw sensor data, which keeps them compact, interoperable, and privacy-tractable.

The plausibility rule adopted in P-OBS-2 is *not* taken from those standards, and earlier drafts of this contribution overstated the precedent. The ETSI framework for misbehaviour detection and reporting specifies detectors for cooperative awareness messages; detectors specific to collective perception messages were left to a future version, and the rule that an object reported outside the reporting station's perception area should be treated as suspect was proposed in the research literature. The vehicular domain standardised the exchange first and left its integrity check open. That is the sequence this contribution proposes not to repeat.

4.5 Normative principles

P-OBS-1 (second class of tags). In addition to path-quality tags, a conformant device shall be capable of publishing environment-observation tags: signed statements describing locally measured conditions within its declared sensing volume, carrying a bounded information content, an independent time to live, and a declaration of the volume from which they derive; readable by neighbouring devices without operator mediation; imposing no obligation on the publishing device to relay third-party traffic.

Rationale: an exchange of non-substitutable goods sustains participation without external payment; a witness root is a special case of such an exchange with a single predicate.

P-OBS-2 (declared volume, overlap, and plausibility). Every observation tag shall carry a declaration of the sensing volume from which it was derived. A receiving device shall reject, and may report through the accountability chain, any observation whose subject lies outside the publisher's declared volume, or which contradicts consistent observations from independent publishers whose volumes intersect the same region. The standard shall specify, per device class and environment class: a minimum *predicate-agreement overlap*, defined as the fraction of a publisher's declared volume within which at least one independent publisher can produce a comparable observation of the same predicate class; and a maximum *vantage overlap*, defined as the fraction of a volume covered by publishers at distinct positions such that triangulation of a subject becomes possible below the granularity floors of the companion specification.

Rationale: verifiability of observation depends on partial overlap between publishers, and exposure of subjects depends on a different sense of overlap. Specifying one scalar for both bounds the wrong quantity.

P-OBS-3 (bounded content and excluded subject matter). Observation tags shall carry interpreted, quantised statements about the state of the environment. Raw channel-state data shall not be published. The occupancy of enclosed spaces, and the presence, activity or physiological state of persons within them, shall not be published to neighbouring devices in any class of tag, and shall be transmitted only to a recipient designated in advance by the subject. The permitted predicate set, the publication limits, and the treatment of persons who are not participants are specified in the companion privacy specification and form part of conformance.

Rationale: the same channel measurements that make a device useful alone are sufficient to identify individuals with accuracy close to complete, from equipment requiring no special hardware. The

prohibition on publishing them takes precedence over every other publication limit: where each statement is rich, identification saturates within a few tens of statements and capping their number achieves nothing. Restricting the published predicate to the state of the environment costs the exchange nothing that carries the incentive, since rain on a field, a blocked road, changed air and signal conditions are all non-substitutable and all concern a place rather than a person. It also keeps conformant publication outside the scope of personal-data regimes of the European type, and keeps a device owner from becoming a data controller by operation of the narrow reading of the household exemption established in Case C-212/13.

---

5. Demonstrable and attested requirements

Part Eight of the accompanying series poses a question to this technical work by name: some absences announce themselves, since the presence of a shared phase reference is measurable by any receiver, while others do not, since no outsider can see how much memory a node has. An absence that only a certifying body can attest to returns the construction to somebody's word, which is the thing it was built to escape. Which absences can be demonstrated rather than certified, that part says, is a question the accompanying technical work has to answer and has not yet answered.

This clause answers it for the requirements of this package.

Requirement	Nature of the guarantee	Verifiable from outside
R18, physical suppression permitted	Physical	Yes, by measurement
P-DENS-2, local density measurement and transition	Behavioural, physically grounded	Yes, by observing transitions against measured density
P-DENS-1, standalone utility	Functional	Yes, by operating a device with no neighbours
R13, no raw channel data published	Content rule	Yes, by inspecting published tags
R15, publication limits	Content and rate rule	Yes, by counting tags over a volume
P-OBS-2, declared volume and plausibility	Content rule, enforced by every receiver	Yes, in part
R12, correct degradation	Behavioural	Yes, by conformance test
R16, evaporation	Absence of retention	**No**
R19, no export of raw measurement	Absence of a path	**No**

The last two are the absences Part Eight describes. R16 binds conformant receivers and offers nothing against a party that records the air; R19 binds a device that has no incentive to advertise a covert path. Neither is thereby worthless: both are enforceable through certification, and certification is a real constraint on a manufacturer. But they are constraints of a different kind, and presenting them alongside the others without distinction misrepresents the strength of the construction.

