24 April 2024

TELEFÓNICA contribution to the draft BEREC report on the entry of large content and application providers into the markets for electronic communications network and services

1. Introductory comments.

BERECs report comes at a critical time where the market for digital infrastructure is undergoing massive changes and the dynamic and interaction in the internet ecosystem is developing with high speed. Furthermore, one could think that **this report comes late considering that these changes in the internet ecosystem started more than a decade ago and have already had severe consequences for the European connectivity sector.**

As the report correctly stated, the ECN/ECS markets are becoming more dynamic and players from other markets are entering them, leveraging their positions in adjacent markets and bargaining power. Nevertheless, the report does not provide clear solutions to the challenges described and, in some cases, it minimized the challenges identified using, in our view, some erroneous presumptions.

The risk to affect the open internet is huge. Big CAPs act independently of its competitors in the internet ecosystem through concentration, controlling more and more the open internet. CAPs only invest in transport & interconnection, not in the expensive delivery networks including access networks. They have been able to monetize their services and traffic while telcos have been delivering service to CAPs, without being paid for the service delivered to CAP.

As mentioned, ECN/ECS are very dynamic, and competition is not only between traditional telco operators anymore but with other digital players that are playing an increasingly relevant role in the market. This should imply **technology neutrality, a level playing field, meaning amongst others, a fair use of the internet ecosystem, market analysis/definition and framework definitions, and a revision of the traditional obligations in the ECN/ECS area**. Telefonica understands that BERECs upcoming IP-IC interconnection report will also contribute importantly to a comprehensive analysis of internet ecosystem considering the technological shifts and the significance of large CAPs own infrastructure.

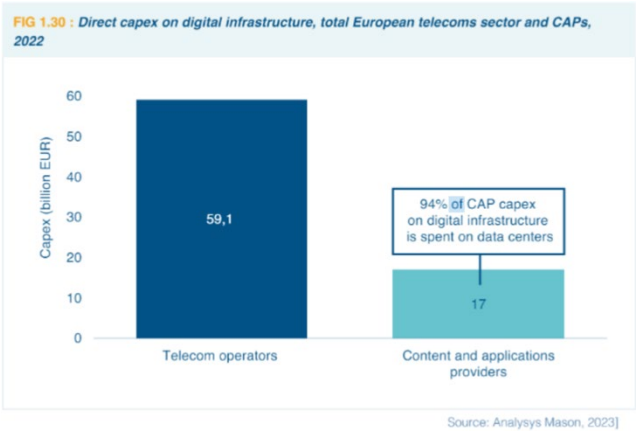
While BEREC rightly assesses the individual impact of CAPs entering in specific layers / services of the Internet value chain, recognizing factual and potential market failures, BEREC does not consider the global jointly impact of CAPs becoming vertically integrated, gaining market power across the whole Internet value chain further leveraging into adjacent untapped markets and gaining market and bargaining power versus ECN and ECS providers.

Below we have provided some general and detailed comments that we believe are important aspects to consider by BEREC, to correctly identify the size of the challenges the European telco industry faces**. In our view it is not necessary to elaborate additional reports on the challenges identified as there are enough evidence of the failures in the internet ecosystem due to the entry of large content and application providers into the markets for electronic communications network. The time for solutions is now.**

2. Overview of large CAPs investments.

Although, CAPs are increasing their investments, their direct capex on digital infrastructure is well behind of the European telco sector.

An illustration provided by Analysys Mason is helpful in placing the high numbers of CAP investments in perspective.



Moreover, in page 34 is stated "Large CAPs have traditionally provided services on the client and server sides of the internet ecosystem. However, in recent years, they have increasingly invested in network infrastructure and provides services related to ECN and ECS or qualifying as such." In our view, **the CAPs only invest in transport & interconnection, not in the expensive delivery network, including access networks.**

In addition, CAP investments in infrastructure are mentioned mixing markets. More emphasis should be placed on separating the amount of investment in each layer. "CAPs investment in transport infrastructure has grown", but Figure 2 clearly shows that most of the investment is in **data hosting** with very little investment in transport infrastructure and negligible investment in access networks (which is the core of the investment need to deliver content and services to end user). For e.g "In 2022, according to the European Commission's 2022 EU Industrial R&D Investments scoreboard, seven of the largest CAPs25 invested 70,5 billion euros (CAPEX) on infrastructure worldwide (data centers, CDNs, submarine cables, terrestrial and satellite networks) mainly to support the delivery of their own services and bringing content closer to end-users."

