Response to BEREC Call for Inputs on interfaces for mobile networks for developers and third-party services

Respondent

Polish industry association: The Polish Chamber of Information Technology and Telecommunications (Polska Izba Informatyki i Telekomunikacji)

Contact: biuro@piit.org.pl

Executive Summary

The Polish Chamber of Information Technology and Telecommunications welcomes BEREC's initiative to collect market feedback regarding the development of network APIs and the broader ecosystem surrounding initiatives such as GSMA Open Gateway and CAMARA.

The Chamber supports the development of standardised, privacy-preserving and commercially scalable Network APIs as an important enabler of innovation, digital security and new digital services. We believe that standardized network APIs can contribute significantly to innovation, fraud prevention, digital identity services, customer onboarding and the broader development of the European digital economy. At the same time, achieving large-scale adoption requires continued efforts regarding interoperability, commercial scalability, regulatory certainty and ecosystem-wide cooperation among telecommunications operators and vertical industries.

The Chamber considers that any intervention regarding pricing mechanisms or mandatory access models would be premature at the current stage of market development, as such measures could undermine investment incentives, innovation and the emergence of sustainable business models. This is particularly important for the Polish market, where network APIs solutions are currently in the early phases of development and market deployment, and where sufficient flexibility is needed to support innovation, investment and the establishment of sustainable business models.

The Chamber encourages regulators to provide greater legal clarity regarding the use of privacy - preserving data for anti-fraud purposes. In particular, further guidance is needed where sector-specific confidentiality obligations, such as telecommunications secrecy or banking secrecy, may limit the ability to share or validate information. This issue is particularly important for the Polish market suffering from intensive cyberattacks and frauds. It is important to point out that in not enough clear regulatory environment authorities can adopt also a highly cautious approach to the interpretation and application of privacy-related rules, including the ePrivacy and the GDPR, sometimes going beyond the explicit requirements of the legislation. As a result, legal uncertainty may hinder the deployment of Network API-based solutions designed to combat fraud while maintaining high standards of privacy and personal data protection. Providing clear, consistent, and proportionate regulatory guidance would facilitate the development of effective anti-fraud services, while ensuring compliance with applicable confidentiality, privacy, and data protection requirements. Furthermore, a consistent interpretation and application of the ePrivacy and GDPR across the European Union is essential to ensure regulatory certainty, a level playing field, and equal opportunities for service providers to develop and offer Network API-based services throughout the Single Market.

Below, the Chamber presents its views and observations in response to the questions included in BEREC's Call for Inputs.

How does the ecosystem work?

1. **What roles has each player in this complex ecosystem: MNOs, MVNOs, MVNEs, Aggregators, network vendors, CPaaS providers, Channel providers, Developers, cloud providers, end users, etc.?**

The Network API ecosystem relies on a diverse set of stakeholders whose roles are complementary and collectively contribute to the development, adoption and scaling of interoperable digital services. Clear allocation of responsibilities is essential to ensure innovation and security.

- Mobile Network Operators (MNOs) play a central role as they are responsible for ensuring service quality, security, privacy and the integrity of the network data processed and provided through Network APIs.
- Mobile Virtual Network Operators (MVNOs) & Mobile Virtual Network Enablers (MVNEs) may, depending on the characteristics and structure of the market, extend the reach of Network API-enabled services to additional customer segments.
- Aggregators and CPaaS providers help reduce market fragmentation by offering a single commercial and technical interface across multiple operators. They simplify integration support onboarding and enable access through a single implementation.
- Application developers, system integrators, identity providers and other specialized service providers incorporate Network APIs into customer solutions and business processes.
- Standards bodies and industry initiatives (such as CAMARA and GSMA Open Gateway) play a crucial role in developing common API specifications, implementation guidelines and interoperability frameworks. Their work is essential to ensuring that Network APIs can scale across operators, countries and use cases.
- Regulators and public authorities play an important enabling role within the Network API ecosystem as they should provide legal certainty, promote consistent interpretations of applicable regulatory frameworks and ensure non-discriminatory market conditions across EU. In particular, regulators should facilitate clarity regarding ePrivacy requirements and data protection rules, especially where Network APIs are used for fraud prevention, authentication and identity-related services. This role is particularly important in markets where regulatory interpretations of ePrivacy and GDPR may affect the deployment of privacy-preserving Network API use cases, creating uncertainty for operators and service providers seeking to develop innovative anti-fraud and digital identity solution.