R21 (classification of guarantees). Every normative requirement in this framework shall be classified as *demonstrable*, meaning that conformance or its absence can be established by an independent party from observable behaviour or emitted signals, or as *attested*, meaning that conformance can be established only by a certifying body with privileged access. The classification shall be published with the requirement. Where a requirement is attested, the architecture shall state whether a demonstrable equivalent exists and why it was not adopted.

Rationale: a construction that removes the need to trust an operator, and replaces it with the need to trust a certifier, has moved the dependency rather than removed it. Making the distinction visible per requirement is the minimum honesty the construction requires, and it creates pressure toward demonstrable formulations where they exist.

The underlying observation is not original here. Work on transparency in confidential computing notes that attestation verifies that intended software is running on an intended platform but does not establish the absence of vulnerabilities or backdoors, and proposes transparency as a complement to attestation for that reason. Commentary on platform attestation has separately observed that its most contested aspect is not cryptographic but the power relation it creates, since a device may belong to its owner while its ability to function depends on a remote validation service. R21 applies the same observation at the level of a requirement rather than a platform: it does not propose a new mechanism, it requires that the framework state, for each of its own requirements, which kind of guarantee is on offer.

Two limits of R21 should be recorded. It does not prevent self-serving classification, since an implementer with a preference for opacity may argue that a demonstrable requirement is attested; the counter is that the classification is published and can be disputed. And the classification in the table above covers only those requirements for which the distinction is contested; a complete classification of every requirement in the framework, which R21 demands, is work for the group rather than for this contribution, and its absence here is an acknowledged inconsistency between what R21 asks and what this document supplies.

---

6. What this contribution does not solve

Producing an observation is stubbornly local: to know about a place a device must be there, and covering the two-hundredth place costs as much as the first. That linearity resists centralising collection. The value of observations is not linear. An assembled picture of a region is worth far more than the sum of the readings it is built from, and whoever assembles it captures the difference.

This is not hypothetical. Traffic layers in mapping products, crowd-sourced positioning and activity heatmaps are all built from non-substitutable local observations produced by distributed devices, and all are centralised. The physical stubbornness of the raw material did not prevent it; concentration happened one layer up.

Nor is it distant. The ISAC architecture currently under study in 3GPP places sensing signal transmission, measurement and reception in the radio access network, with the core network handling sensing data and exposing results to third-party applications. That is the concentration of assembled knowledge arriving as the default architecture rather than as a decision anybody took.

An architecture that removes the centre from the carriage of data and says nothing about the assembly of knowledge has moved the centre rather than removed it. Candidate answers exist and each costs something: making readability conditional on also publishing, or binding it to physical proximity so that a distant collector receives only ciphertext. Both make the channel less open than the earlier parts of the accompanying series argued for.

The problem is named here, the direction is known, and it is not closed by this contribution. It is the first item of clause 11.

---

7. Diversion analysis

Following the practice of this series, the principles are presented with the scenarios in which they are defeated if left implicit.

Scenario	Mechanism	Counter-requirement
Standalone-only device	Vendor ships sensing, which sells the product, and never enables relaying or witnessing, which cost energy and return nothing. Density never rises	P-DENS-2, autonomous transition fixed by standard, shipped state normative, reported through the accountability chain
Density maximised	Ecosystem reads a floor as an instruction and drives density upward, spending privacy margin at 6 dB per doubling with nothing to stop it	P-DENS-3, declared ceiling per environment class
Full-overlap deployment	All participating devices co-located, for example in one building. Vantage overlap approaches one, exchange carries no new information, reported density overstates useful density	P-OBS-2, maximum vantage overlap
Fabricated observation	Publisher reports conditions it did not measure, cheaply and at scale, to influence routing, pricing, or neighbours' behaviour	P-OBS-2, plausibility against declared volume, cross-check against intersecting publishers
Colluding publishers	Several publishers under one controlling party agree a false report, satisfying naive cross-checks	Owner independence as already required for witnessing, extended to observation; minimum count of independent publishers per confirmed observation
Assumed quorum	Device below the density condition reports a quorum it did not obtain, or proceeds silently at lower k while presenting the higher class	R12, declared conditions and verified degradation; P-DENS-3, unavailability reported rather than degraded operation
Passive aggregator	Party publishes nothing, collects everything, assembles the regional picture and sells it back	**Not closed.** Clause 6; open question 11.1