3. Dynamics between large CAPs and ECS/ECN operators .

BEREC has correctly identified the different types of dependencies (e.g., complementarity, competition and cooperation) between CAPs and ECNs. However, the following points should be considered.

Telefonica wants to highlight, that CAPs enjoy scale and higher returns on investments as **their main business have been unregulated, while telco operators' traditional business has been subject to a very high level of regulatory scrutiny, with a clear focus on reduction of prices** by fostering artificial competition, reduction of economies of scale and lower return on investment being able to have captured most of the value created in the Internet ecosystem. **They have been able to monetize their services and traffic while telcos have been delivering service to CAPs, without being paid for the service delivered to CAPs.**

Furthermore, t**he basic philosophy of CAPs is to occupy the complete value chain, as they are not interested in sharing their business with partners, due to their huge scales compared to national network operators**. This raised concerns on leveraging practices and highly asymmetrical bargaining power for the detriment of competition.

Large CAPs increasingly insource what was formerly purchased from traditional ECS/ECN providers; a development reflected in CAPs increasing annual investments in infrastructure. This could be explained as they do free riding on the delivery networks, including access networks.

In fact, **several of the markets where large CAP have invested are increasingly concentrated** e.g. the market for cloud services where the three biggest players in Europe accounted for 72% in Europe in 2023 in a market that is expected to grow significantly driven by VHCN, cloudification and virtualization of networks. The market for voice assistants, the market for CDN and sub marine cables supporting the CAPs own businesses, online advertisement, private relay services are other examples of markets with high concentration.

Large CAPs proprietary caches within ISP networks, their global backbone infrastructure connecting their data centers and their proprietary content and application ecosystems are thus **providing them with more control over their content delivery and strengthen their market position vis-à-vis ECS/ECN providers**. As a matter of fact, **large CAPs have already built not only proprietary content and application (OTT) ecosystems but are also aiming for "private" Internet.**

In view hereof, it is vital that the regulatory framework in place from time to time does not unreasonably restrict or advantage any of the players who are part of the same digital ecosystem. The potential to innovate is therefore much higher at network borders than within the networks which is an unproportioned and structural disadvantage for IASP. The upcoming review of the regulatory framework does indeed provide an opportunity to adapt the framework to ensure that collection of all relevant data can be collected, and the ecosystem properly assessed by competent authorities.

Secondly, it is important to consider the two-sidedness between CAPs on the one side and ECNs on the other side. It is correct, that services are **complements** in some areas. However, we do not fully agree with the statement "Since no online content and applications could be consumed without connectivity, and no connectivity would be required without any online content and applications, there is an interdependence between CAPs and ECS/ECN operators." (p. 16). It is correct, that "no online content and applications could be consumed without connectivity" as CAPs "have not yet invested in

access networks in the EU" (p. 9). However, there are still services which would make connectivity necessary if large Caps 'services were not as widespread.

In relation with **cooperation**, in page 1 is mentioned that: "We can also see examples of projects where CAPS and ECS/ECN have been cooperating". This is kind of misleading because such technical cooperations arrives when the network operators assume the investment for this kind of cooperation.

Finally, Telefonica believes there are more issues that deserve more attention in the report:

• The regulatory imbalances between CAPs and ECS/ECN providers e.g. CDN providers ability to control the user experience on top of the internet connectivity and the relationship with the Open Internet Regulation.

• The imbalance in negotiation power between CAPs and ECS/ECN providers e.g. the CAPs ability of CDNs to direct traffic in ISPs networks.

Taking into account all of the above, Telefonica believes that it is not enough what the report concludes "This report highlights several issues which can raise some challenges in the context of ECS/ECN regulation, and which could be further investigated by BEREC in the future". It is our view that BEREC, once identified challenges and market failures should draw less ambigous conclusions, leading to a proposal to address those challenges. Continuing with never ending analysis will only increase the size of the problems until it becomes too late for market repair.

4. CASE STUDY 1: content delivery networks.

The origin of CDNs dates to the late 1990s, designed to avoid bottlenecks of internet traffic and improve the user experience. Over time, CDNs have evolved from static delivery mechanism to sophisticated platforms that can handle dynamic content, video streaming etc. Another important development is the emergence of proprietary CDNs by vertically integrated CAPs.