End users can be considered from two complementary perspectives.

- Business customers of Network API services, such as banks, financial institutions and enterprises from various sectors, are key users of Network API-enabled capabilities. Given the growing interest from businesses across multiple industries, Network APIs should be enabled and promoted as tools that support fraud prevention, risk management and the enhancement of security in digital services. By leveraging trusted network-derived signals, enterprises can strengthen authentication processes, improve risk assessments and reduce exposure to increasingly sophisticated fraud schemes. In the future this group of customers will be able to use new Network APIs (e.g. Quality on Demand) to differentiate their offerings for their end customers e.g. gaming, communications apps could enhance service level by steering network functions and allocating bandwidth in real time.
- End users of Network APi business customers (including consumers and business users) are the ultimate beneficiaries of Network API-based solutions. In sectors exposed to fraud, identity theft

and account takeover attacks, service providers can use privacy-preserving information obtained through Network APIs to improve security risk assessments and implement more effective fraud prevention measures. This can help enhance user protection and increase trust in digital services while maintaining a high level of privacy and data protection. In the future Nework APIs like QoD or Edge Discovery could be used for their own SIM cards for video reporting or some Industry 4.0 use cases (e.g. self-driving cars, drones, Augmented Reality or Robotics).

How will the market be developed?

2. **Can you provide any publicly available information on (current/future) market demand analysis, market prediction/projection and market development?**

The Chamber is not in a position to provide detailed market data regarding the development of the Network API market. Nevertheless, based on ongoing discussions with stakeholders and observed market developments in Poland, there is growing interest in Network API solutions across multiple sectors, including financial services, e-commerce, digital platforms. This interest is driven by the need to strengthen security, improve customer experience and address increasingly sophisticated fraud scenarios.

It should be noted that demand is unlikely to develop uniformly across all Network API categories. Different sectors and use cases are expected to prioritise different API capabilities depending on their operational needs and regulatory environment. In the near term, fraud prevention APIs are likely to be the primary demand drivers, as they provide tangible and immediate benefits in combating account takeover fraud, social engineering attacks and other forms of digital crime. APIs supporting number verification, call forwarding, SIM and device swap, scam signal and identity assurance are therefore expected to attract particular attention from businesses seeking to strengthen security while maintaining a seamless user experience.

3. **Can you provide any publicly available information on business models and successful pricing models?**

The Chamber is not in a position to provide detailed information on business or pricing models, as the market for Network API services in Poland remains at an early stage of development therefore it is too early to identify one generally successful pricing model. Different APIs create different types of value and may therefore require different commercial models.

Today the most dominant pricing scheme is transaction-based model. There are some expectations coming mainly from global aggregators about volume-based or even subscription-based pricing models which may be appropriate where APIs are used repeatedly but they are on very early stage and still need to reach some maturity. For future network programmability services such as Quality on Demand may require models linked to sessions, duration or service characteristics.

An important factor is commercial simplicity. Customers operating across several networks should, where possible, be able to obtain broad coverage through simple aggregated offers instead of negotiating and integrating separately with every operator.

At this stage, commercial experimentation should be encouraged. Transparency and predictable commercial conditions are desirable, but mandatory uniform pricing or ex-ante price regulation would be premature and could reduce incentives to invest and experiment in a market that has not yet reached maturity.

4. **In what way can Open APIs enable or support a dynamic and well-functioning European market of both application service developers and providers as well as telecom service providers?**

Open and standardised APIs can substantially reduce the cost and complexity of developing applications that use mobile network capabilities. Developers should increasingly be able to build against a common API specification rather than creating different integrations for individual operators.

