Body of European Regulators for Electronic Communications (BEREC)
BEREC Office
For the attention of the Wireless Network Evolution Working Group
By email: PC_MobileAPI@distro.berec.europa.eu

Zigmārs Ancveirs
Independent technology and cybersecurity professional
Latvia

23 August 2026

Interoperable anti-fraud network API profile for Europe

Common semantics, privacy-preserving assertions and interfaces to national anti-fraud systems

Submission status: Public contribution; no confidentiality requested
Capacity: Independent stakeholder; personal capacity
Validation: Sources and legal status checked 23 August 2026
Scope: Direct response to BEREC Questions 1 and 4-9; explicit non-answers to Q2-Q3

1. Executive position

BEREC should treat anti-fraud network APIs as a priority interoperability use case for the European network API ecosystem. The goal should not be a central EU fraud database. The goal should be a portable interoperability profile that allows operators, aggregators, developers and competent national systems to exchange narrowly scoped network assertions using common semantics, clear provenance, freshness and correction mechanisms, while minimising exposure of protected communications and traffic data.

The timing is appropriate. BEREC's Call records that, at publication, 38 CAMARA APIs were listed as mature, 30 were in earlier development and 228 operator-supported API deployments existed in Europe. BEREC also identifies authentication and anti-fraud services, including KYC and SIM Swap, as network API use cases. [1] The policy question is therefore not whether network APIs exist, but whether European implementations will be interoperable and portable enough for developers, service providers and end users.

This contribution does not ask BEREC to standardise fraud law, create a cross-sector enforcement database or prescribe one national architecture. It proposes a narrower role: help ensure that anti-fraud network capabilities can be consumed across networks through portable technical, semantic and operational conventions, while legal powers remain where Union and national law place them.

2. Response to BEREC's nine questions

The contribution is deliberately selective. It answers the questions for which a technology/cybersecurity interoperability proposal can add evidence, and it does not manufacture market forecasts or pricing evidence.

BEREC question	Contribution
Q1 - Ecosystem roles	Answered. Section 3 defines roles and responsibility boundaries for MNO/MVNO/MVNE, aggregators/channel providers, network vendors, CPaaS/cloud, developers, NRAs/competent authorities, national anti-fraud systems and end users.
Q2 - Market demand/projections	No independent market-demand forecast is submitted in this contribution.
Q3 - Business/pricing models	No independent pricing-model evidence is submitted; the proposal does not depend on a particular commercial model.

BEREC question	Contribution
Q4 - Dynamic EU market	Answered. Common semantics and portable implementation reduce repeated provider-specific integration and semantic mapping.
Q5 - Adoption acceleration	Answered. Predictable onboarding, common semantics, reference sandbox, conformance testing, stable versioning and portability reduce adoption friction.
Q6 - Adoption drivers	Answered. Anti-fraud is a high-value, measurable, cross-border use case that can reuse existing Open Gateway/CAMARA capabilities.
Q7 - Technical/commercial challenges	Answered. Section 5 lists onboarding, authentication/consent, availability, semantic/version drift, lock-in, multi-country complexity, freshness/revocation, liability/redress and commercial-condition uncertainty.
Q8 - Regulatory challenges	Answered. Section 7 separates protected-data processing, minimised assertions and advisory API output from statutory enforcement powers.
Q9 - Actual interoperability	Answered. Section 4 distinguishes schema/API interoperability from authentication/consent, onboarding, semantics, availability, commercial portability and operational behaviour.

3. Ecosystem roles (Q1)

Responsibility should follow who controls or directly observes the underlying fact. An aggregation layer can simplify discovery, routing and contracting, but it should not become an authoritative source merely because it relays an assertion.