The CDNs capability to bringing high quality content to end-users is indisputable and underlined by the fact that in 2023 CDNs delivered more than 70% of all internet traffic worldwide and the demand is only expected to increase.

Regarding business models, as noted by BEREC, there have been a significant shift in the CDN market in recent years. **All major CAPs now operate their own CDNs (vertical integration)** and place little reliance on the offerings of commercial CDN providers. An important aspect of the increasing concentration of proprietary CDNs is the implications on the competitive landscape vis a vis smaller commercial CDNs (public CDNs in BEREC terms) as well as smaller CAPs. The number of commercial CDNs has decreased over the last years with fewer players offering CDNs to third parties. This has a direct effect on the options of smaller CAPs that may face higher input costs. Also, smaller CAPs may be disadvantaged in delivering content to end users as a result of the crowding out of specialised commercial CDNs making them more dependent on large CAPs (vertically integrated CDNs). This is a development that it should be monitored closely as it might

result in **foreclosure effects by large CAPs such as self-preferencing to decrease competition.**

Private CDNs and cache servers are increasingly in control of the customer experience.

Proprietary CDNs deployed by a non-ISP allow enhanced customer experience exclusively for the traffic delivered through that CDN, providing a competitive advantage over other content. CDN providers like Akamai can differentiate the prices and quality they offer to content providers. They can also apply traffic management techniques such as load balancing and prioritisation of traffic (e.g. in favour of live streaming) when delivering traffic.

On the contrary, rigid traffic management constraints together with restrictions on internet access services limit the possibilities of ISPs to develop competing commercial solutions. This is an important imbalance in the regulatory framework which directly effects the competitive outcome and the telecoms business ability to flourish and which could lead to disintermediation of operators by digital gatekeepers and CAPs, who can provide the differentiation in services, without concern for the principles in the Open internet regulation.

It is not the IASPs who are acting as a bottleneck. The challenge to the open internet rather stems from certain CAPs (Hyperscalers), **who are able to control** e.g. which slice covers a certain application. CAPs thus act as gate-keeper on a i) **traffic level** by using proprietary CDNs to allow for QoE, ii) **service level** by allowing only certain apps in app-stores, iii) **device level** by providing certain services only on certain devices and iv) **content level** by interfering with unwanted content rated dangerous or simply false.

Equal rights and obligations for IASP and CAPs alike in the internet space are thus an essential aspect to consider.

Increasing the imbalance in bargaining power.

The CDN landscape as described above also contribute to increasing the imbalance in bargaining power between ECS/ECN providers and large CAPs. **Large CAPs have a superior bargaining power over ISPs when it comes to negotiating over fees for IP data transport** which has resulted in the imbalanced ecosystem we see today. This superior bargaining power of large CAPs stems from several factors:

First, the OIR establishes the principle of Network Neutrality. Based hereon, ISPs are, in effect, subject to a "**must carry" obligation** of all traffic based on certain rules that are to some extend commercially and technically restricting operators from reaching optimum IP solutions.

Second, **large CAPs have become indispensable for ISPs,** as they provide the content and applications that end users expect from any internet service and that play a key role in their everyday lives due to their strong network effects **which result in a dominant position**. ISPs cannot afford to deny or degrade access to large CAPs' services, as they

would face strong legal and customer reactions: ISPs are prevented by law from discriminating between types of CAPs for commercial reasons, and if an ISP denied its customers access to Netflix or Facebook, it is more likely that its customers would switch to another ISP than that they use another content. Thus, those players can make use of their dominant position in their core revenue generating markets.

Third, **large CAPs are less dependent on large ISPs, as they have alternative options (routes) to reach their end users** via other networks, such as commercial CDNs, cloud operators, or other carriers. **These networks are interconnected to the ISPs' networks through existing peering and transit agreements,** which enable the free flow of traffic between different networks in line with the OIR. Therefore, large CAPs do not need to obtain direct connectivity from a particular ISP to access its customers even if for the detriment of CAPs' customers; in fact, CAPs have adopted traffic routing decision detrimental to their customers with the purpose to pressure network operators as publicly responsible worsened customers' experiences. A vertically integrated ISP is not able to withhold access to its infrastructure, as it applies the principle of network neutrality and must deliver any traffic that enters its network to end users on a non-discriminatory basis. As a result, even without a direct commercial agreement with a carrier, a CAP is still able to reach its end users via indirect connections and/or CDNs and/or cloud operators.