Scenario	Mechanism	Counter-requirement
Occupancy by another name	Predicate nominally environmental but chosen so that occupancy is recoverable, for example fine-grained motion in an enclosed volume	P-OBS-3 and the predicate allowlist of the companion specification
Density-based exclusion	Permanently sparse areas never satisfy the condition, and the higher agent classes are unavailable exactly where centralised service was already absent	Declaration under R12 makes the exclusion visible and reviewable rather than silent; open question 11.4

8. Validation protocol

The principles of clauses 3 and 4 make an empirical claim: that standalone utility and reciprocal observation raise the proportion of devices that end up participating. The claim can be wrong, and this series holds that a principle which cannot survive attack should not be standardised.

- **Arms.** Three configurations: (A) communication only; (B) communication with local sensing available to the owner; (C) communication with local sensing and reciprocal exchange of observation tags between neighbours.
- **Unit of randomisation.** Geographic clusters, not individuals. The effect propagates between neighbours by construction, so individual assignment violates the independence assumption and biases the estimate toward zero.
- **Stratification.** Clusters stratified by built density and baseline device density before assignment.
- **Primary metric, pre-registered.** Proportion of devices with relaying or witnessing behaviour active at day 90. Secondary: median number of qualifying neighbours; median predicate-agreement and vantage overlap. Tertiary: retention at month 12.
- **Sample.** Of the order of thirty clusters per arm for a medium effect, the unit of observation being the cluster. A formal power calculation is required before launch.
- **Success criterion, fixed in advance.** Arm C exceeds arm A by at least fifteen percentage points on the primary metric, and the advantage persists at month 12. Where a power calculation on pilot data indicates a different margin, the revised margin shall be published before enrolment begins.
- **Falsification.** If arm B does not differ from arm A, P-DENS-1 is not supported. If arm C does not differ from arm B, the reciprocal-exchange argument of clause 4 is not supported and P-OBS should be withdrawn.
- **Ethical precondition.** Arm C publishes observations concerning volumes in which persons who are not enrolled are present. It shall not be initiated until the publication limits of the companion specification have been calibrated for the relevant environment class, and not without an assessment of the impact on those persons. Arms A and B carry no publication channel and are not subject to this precondition.

A twelve-month observation is required rather than optional, because a ninety-day advantage is consistent with novelty effects that decay.

9. Relationship to existing work

9.1 Principles of this series

P-AUTH. Inherited unchanged. Observation tags are traces with a lifetime, not stored secrets.

ACP. The accountability registry is the reporting channel for measured density, class transitions, misbehaviour reports under P-OBS-2, and violations of publication limits detected by neighbours.

P-INDEP. Complementary, not competing. P-INDEP governs whether roots fail together; R12 governs whether they are present. The generative rule of R7 is defined over compromise and by construction does not range over absence, which is why this condition was not caught by it.

P-DELEG. Mandate width follows agent class, and agent class follows available quorum, so the density condition propagates to mandate width. A device below the condition should issue Executor-class mandates and no wider.

9.2 External standards

IEEE Std 802.11bf-2025 for standardised sensing measurement between stations. Recommendation ITU-R M.2160-0 for the IMT-2030 framework. ETSI TS 103 324 and SAE J3224 for cooperative perception between independently owned devices. ETSI TR 103 460 and TS 103 759 for misbehaviour detection and reporting practice.

9.3 Current 3GPP work, and why timing matters

The Release 19 channel-modelling study for ISAC encompasses all six sensing modes: BS monostatic, BS-BS bistatic, BS-UE bistatic, UE-BS bistatic, UE-UE bistatic, and **UE monostatic**. The mode on which P-DENS-1 depends is therefore defined and modelled.