CAMARA has been established specifically to develop consistent and developer-friendly telecom APIs across operators and geographies, while GSMA Open Gateway provides the broader framework for their exposure and commercial implementation.

This can support a European market in which providers compete on service quality, coverage, customer experience, commercial conditions and innovation rather than on proprietary API interfaces.

However, technical API specifications alone are not sufficient. Practical interoperability also requires compatible authentication and consent approaches, stable versions, consistent responses and error handling, testing environments, transparent coverage and efficient commercial onboarding.

BEREC can support this development by encouraging common standards and interoperability while avoiding the creation of a single mandatory technical or commercial architecture.

5. **How can the adoption of network APIs be accelerated?**

The most important step is to make a smaller number of high-value APIs genuinely easy to use in production and which are demanded on the market.

Operators and other ecosystem participants should provide reliable documentation, realistic testing environments, clear information on network coverage and API versions, predictable onboarding processes and appropriate operational support. An API should be considered commercially available only when the complete end-to-end service can be used reliably, not merely when the technical interface has been implemented.

Commercial and legal onboarding should also become simpler and more standardized. Common API information, common legal bases guidance, reusable contractual documentation and efficient processes for moving from testing to production would help reduce implementation time and ease of use by aggregators and service providers.

Finally, adoption should be driven by concrete use cases with measurable customer benefits. Cooperation with banks, digital service providers, identity providers, fraud-prevention platforms and other relevant sectors can help demonstrate practical value.

The adoption of Network APIs can be accelerated by providing greater legal certainty, regulatory consistency and a supportive innovation framework across the European Union. Clear and harmonised rules governing the use of network-derived data for legitimate purposes such as fraud prevention, authentication and digital identity would reduce barriers to investment and facilitate the deployment of Network API-based services at scale.

A key prerequisite is ensuring a coherent interpretation of the relationship between GDPR, ePrivacy rules, telecommunications secrecy obligations, cybersecurity requirements and sector-specific regulations. Legal uncertainty regarding the conditions for processing, sharing or verifying telecommunications-related data may discourage market participants from developing and adopting innovative solutions, even where such solutions are designed to enhance security and consumer protection.

The legal framework governing the use of Network APIs should be applied consistently across sectors, without imposing additional obligations on telecommunications operators that do not apply to other market participants processing comparable data for similar purposes. Consequently, there is no need for sector-specific provisions in the ePrivacy framework, provided that equivalent privacy, security, and accountability requirements are ensured under GDPR rules.

6. **What are the main drivers for the successful adoption of Open APIs in Europe?**

The successful implementation of open APIs in Europe will be determined by several interlocking regulatory, technical, security, economic, and cooperation elements between implementing and using open APIs.

A coherent European regulatory framework. Legal certainty is important, which can be achieved through the application of a uniform legal basis for the implementation of open APIs. Important confirmation by national data protection regulators, the electronic communications market. It is essential to comply with the General Data Protection Regulation (GDPR) and with sector-specific regulations. Attention should also be paid to national rules. Some of them may need to be amended to obtain a clear legal basis for sharing data under open APIs. Regulatory openness to the use of Network API services by stakeholders across different sectors, enabling innovative and secure digital services.

Stakeholder Collaboration. Effective implementation requires collaboration between stakeholders. It is also very important for the smooth functioning of the API to clearly define the roles and responsibilities of all participants of the API ecosystem, including network operators, developers and service providers.

Economic value. There must be clear economic value for providers and users of APIs, which may include new business models, increased efficiency or access to new markets.

What are the main challenges?

7. **What are the main technical and commercial challenges, from the perspective of MNOs, MVNOs, MVNEs, Aggregators, network vendors, CPaaS providers, Channel providers, Developers, cloud providers, end users, etc.?**

From the perspective of the telecommunications sector, the main challenge is not the standardisation of the API interface itself, but turning a standardised interface into a scalable, interoperable, secure and legally robust commercial product.