Fourth, large CAPs have a significant quality lever over ISPs, as **they can influence the quality of service and network stability of ISPs by their own routing decisions**. Large CAPs, which send particularly large volumes of data, can congest specific interconnection points by spontaneously re-routing a portion of their traffic via indirect connections to the ISP's network, thereby affecting the quality of service for all online services routed via the affected interconnects. This can induce a quality-adjusted price increase for end users on the ISP's network, which would deteriorate the ISP's competitive position if the CAP leaves connections to other ISPs unaffected.

Fifth, end users tend to hold ISPs responsible for any quality problems, even if caused by the CAP, and are more likely to switch their ISP than to stop using the CAP's services in case of persistent connection issues. Large CAPs can impact the quality of services of a network carrier with an integrated ISP business towards its end customers, which is a central dimension of competition at retail level, and evidence shows that in case of any connection problem, **end users react negatively towards their ISP and not the CAP**. This effect is exacerbated by the fact that certain CAPs display to internet users ISPs ranking according to the quality level of the provision of their own service(s) with respect to CAPs' chosen criterion, effectively steering end-users to their preferred ISP.

In this sense, Telefonica supports the EC suggested approach to this imbalance situation recognized in its White Paper. **We believe, BEREC could include the same proposal into its Report:** "*subject to careful assessment, policy measures could be envisaged to ensure swift resolution of disputes. For example,* ***the commercial negotiations and agreements could possibly be further facilitated by providing for a specific timeline and by considering the possibility for requests for dispute resolution mechanisms, in case***

***commercial agreements could not be found within a reasonable period of time**. In such case, NRAs or (in cases with a cross-border dimension) BEREC could be solicited, as they have the necessary technical knowledge, and important experience in dispute resolution and in assessing market functioning"*.

The benefits of CDNs for ECN operators are not significant.

As pointed out by BEREC, ISPs may be interconnected with CDN providers via peering agreements, or ISPs may host CDN servers in their networks. BEREC suggest that ISP hosting CDN services may also be motivated by reduced capacity costs (peering interconnection, backbone and backhaul links; see p. 29).

While CDNs may have a positive impact on improving the quality of content to the end users, the view of GSMA and ETNO's members are that their impact on capacity cost and thus network investment requirement for delivering the traffic from CAPs is, however only limited.

The cost savings resulting from CDNs and on-net CDNs (i.e. cost saving related to international transport and operators' national backbone) are not significant when compared to the total and traffic related networks costs, considering that CDN investment has very limited bearing on the volume of traffic on the access network.

To note is that BEREC, itself, assessed the cost drivers of fixed and mobile network and concluded in its preliminary position on the internet ecosystem that the cost of increasing IP interconnection links capacity and backbone capacity can be considered very low, in particular when compared to the cost of building access networks.

Further, CAPs normally provide and maintain the cache servers (on-net CDNs) but **operators have to bear the set-up costs and operational costs, further limiting eventual benefits**. **For mobile networks the use of on-net CDNs is even less viable** as the international transport cost saving is relatively lower when compared to total network costs, as access network bears highest share and CDNs do not reduce bandwidth requirements for mobile access networks since cache servers must be located upstream where mobile traffic is aggregated.

Additionally, having CAPs minimized and limited their traffic delivery cost by building their own cable infrastructure and deploying on-net CDNs, they have entered into a never ending race to provide highest quality content (from SD to HD, 4K …, increasing volume of prefetched of content,…) irrespective of efficiency as if end users can fully enjoy such enhanced quality on their devices. As CAPs do not pay for the service provided by network operators to transport their traffic through delivery and access networks, they have no incentive to deliver the traffic efficiently. The result is network operators having to cope with such inefficient traffic growth devoting relevant investment resources to upgrade network capacity limiting their flexibility to invest into innovative services and network technological and coverage upgrades.

Finally, with regards to what BEREC states in page 23: "This duality, in which some CDN providers act as applications on top of the internet, while others have their own

infrastructure and therefore do not need to acquire connectivity from an ISP, was highlighted in a previous BEREC Report "An assessment of IP interconnection in the context of Net Neutrality", **we would like to highlight that connectivity does not only mean the "interconnect" but also includes the connectivity to the end-user**. Thus, "do not need to acquire connectivity from an ISP" does not provide the full picture.