It is not, however, being specified normatively. Release 20 work in the 5G-Advanced track concentrates on gNB monostatic sensing for the uncrewed-aerial-vehicle use case; the RAN plenary consensus recorded in working-group discussion is gNB monostatic, and UE-based sensing is noted as carrying a strong RAN dependency. The first normative 6G specifications, including 6G ISAC, are expected in Release 21.

Three consequences follow, and they are the reason this contribution is submitted now rather than later.

First, **P-DENS-1 is unimplementable in the cellular track unless UE monostatic sensing is specified.** The requirement is not exotic: the mode exists, the channel model exists, and other participants are already arguing that the architecture should be extensible to UE-based sensing rather than redesigned later.

Second, **the terminology is undefined.** Working-group discussion records that TS 22.137 refers to monostatic, bistatic and multistatic sensing, while the terms *gNB-based sensing* and *UE-based sensing* are not defined anywhere in 3GPP. A framework that needs to say "the device senses without network participation" currently has no standard term for it.

Third, **the architecture on the table is the aggregation architecture** described in clause 6. An architecture designed around one topology is not later redesigned around another.

---

10. Effects on the earlier contributions of this series

Four kinds of effect are distinguished, because conflating them makes notices of this sort useless.

Corrected. The resolution document argues that the cost of a witness root is negative, on the grounds that witnessing is one more service of network participation alongside relaying and is therefore already paid for. That holds where relaying is already occurring. Below the condition of R12 it is not occurring, and it is not occurring for reasons that include the absence of the participation the argument assumes. The claim should be scoped: the cost of a witness root is negative in deployments already above the density condition, and is not established below it. The recognition of the witness root and the three-independent-owner threshold are unaffected.

Answered. The resolution document lists the economics of witnessing as an open question. P-OBS supplies the model. One part should stay open: protection against collusion among publishers acting in bad faith remains unresolved here as well.

Qualified. The generative rule of R7 and the closure of the first P-INDEP open question are correct and are defined over compromise. A scope note should record that the closure is complete for compromise and does not extend to availability, so that the question is not treated as fully settled.

Extended. The agent-class table should carry the density condition per class, or a note referring to R12. Four new record types are proposed for the accountability registry: measured density and resulting class; transitions between end-device and relaying behaviour; rejections of implausible observations; violations of publication limits detected by neighbours. One interaction is registered: the personal baseline protected under P-AUTH and the observations bounded by P-OBS are the same physical quantity measured for different purposes, and R19 of the companion specification exists so that no export path allows a publication channel to become a baseline repository by accumulation.

Requested action. One re-issue only, of the resolution document, carrying three small edits. One scope note appended to P-INDEP. Registration of four record types and one interaction. No action on the P-AUTH or ACP texts.

---

11. Open questions

11.1 Aggregation. Clause 6. The largest unresolved item in this package. Candidate directions: reciprocity as a condition of readability; binding readability to physical proximity through keys derived from the channel state, so that a distant collector receives ciphertext and a recorded tag becomes unreadable as the channel decorrelates. The second turns a lifetime enforced by a timer into a lifetime enforced by physics, which by the criterion of clause 5 is the stronger construction. Neither is specified here.

11.2 Enforcement of publication limits without a coordinator. Publishers must collectively respect a limit on a shared volume with no party counting.

11.3 Calibration. Numerical values for density thresholds, ceilings, overlap fractions and publication limits do not exist. The protocol for obtaining them is in the companion specification.

11.4 Permanently sparse areas. Declaration under R12 makes the limitation visible but does not remove it. This bears directly on *connecting the unconnected*, which Recommendation ITU-R M.2160-0 states as an overarching design principle applicable to all usage scenarios, requiring universal and affordable access independent of location. An architecture whose higher agent classes are unavailable below a density threshold does not satisfy that principle in sparse deployment, and saying so is a condition of proposing it honestly.

11.5 Availability conditions for other scenarios. The reasoning of R12 is not specific to this framework. Reliability and latency targets in the hyper-reliable and low-latency usage scenario are stated as performance figures; where the service depends on a distributed topology, a performance figure without a declared density condition is not a specification. Whether that generalisation belongs in this activity or elsewhere is for the group to decide.

11.6 Connection density is not participating-node density. The massive-communication usage scenario targets very high connection density, largely of devices that do not relay or witness. A deployment can meet those targets and remain below the percolation threshold of clause 2.2. The two quantities share a word and measure different things, and the framework should distinguish them.