Actor	Proposed role
MNO / network provider	Authoritative provider for network facts it directly controls or observes; resolve protected context locally; expose only authorised, minimised assertions; maintain freshness and correction.
MVNO / MVNE	Expose or consume capabilities according to actual technical control and contractual responsibility; avoid responsibility gaps where the underlying network fact originates elsewhere.
Aggregator / channel provider	Discovery, routing and commercial aggregation; preserve issuer/provenance and common semantics; not automatically the authoritative source of the underlying network fact.
Network vendor	Implement network capability and telemetry interfaces consistently across equipment; avoid vendor-specific behaviour that breaks operator-to-operator portability.
CPaaS / cloud provider	Integration and delivery layer; may package APIs for developers but should preserve semantics, source identity, freshness and correction status.
Developer / service provider	Consume portable assertions, combine them with application-side evidence, preserve reason codes/unknown states and apply proportionate user-facing actions.
NRA / competent authority	Set or supervise national telecom/numbering rules within legal competence; support cross-border interoperability, transparency and conformance without turning developer APIs into enforcement powers.
National anti-fraud / communication-identity system	External authorised consumer/producer of minimised assertions where law permits; federate existing authoritative sources rather than centralising all raw operator data.
End user	Protected party and beneficiary; should receive understandable warnings where relevant and have transparency/correction/redress pathways for materially adverse false positives.

4. What "interoperability" should mean (Q9)

CAMARA/Open Gateway standardisation is a strong foundation, but a common API schema does not by itself prove end-to-end interoperability. Current Open Gateway documentation states that specific authorisation flows are agreed during onboarding, taking account of the declared purpose and local legal framework; GSMA technical guidance separately covers catalogue, onboarding, ordering, routing, consent and aggregation. [9][10][11] For BEREC purposes, interoperability should therefore be assessed across several layers:

Interoperability layer	What should be portable or explicit
Schema / API surface	Common endpoints, payload shapes, error conventions and versioning.
Authentication / authorisation / consent	Equivalent security outcomes and predictable flows; local-law differences are explicit rather than hidden.
Onboarding / discovery / routing	A developer or aggregator can discover capability availability and onboard without bespoke undocumented processes for every operator.
Semantics	The same status/reason means the same thing across providers; UNKNOWN, NOT_AVAILABLE and negative results remain distinct.
Availability / market coverage	Capability presence, supported parameters and geographic/operator coverage are machine-discoverable and not assumed from schema compliance.
Operational behaviour	Freshness, revocation, retries, timeouts, caching and failure modes are predictable enough for cross-provider applications.
Commercial portability	Changing operator/aggregator does not force a redesign of core application semantics even if prices/contracts differ.

Accordingly, "CAMARA-compliant" should not be treated as automatically synonymous with complete operational or commercial interoperability. The objective is not identical national implementation; it is predictable portability where differences remain necessary.

5. Technical and commercial adoption barriers (Q7)

BEREC itself identifies historical proprietary-interface fragmentation as a barrier to scalable services. GSMA likewise describes operator-by-operator integration as commercially impractical at scale because separate negotiation, integration and maintenance are required. [1][9] For anti-fraud APIs, the following barriers are especially relevant:

- operator-by-operator onboarding, contracting and application vetting;
- different authentication, authorisation and consent flows driven by implementation and local-law requirements;
- uneven API availability, optional parameters and market/operator coverage;
- semantic and version differences even when the transport/API style is similar;
- aggregator or operator lock-in where changing provider requires remapping decision semantics;
- multi-country discovery, routing, contracting and compliance complexity;
- inconsistent freshness, caching, expiry, correction and revocation behaviour;
- false-positive liability, user transparency, complaint handling and rapid redress;
- uncertainty about access criteria and commercial conditions, without assuming one preferred pricing model.

6. PROPOSAL - anti-fraud assertion profile

The following profile elements are design proposals, not claims that all listed capabilities already exist as CAMARA/Open Gateway standards. Existing capabilities should be reused where mature; the proposed profile adds portable anti-fraud semantics around and between them. Exact enum names are illustrative and should be validated through standards/conformance work.

Capability/status	Illustrative portable output	Boundary
[PROPOSAL] CLI / origin consistency	CONSISTENT / INCONSISTENT / NOT_AVAILABLE + reason code + observation time	Operator resolves signalling/interconnection context; do not expose unnecessary raw traffic/location data.
[PROPOSAL] DNO / protected-number policy	POLICY_MATCH / NO_POLICY_MATCH / NOT_AVAILABLE + issuer + validity	Represents a policy/registry fact, not a conclusion that the number owner is fraudulent.
[PROPOSAL] SMS Sender ID authorisation	AUTHORISED / UNAUTHORISED / UNKNOWN + policy reference where publishable	Separates authorised organisational sender identity from message-content analysis.
[PROPOSAL] Roaming/origin consistency	CONSISTENT / INCONSISTENT / NOT_AVAILABLE + reason code	Can reuse national/operator roaming signals where lawful; avoid exposing unnecessary location.
[REUSE EXISTING] Device/account capabilities	Use existing CAMARA/Open Gateway semantics for Number Verification, SIM	Do not duplicate mature APIs; compose them into fraud-prevention workflows.