5. CASE STUDY 2: submarine cables

BEREC has correctly highlighted that "the international submarine cable connectivity market has witnessed significant changes, particularly with the involvement of large CAPs" (p. 31). However, there are two points we would like to highlight.

First, it would be important to dig deeper into the reasons for the deployment of own submarine cables, as there might also be some additional incentives in addition to the better control of the provision of services in terms of improvement of quality. This can be especially seen once looking into investments in submarine cables. Despite ample capacity at peak supply, large CAPs continue to invest heavily in subsea cables notably on the routes connecting Europe with the US. CAPs benefit from deep pockets, facilitating strategic investments in critical infrastructure without the need for an adequate return. Given that cheap trans-Atlantic capacity is generally available this means that the intention of large CAPs can only be to **acquire "control" over the Internet**. In fact, Google, Meta and other large CAPs are quietly buying up the most important part of the Internet. Historically, subsea-cables were owned by various groups of private companies — mostly regulated telecom providers. That's beginning to change. 2016 saw the start of a massive submarine cable boom, and this time, the buyers are content providers — corporations like Google, Meta, Amazon and Microsoft. Amazon and Microsoft part-own one and four networks, respectively. By routing traffic through their own infrastructures, large CAPs can bypass the public Internet, thereby strategically reducing or eliminating their reliance on best-effort Internet. The increasing circumvention of the traditional Internet architecture of Tier-1 and Tier-2 networks is referred to as "Internet flattening". These unregulated infrastructure investments are the reason **why the formerly decentralized architecture of the Internet became increasingly centralized towards a few large CAPs and represent a significant change compared to the original aim of the open Internet to globally connect all users for the benefit of society at large.**

Second, as correctly stated "Large CAPs predominantly use the capacity on the submarine cables for their own internal needs, particularly for interconnecting their data centers" (p. 33). Therefore, those investments mostly do not provide any additional competitive or resilience component as BEREC correctly states: "In this context, while large CAPs deploy submarine cables primary for their own use, traditional **ECS/ECN providers still play a key role on the transmission of data for other CAPs, connecting areas which may not be economically profitable.** Moreover, by primarily interconnecting their data centers and regional PoPs to data centers, **large CAPs' investments have limited impact on the global network resilience." (p. 54)**

As ECS providers are forced into routes which are "not economically profitable" there is a further imbalance between CAPs and ECNs. **It, furthermore, makes Europe more reliant on the large CAPs, thus decreasing sovereignty.**

Finally, Telefonica wants to highlight that in the case of submarine cables, **BEREC does not appear to include investments made by operators or other infrastructure players** (which are in turn invested in by operators) **and seems to consider only CAP agent investments**; many operators have sold their investments to infrastructure companies (in which they may still hold investments and pay for services). This is the case for Telxius. In fact, some of the submarine cables are included as examples are not only invested by CAP agents.

6. CASE STUDY 3: internet relay services

Internet encryption is not new, and most of the internet traffic is encrypted. This is a trend that has been going on for some years. What has changed with the emergence of "privacy proxy relays" is that **network operators can no longer see the destination IP address or data nor the DNS query**. As a result, the network operator has lost its means to inspect, filter and block traffic routed via the relays, having shifted that capability to the provider of the Internet Relay service on exclusivity basis . The protection of privacy and personal data is an important and recognized objective. However, private relay solutions tend to go beyond what is necessary and lead to a number of undesirable effects in areas that are also important and worthy of protection.

As a result of respective encryption and the masking of IP-Addresses, the affected traffic will no longer be identifiable, even to providers of Internet access services. This has not only a negative impact on the established business models of these providers, but also leads to restrictions on competition and innovation and a further undesirable concentration of traffic on the Internet in the hands of a few powerful Internet companies. Above all, it also **jeopardizes the security and resilience of communication networks and the efficient routing of traffic (even more in the edge). Overall, this further undermines the desired European sovereignty in digitalization.**

Concerning the nature of the services, **BEREC seems to consider Internet Relay Services as a kind of VPN**. **This is debatable because there is no notion of network or management in connectivity. In other words, there is no management of the service, but simply encryption of content** between two ends (browser and relay, or between relays). Furthermore:

- There is no ability to influence routing, quality of service, or SLA management.
- Transmission is not between networks (or multiple sites) in the first segment (users to relay#1), but between users and content providers, leading to a centralization of connectivity services. Linking it to VPN concepts is a misguided association of ideas because content providers do not create or take responsibility for the management of that connection. Nor do they assume any obligation in terms of securing SLAs.
- The Internet relay service is oriented towards mass service, while the telco VPN has a concept of limited use within the client organizations (or their own), with the guarantee that the data remains within the scope of each of them.