---

12. Conclusion

The four contributions of this series specify a quorum of trust roots that cannot be reached by a single compromise. Two of the carriers that make that quorum affordable live outside the device, in the neighbourhood, and are available only where a neighbourhood exists. Connectivity in such a neighbourhood is a phase transition rather than a gradient, so their availability is not a matter of degree.

The condition can be met without new entities. A device worth owning alone creates the density its own security model needs, and reciprocal exchange of what each device can measure and no other can supply justifies making participation the shipped state. Both mechanisms exist in deployed standards.

Two things are added that the earlier drafts of this contribution did not carry. Density has a ceiling as well as a floor, because the geometry that carries the link also erodes the margin by which a person reads their own body better than the infrastructure does. And the guarantees of this framework are not all of one kind: some can be demonstrated by anyone, and some rest on a certifier's word, and the difference should be published with each requirement rather than left for a reader to work out.

Trust stays in the roots. This document adds that the roots have to be there, that there is such a thing as too many of them, and that a reader is entitled to know which promises can be checked.

Invitation. This document is submitted for technical review. The authors invite criticism of structural weaknesses in preference to implementation detail, and in particular of the three items in clause 11.1 to 11.3, on which the rest depends. A principle that cannot survive attack should not be standardised.

References

A. Contributions and articles of this project

The documents in this section are contributions to this Industry Connections activity and articles of the accompanying series. Contributions are held by IEEE SA and available to activity participants; articles are published by the authors. Neither category has a stable public URL of the kind given for external sources in section B, and none is cited here for a fact that an external source could supply.

[1] IEEE SA Industry Connections Activity IC25-009-01, *A Technical Reference Architecture Framework for an Open 6G Device Ecosystem*, ICAID v1.0, approved 3 December 2025.

[2] *Presence Protocol: A Principle of Authentication Without Stored Secrets for the Open 6G Ecosystem* (P-AUTH-1 to P-AUTH-3), contribution to IEEE IC25-009-01, April 2026.

[3] *Accountability Chain Protocol (ACP): A Framework for Verifiable Subjecthood in the Open 6G Device Ecosystem*, contribution to IEEE IC25-009-01, v0.9, April 2026.

[4] *The Independence-of-Foundations Principle (P-INDEP)*, contribution to IEEE IC25-009-01, v0.9, June 2026.

[5] *Resolution of the P-INDEP Open Questions and the P-DELEG Principle*, contribution to IEEE IC25-009-01, v0.91, July 2026.

[6] *Bounded Observation: A Privacy Specification for Environment-Observation Tags*, companion specification to this contribution, v2.0, July 2026, including its annex on the calibration of R15.

[7] *The First Node: How a Network With No Owner Actually Begins*, Part Seven of the accompanying series, July 2026.

[8] *A Network With No Owner, a Reflection With One*, Part Eight of the accompanying series, July 2026. Source of the density-to-privacy-margin exchange rate in clause 3.3 and of the demonstrable-versus-attested question answered in clause 5.

B. External sources

All links checked in July 2026. Where a document is sold rather than published, the link is to the official record.

[9] P. Balister, B. Bollobas, M. Walters, "Continuum Percolation with Steps in the Square or the Disc," *Random Structures and Algorithms* 26(4), 2005, pp. 392-403. DOI 10.1002/rsa.20064. Author copy, open: http://web0.msci.memphis.edu/~pbalistr/papers/contperc.pdf. Model due to E.

N. Gilbert, "Random Plane Networks," *J. Soc. Indust. Appl. Math.* 9(4), 1961, pp. 533-543, DOI 10.1137/0109045 (sold).

[10] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing* 1(1), 2004, pp. 11-33. DOI 10.1109/TDSC.2004.2 (sold). Author copy, open, at the University of Maryland institutional repository: http://drum.lib.umd.edu/bitstream/1903/6459/1/TR_2004-47.pdf.

[11] "Root of trust: survey, taxonomy, and open challenges," *Telecommunication Systems*, 2026. DOI 10.1007/s11235-025-01398-5, https://link.springer.com/article/10.1007/s11235-025-01398-5. Cited in clause 2.1 for the absence of availability from the evaluated security goals.