Capability/status	Illustrative portable output	Boundary
	Swap, Device Roaming Status, Call Forwarding Signal and related APIs	
[PROPOSAL] Fraud assessment	ADVISORY SIGNAL / ASSESSMENT + reason codes + evidence class	Technically distinct from a binding legal/regulatory action.
[PROPOSAL] Freshness / correction	observation time + expiry/freshness + supersedes/revokes where applicable	Required for cached/federated assertions and false-positive correction.

7. Legal and privacy boundary (Q8)

The proposed profile should be designed around data minimisation, not around exporting raw operator telemetry. Article 5 of the ePrivacy Directive protects communications and related traffic data, while Article 6 regulates traffic-data processing. Article 6(5) expressly refers to fraud detection among functions for which traffic data may be processed by persons acting under the authority of communications providers, but it does not create a general cross-sector right to disclose raw traffic data. [5] GDPR Articles 5 and 6 separately require purpose limitation, data minimisation and an applicable legal basis where personal data are processed. [6]

A useful default is therefore local resolve: the operator evaluates protected network context internally and returns only the purpose-specific assertion required by the authorised API consumer. A fraud-prevention service may need to know that a presented CLI is inconsistent with network origin/roaming context; it does not necessarily need the underlying location or signalling records.

Technical output should also remain distinct from legal effect. Article 97(2) of the European Electronic Communications Code provides for competent authorities to be able to require blocking, on a case-by-case basis, where justified by fraud or misuse. [4] That statutory power is conceptually different from a developer API returning an advisory risk signal. A portable profile should preserve that distinction and support transparent reason codes and rapid correction/redress where a false positive materially affects a user or service.

8. Latvia and the Baltic region as a pilot context

The proposal is grounded in an existing regulatory trajectory. BEREC's 2025 workshop report records the Latvian regulator (SPRK) considering a decentralised anti-fraud API, initially voluntary and potentially mandatory for transit operators, aimed at verifying call-origin legitimacy. The report also states that Latvia was trialling a solution used in Lithuania and Estonia, with cross-border potential, and that broader market participation beyond telecommunications would become increasingly important as fraud shifts towards messaging and OTT services. [3]

Latvian law already provides concrete building blocks. Section 64 of the Electronic Communications Law regulates numbering fraud and requires providers to stop call routing/access when numbering fraud or misuse is detected; Section 66 establishes the Numbering Database as a state information system. Section 98(8^1), in force in 2026, requires an electronic communications provider receiving a call via interconnection from a foreign operator, for the purpose of preventing fraud or other unlawful activity, to process terminal location data and to process, receive and pass to other electronic communications providers information on whether the terminal is roaming. [7] These provisions do not themselves create the proposed developer API, but they provide an existing lawful national anti-fraud signal-sharing context that can be reused rather than duplicated.

Latvia's Ministry of Transport has separately identified further anti-fraud policy directions, including spoofing, malicious links, SIM-box issues and alphanumeric SMS sender identifiers. [8] Those policy items should be distinguished from the binding legal provisions above and assessed on their own legal status.

Comparable national experience supports early interoperability work. Lithuania reported more than 13.8 million spoofed foreign calls and 2.12 million fraudulent SMS blocked in Q1 2026. [13] Finland made SMS sender-ID authorisation mandatory from 4 May 2026 and is phasing in related technical procedures. [12] Ireland has implemented DNO, protected-number and CLI-blocking interventions and continues to develop network-level protections. [14] These examples

demonstrate the value of common concepts but also the risk of incompatible national technical islands.