In the context of mobile network APIs, these challenges are particularly relevant for MNOs and for entities directly cooperating with them in the provision of such APIs, including MVNOs, MVNEs, aggregators and business customers. Regulatory uncertainty can directly affect technical architecture, onboarding requirements, contractual arrangements, liability allocation and ultimately the investment case for commercial deployment.

MNOs

CAMARA successfully standardises the external API interface, but the internal implementation behind that interface may differ between operators. MNOs use different network architectures, underlying technology stacks, data sources and IT environments. Consequently, implementation effort and the way in which data is collected and processed to produce the same CAMARA response may differ.

Interoperability is handled by cooperation between CAMARA, GSMA Open Gateway and TM Forum, and it is too early to say what challenges MNOs might face in the future. Potentially challenges might go beyond compliance with the same OpenAPI specification. Operators may differ in data availability and freshness, response times, error handling, operational limits and treatment of edge cases but it remains to be seen to which extend, they affect final product and its commercial relevance. Lifecycle management is another consideration, as operators are unlikely to migrate to new API versions simultaneously.

Commercially, expected demand and achievable revenues remain uncertain, while many implementation, security, compliance, onboarding and operational costs are largely fixed. This may create an unfavourable

risk/reward balance, particularly where potential regulatory or contractual exposure is significant compared with the expected revenues from an individual API product.

MVNOs and MVNEs

For MVNOs, technical capabilities depend strongly on the deployment model. A light MVNO may not have direct access to network information necessary to provide a particular API, while a full MVNO may control some relevant systems and data but still remain dependent on its host MNO for other elements.

Depending on the specific service and processing activity, the MVNO and host MNO may also have different regulatory and data protection responsibilities. Implementation may therefore require both technical integration and a clear allocation of responsibilities between the parties.

Similar challenges apply to MVNEs, potentially across multiple partners operating under different technical and contractual models.

Aggregators

Aggregators, including CPaaS and channel providers, can play an important role in achieving commercial scale by providing access to multiple operators and markets through a single integration.

However, multi-operator and cross-border scalability remains challenging. Even where operators expose the same CAMARA API, differences may exist in availability, supported versions, operational parameters, commercial conditions and regulatory requirements. Aggregators may also require mechanisms to identify the relevant operator for a particular subscriber, taking into account number portability and MVNO arrangements.

Another important issue is the contractual chain. MNOs typically do not have a direct contractual relationship with downstream API customers. Appropriate contractual assurances and controls are therefore required regarding downstream use of the APIs. This increases contractual complexity and may require back-to-back obligations, audit mechanisms and appropriate allocation of commercial risk, without necessarily changing the statutory responsibilities of the respective parties.

Business customers

Business customers may operate in sectors subject to additional regulatory requirements, for example financial services. Consequently, an API implementation suitable for one use case or sector may require additional controls in another.

Commercially, customers also need predictable multi-operator coverage and pricing. Significant differences between operators in API availability, commercial models or technical behaviour can reduce the benefits of standardisation and make it more difficult to build services that can be deployed consistently across markets.

Regulatory uncertainty as a technical and commercial challenge

For APIs involving personal data or information protected by electronic communications confidentiality rules, regulatory uncertainty can become a significant obstacle to commercial deployment.

A legal basis under the GDPR may not by itself resolve all requirements where sector-specific electronic communications rules impose additional restrictions. Interpretation and practical application may also differ between Member States. Consequently, the same CAMARA API and use case may face materially different deployment conditions across national markets.

This uncertainty has direct technical and commercial consequences. It affects which data may be exposed, what authorisation or consent mechanisms are required, for how long certain information may be retained, what evidence must be recorded and which party must perform particular compliance checks. It also increases the duration and cost of legal, compliance and security assessments.

CAMARA is increasingly addressing the technical side of consent management through standardised purpose handling, authorisation flows and consent-related mechanisms. However, a technical consent mechanism does not itself determine whether consent is legally required or sufficient in a particular jurisdiction, which party is responsible for determining the legal basis, or how responsibilities should be allocated across the API value chain.