- A similar situation (with no visibility) also exists with VPN networks. However, unlike private relay proxy solutions, VPN service operators do have visibility of source IP address, traditional DNS queries (if used) and HTTPS SNI headers.

Telco networks are prepared and configured so that each customer's traffic leaves the Internet through the most optimal peering point according to their location to provide them with the best possible latency and QoE. With the activation of the relays, the traffic of these clients becomes dependent on the logic of the relays in terms of the destination where this traffic is delivered, which does not have to be the most optimal. It also means adding two more hops to the destination possibly making the content have to travel farther, and an additional double level of encryption. In short, it can alter the topological efficiency of the network and worsen the end user's perception of quality for reasons beyond the operator's control.

This is especially serious if coupled with edge strategies, because a user could have a service deployed at the edge to allow for an optimal connection, and yet this user traffic could be suffering "Tromboning" by having to reach other previous destinations (relay locations), which would increase the latency of the connection. **It is regrettable that the wide range of innovative services enabled by ultra-low latency 5G and FTTH networks deployed by telecom operators will be limited by the decision of CAPs to deploy Relays negatively impacting latency.**

For the reasons mentioned above, we disagree with this BEREC statement: "*in principle, VPN or internet relay services do not make it more difficult to use and control the network efficiently, since the data traffic would be concentrated towards the VPN/relay service providers, and all traffic originally transported to different destinations and interconnection points now can be transported to the interconnection towards the VPN/relay service provider*".

As well, Telefonica disagrees with the following statement in BEREC´s Report: "*Internet relay services are made possible by innovative transport protocols such as QUIC and represent a contribution to increasing data security and privacy*". We think it gives an additional level of privacy, but not security: there are already mechanisms that offer security, such as TLS/HTTPS (even more so with initiatives such as TLS 1.3 or SNI encryption). This is focused on not being able to see anything at all, but not on preventing identity theft etc.

Finally, in our opinion, this statement is not right: "*However, lawful interception is still possible, where internet access providers are able to intercept communications data. This data can be provided to the authorities only in encrypted form, as opposed to clear text. This encrypted format provided to authorities is not just the case for internet relay services or VPNs, but is the norm generally, due to a trend towards higher demands in relation to the citizens' privacy and the increasing use of encryption on different layers and in more and more applications*". It is true that internet service providers can continue to do ILT, another thing is that it is useful to the LEA (Law Enforcement Agency). But:

- Currently, the usual use involves a single level of encryption when using HTTPS to access a website, and the user is more easily identifiable because the operator can

give them the identity behind each IP, now what the operator gives them will be traffic whose destination is relay #1.
- They won't even have the way to ask the owner of relay #1 to ILT that person's traffic, because they won't be able to give them any information about the traffic that belongs to that person, relay #1 doesn't have that information.
- Of course, relay #2 has even less information about the client, although it could provide the "decrypted" content (i.e. once the double encryption of the relays has been removed) or inform the destination, it could not know which specific flows it has to supply.
- An additional problem is that relays 1 and 2 may not be national/European companies and obtaining the certificates can be complex.
- The problem doesn't just affect LI, it also affects the "IPAR"/Data Retention (record of who had an IP in use at any given time for a time of X years). Law enforcement will not be able to ask relay #2 which person used a particular IP address at any given time XX/YY/20ZZ.

About the areas of competition, we want to comment that on the last paragraph of section 3 of the report, about private Relay services, BEREC focus on the fact that they prevent us from advertising services. But that is not the only concern. What really prevents us, are amongst others the following services: security, child protection, sponsored services, packages per application, etc... In our view, it should be used “content-based services” instead of advertising, and list those services, some of them of regulatory origin, such as for example, protection of minors, verification of the IWF list.