9. Minimum interoperability and portability requirements

- common schema and versioning conventions aligned with OpenAPI and existing CAMARA security/interoperability profiles where appropriate;
- a common reason-code registry rather than opaque provider-specific fraud scores;
- machine-verifiable provenance: issuer/source class, ruleset/policy version, observation time and freshness/expiry; cryptographic integrity where assertions are cached, relayed or federated;
- portable error and unknown-state semantics - unsupported capability, temporary unavailability and negative result must remain distinct;
- conformance tests and a reference sandbox covering semantics and operational behaviour, not only HTTP syntax;
- published, proportionate and non-discriminatory onboarding criteria appropriate to the sensitivity of the API;
- explicit switching/aggregator portability so that a provider change does not require remapping every fraud decision;
- service-class-specific performance objectives for live lookup, event/webhook and bulk/delta feeds rather than one universal latency target;
- fast revocation/supersession propagation for cached assertions and documented user/partner correction paths.

10. Suggested BEREC outputs

- Develop, or convene stakeholders to develop, a reference interoperability profile for anti-fraud network APIs that complements GSMA Open Gateway/CAMARA.
- Define common semantic principles separating network facts/assertions, advisory risk assessments and binding legal/regulatory actions.
- Establish conformance criteria and a reference test suite covering semantics, freshness/revocation, unknown states and operational behaviour.
- Provide guidance on developer portability, aggregator/channel-provider roles, capability discovery and predictable onboarding.
- Promote a standard interface pattern by which authorised national anti-fraud or communication-identity systems can consume minimised network assertions without centralising raw telecom data.
- Encourage a cross-border pilot involving willing NRAs/operators, with the Baltic region as one plausible environment alongside other Member State practices.
- Coordinate relevant privacy and cybersecurity aspects with competent data-protection authorities and ENISA while keeping sector-specific legal powers outside the developer API.

11. Pilot acceptance criteria

- same test case produces semantically equivalent results across participating operators/aggregators;
- unknown/unavailable data never silently maps to a positive safety result;
- false-positive corrections and revocations propagate within a defined service-specific window;
- developers can switch provider/aggregator without rewriting core decision semantics;
- raw traffic/location data are not exposed where a minimised assertion is sufficient;
- API output cannot be confused with a statutory blocking/enforcement order;
- audit evidence can reconstruct issuer, ruleset/version, observation time and decision path;
- performance targets are defined by service class rather than one universal latency number.

12. Scope limits and conclusion

This contribution is deliberately not a proposal for BEREC to create or operate a pan-European police, banking, platform-enforcement or raw-telecommunications-data database. National cross-sector anti-fraud systems may interface with network APIs where law permits, but sector-specific powers, controller responsibilities, retention rules and enforcement decisions remain with the competent actors.

The central recommendation is narrower and actionable: Europe should not stop at common API syntax. For anti-fraud use cases, portability also requires common meaning, provenance, freshness, correction, onboarding and legal-effect boundaries. BEREC is well placed to bring NRAs and market participants together around those interoperability questions while the European network API ecosystem is still developing.

References

[1] BEREC - Call for Inputs on interfaces for mobile networks for developers and third-party services (2 July 2026; deadline 26 August 2026). - Source

[2] BEREC - Wireless Network Evolution Working Group, work item on mobile-network interfaces / 2026 work. - Source

[3] BEREC BoR (25) 129 - Summary Report on practical issues preventing number misuse and possible fraudulent activities (2 October 2025). - Source

[4] Directive (EU) 2018/1972 establishing the European Electronic Communications Code, Article 97(2). - Source

[5] Directive 2002/58/EC (ePrivacy), Articles 5 and 6, including Article 6(5). - Source

[6] Regulation (EU) 2016/679 (GDPR), Articles 5 and 6. - Source

[7] Latvia - Elektronisko sakaru likums, Sections 64, 66 and 98(8^1). - Source

[8] Latvia - Ministry of Transport, anti-telephone-fraud working-group directions (12 January 2026). - Source

[9] GSMA - Understanding Network APIs (10 July 2026), including fragmentation and standardisation discussion. - Source

[10] GSMA OPG.10 - Open Gateway Technical Realisation Guidelines (22 February 2026). - Source

[11] GSMA Open Gateway / CAMARA API documentation - authorisation and onboarding depend on purpose and local legal framework. - Source

[12] Traficom - SMS sender-ID authorisation requirements effective 4 May 2026. - Source

[13] Lithuania RRT - 13.8 million fraudulent/spoofed calls and 2.12 million SMS blocked in Q1 2026. - Source

[14] Ireland ComReg - anti-scam call/text interventions and network-level protections (2025 update). - Source

Sources and legal status last checked: 23 August 2026. Proposed EU legislation is not relied on as a current legal basis.