[12] A. Sarkar, M. Haenggi, "Percolation in the Secrecy Graph," https://arxiv.org/abs/1107.4613; R. Vaze, "Super Critical and Sub Critical Regimes of Percolation with Secure Communication," https://arxiv.org/abs/1104.1075. Adjacent work on minimum node density for connected secrecy.

[13] IEEE Std 802.11bf-2025, Amendment 4 to IEEE Std 802.11: Enhancements for Wireless LAN Sensing, published 26 September 2025. Working group record: https://www.ieee802.org/11/. Free through the IEEE GET programme.

[14] Recommendation ITU-R M.2160-0 (11/2023), *Framework and overall objectives of the future development of IMT for 2030 and beyond*, approved by the ITU Radiocommunication Assembly, Dubai, November 2023. Free: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I!!PDF-E.pdf. Source of the six usage scenarios and of the four overarching aspects cited in clause 11.4.

[15] 3GPP TR 38.901, official record: https://www.3gpp.org/dynareport/38901.htm. Release 19 ISAC channel-modelling study initiated December 2023, modelling specification finalised May 2025. Scope covering all six sensing modes, and the Release 20 position on gNB monostatic sensing, as cited in clause 9.3.

[16] J. Todt, F. Morsbach, T. Strufe, "BFId: Identity Inference Attacks Utilizing Beamforming Feedback Information," *Proc. ACM CCS 2025*, Taipei, October 2025. DOI 10.1145/3719027.3765062. Open access: https://publikationen.bibliothek.kit.edu/1000185756.

[17] ETSI TS 103 324 V2.1.1 (2023-06), *Collective Perception Service; Release 2*, free: https://www.etsi.org/deliver/etsi_ts/103300_103399/103324/02.01.01_60/ts_103324v020101p.pdf. SAE J3224_202208, *V2X Sensor-Sharing for Cooperative and Automated Driving*, August 2022, DOI 10.4271/J3224_202208, official record: https://www.sae.org/standards/j3224_202208-v2x-sensor-sharing-cooperative-automated-driving (sold).

[18] M. R. Ansari, J.-P. Monteuuis, J. Petit, C. Chen, "V2X Misbehavior and Collective Perception Service: Considerations for Standardization," IEEE CSCN 2021. DOI 10.1109/CSCN53733.2021.9686156, preprint: https://arxiv.org/abs/2112.02184. Source of the perception-area plausibility rule adopted in P-OBS-2.

[19] ETSI TR 103 460 V2.1.1 (2020-10), *Pre-standardization study on Misbehaviour Detection; Release 2*, free: https://www.etsi.org/deliver/etsi_tr/103400_103499/103460/02.01.01_60/tr_103460v020101p.pdf; and ETSI TS 103 759 V2.2.1 (2026-01), *Misbehaviour Reporting service;*

Release 2, free: https://www.etsi.org/deliver/etsi_ts/103700_103799/103759/02.02.01_60/ts_103759v020201p.pdf. Neither specifies detectors for collective perception messages.

[20] Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, Judgment of the Court (Fourth Chamber), 11 December 2014, ECLI:EU:C:2014:2428. Full text in English at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62013CJ0212. Party names appear in the original Czech in the official English-language record; the respondent is the Czech data protection authority. Cited in P-OBS-3 for the narrow reading of the household exemption: the Court held that video surveillance covering, even partially, a public space and thereby directed outwards from the private setting of the person processing the data cannot be regarded as an activity that is purely personal or household in character.

[21] *A Confidential Computing Transparency Framework for a Comprehensive Trust Chain*, 2024, https://arxiv.org/abs/2409.03720. Source of the observation acknowledged in clause 5 that attestation does not establish the absence of a capability.

[22] *ISAC Privacy: Challenges and Solutions for 6G*, https://arxiv.org/abs/2605.28325; A. Sedrati, *Unconsented Sensing: A Sociotechnical Governance Framework for 6G ISAC*, https://arxiv.org/abs/2605.07328; *Seeing Without Being Seen: A Review of Ethical and Human-Centric ISAC in 6G*, Telecom 7(3), 2026, DOI 10.3390/telecom7030052. Governance literature on sensing of non-participants, acknowledged in clause 2.1 of the companion specification.