Below we have highlighted issues of particular importance for network operators and encourage BEREC to further investigate the impact of relay services. The potential for impact for operators includes e.g:

- The ability to legally inspect, filter and/or block data across the network.
- The launch of Innovative services
- The ability to route traffic optimally
- Overall network resilience

Network Operators thus must consider the impact of private proxy relays on the **obligations** they have **to inspect, filter or block network traffic**. Some identified examples include:

- Providing free of charge traffic to legally mandated information or content (public domain names and websites) and low barrier customer identification thereby prohibiting operators’ ability to provide customer support.
- Requirements to block access to various domain names/IP addresses by national law (e.g. CSAM) or court orders (e.g. infringing copyright.
- The ability to offer adult content filtering services.
- Obligation to log internet activity records. Although this is technically still possible, the records will be less meaningful with incomplete records.

Network resilience is another area that may be impacted by proxies and the reliability of proxy servers. This is important to consider especially given that internet services and telecommunications are now considered critical infrastructure.

Since private relay services are currently not considered a publicly available telecommunication service**, there is no requirement of notification of the service to regulatory authorities (subject to local law).** So **far relay services would not comply with the measures under European law such as the directive on Network and Security Systems, legal interception measures and privacy legislation and identifying users accessing certain websites as requested by law enforcement authorities**. Currently competent authorities of the Member States are not able to intercept Internet traffic because of the lack of obligations on the part of the relay provider to enable lawful interception.

From the perspective of a network operator a main concern is also that the significance of private proxy relays **has the potential to develop from affecting a minor portion of traffic into potentially being the mainstream default**.

Finally, although all the disadvantages of 6.4 are correctly identified by BEREC. The following points could be added:

- Difficulty of this model to comply with regulatory standards or to ensure secure service (e.g. attack filtering).
- control of the content that you can/cannot access is loss (e.g. if you access content that you should not be able to access by law).
- The control of user traffic is concentrated in the few operating system owners, since the encrypted connection begins in the OS, outside the scope of the operators and regulators.
- It is difficult to correctly operate and plan the network and maintain an adequate user experience as it does not depend on a single agent. **The relays become a 2nd agent of the provision of internet access "de facto".**

7. Restrictions on access to services or functionalities by OS providers

As highlighted by BEREC, recent technological developments have led to a situation where OS providers increasingly are in control of access to services and functionalities.

As a matter of fact, OS providers are another group of players in the internet ecosystem that are not constrained by compliance with the current Open Internet regulation: instead, they are able to exploit it, whilst at the same time foreclosing the capability of network operators to offer differentiation-based services and business models widely adopted by CAPs or operating systems providers.

OS & slicing

Operating systems have developed so they can 'open up' end-user devices to network slices. For example, it is now possible to split the applications on a device between 'work' and 'personal' and deliver the 'work' applications over a specific slice, optimised for that content. **However, the operating systems are, for now, maintaining sole control over the designation of applications and the mapping of applications to dedicated slices**.

The provision of services over Network Slicing depends critically on the ability of operators to identify and authenticate applications that use the slices. Without this, there is no possibility of controlling access to the slices, with the restriction on innovation, commercial, security and privacy problems that this entails.

There are several technical solutions for this procedure, but the only ones that are scalable in cost and complexity and are compatible with privacy and Open Internet Regulation in Europe **require the participation of Operating System providers** (BELOW SEE an annex with additional information). Although, efforts are being made to agree on a solution to this problem, so far, the cooperation of the OSs has been limited.

- Operators require visibility of the IDs of the Apps accessing a slice.
- App IDs assignment cannot be limited to the APP Store of the OS.
- Operators shall have a mean to authenticate an App ID accessing a slice.
- Operators shall have a mean to authorize an APP ID to access a slice. This enforcement capability needs to be done in conjunction with the network and cannot be limited to the OS only.

OS & Rich Communication Services

RCS (Rich Communication Services) is a standard promulgated and developed by GSMA. It involves collaboration from mobile OS providers, device manufacturers, and network operators. Thanks to Apple’s announcement in 2023 regarding the implementation of RCS in iMessage, we remain confident that the dominant ecosystem for mobile devices (iOS and Android) will cover nearly all mobile devices starting from 2024.

With Apple’s participation in the development and implementation of the RCS standard alongside Google, the interoperability of messaging applications based on this standard is assured. Once Apple integrates RCS into iMessage, the messaging app on Android devices will naturally become interoperable with iMessage. As a result, users on these platforms (iOS+Android) will be able to communicate with each other without the need to download an additional NI-ICS application. Of course, this announcement from Apple must became a reality and authorities must monitor the effective implementation of the solution, to avoid any delays.