Conclusion

Standardising the API interface is necessary but not sufficient. The main challenge is to create conditions in which standardised network APIs can become scalable commercial products across multiple operators and markets.

This requires not only common API specifications, but also sufficient interoperability of operational implementations, predictable multi-operator reach, workable commercial and liability models, and greater regulatory certainty regarding the processing of network and subscriber-related information.

Without greater convergence in these areas, network APIs may remain technically available but commercially difficult to scale. This may result in uneven availability across Europe and, particularly in the case of fraud-prevention and security-related APIs, may limit the development of services that could improve end-user security.

8. **Do you see any regulatory challenges, for instance, with regard to enabling certain APIs or an evolution towards a well-functioning market?**

Yes. In the Chamber's view, a key regulatory challenge is ensuring consistent legal conditions across the European Union for the processing and use of data for specific purposes, including supporting businesses in their efforts to combat fraud through the provision of information necessary for their risk assessment processes.

A well-functioning Network API ecosystem requires legal certainty regarding the interaction between data protection rules, ePrivacy requirements, telecommunications secrecy obligations, cybersecurity requirements and sector-specific regulations. This is particularly important for use cases related to fraud prevention, authentication and digital identity, where the processing of network-derived data may raise questions concerning purpose limitation, necessity, data minimisation and the allocation of responsibilities among the parties involved.

The Chamber considers that regulatory frameworks should clearly distinguish between access to underlying network data and the provision of privacy-preserving API outputs, such as risk assessments or validation responses. The use of privacy-enhancing technologies, strict purpose limitation and auditable access mechanisms can significantly reduce privacy risks while enabling valuable anti-fraud and security-related services. In some cases, uncertainty regarding the legal basis for sharing, verification or use of specific data may limit the deployment of solutions designed to combat fraud and enhance consumer protection.

This issue is particularly important for the Polish market, where the competent authorities have traditionally adopted a cautious approach to the interpretation and application of privacy-related rules, including the ePrivacy and the GDPR. As a result, legal uncertainty may discourage investment and slow the deployment of privacy-preserving Network API solutions, despite their potential to strengthen digital security and support fraud prevention efforts. In the Chamber's view, greater consistency in the interpretation and application of ePrivacy and GDPR rules across the European Union would contribute to regulatory certainty, facilitate the development of cross-border services and ensure a more level playing field within the Single Market.

At the same time, regulatory intervention should remain proportionate and technology-neutral. The Chamber does not support the premature regulation of pricing models or the imposition of mandatory access obligations while interoperability frameworks and business models are still evolving.

A key objective of regulatory policy should be to enable the use of commercial Network API solutions offered by telecommunications operators across the EU as a trusted tool supporting businesses in fraud prevention and risk management. Such solutions should be available to organisations across different sectors, as many face similar security threats and could benefit from mechanisms relying on the verification of telecommunications-related data. The standards established within the Network API ecosystem already incorporate robust safeguards regarding access to, sharing and use of information, ensuring that data processing remains proportionate and privacy-preserving. This enables the achievement of public policy and regulatory objectives without favouring any particular sector, thereby maintaining a sector-neutral framework for the deployment of anti-fraud solutions.

1. **To what extent are the current APIs truly interoperable across operators with network equipment from different vendors in Europe? Are there differences in interoperability between certain application sectors or other aspects?**

At this early stage of Network API market development, we are not aware of material interoperability issues across European operators or network equipment vendors. Interoperability is already a core focus of the relevant industry bodies, including CAMARA, GSMA Open Gateway and TM Forum, which are actively developing and aligning common technical and operational specifications. We therefore see no evidence that any regulatory intervention or alternative interoperability standards are needed. Taking into account the continuous development of the CAMARA API, we believe that premature regulation could hinder innovation and progress. Instead, we recommend considering only commercial activities to foster the growth and maturation of this initiative. This approach would allow for the natural evolution of interoperability standards while providing a supportive regulatory approach for development.