>>

ANNEX: OS/SLICING

Network slicing is a key 5G SA enabler that will bring new values to B2B and B2C customers and the Telco industry. Indeed, it allows the customization of connectivity and dedication of network resources and instances on per use case or customer basis.

Some operators are currently building and launching slicing capabilities in parallel to their 5G SA deployments, while others are considering such an investment. However, through initial design and product definition a set of restrictions have been observed that, unless solved, will hinder the service from thriving and reaching full scale to cover market demand, putting at risk the business case for investment.

This is because the provision of services through network slicing has a high dependency on the Operating Systems (OS) running on mobile handsets. OSs are currently the enforcement point where the routing of the traffic of the App running on the User Equipment (UE) towards available slices is decided.

Due to the importance of this process and the fundamental role that OSs play in it, we believe that it is very relevant that BEREC is made aware of the associated technical details. With this, NRAs will be in a better position to identify the current gaps and limitations that could impact the commercial viability of the service from an operator perspective. Section 2 of this document tries to provide such information. In section 3, we suggest some guidance and possible next steps to solve the identified issues.

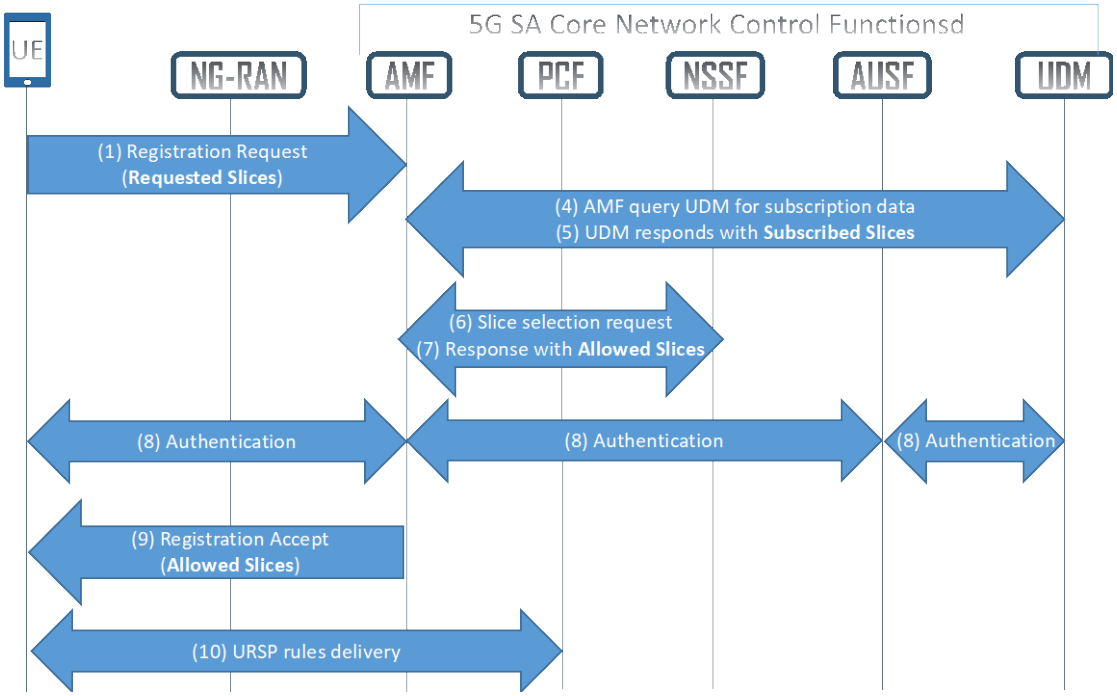
1. Slicing current limitations

1.1 Slicing E2E high level view

How the allowed network slice instances for a concrete UE are determined?

During the UE initial registration procedure in the 5G SA network, the UE is instructed with the set of network slice instances which is allowed to use. This set of allowed network slice instances for this particular UE is based on criteria such as the UE subscription information, the UE location in that moment… Then, thanks to this procedure, the UE is registered in the 5G SA network, authenticated, and authorized to use this set of allowed network slice instances.

This process is depicted in the following flow.

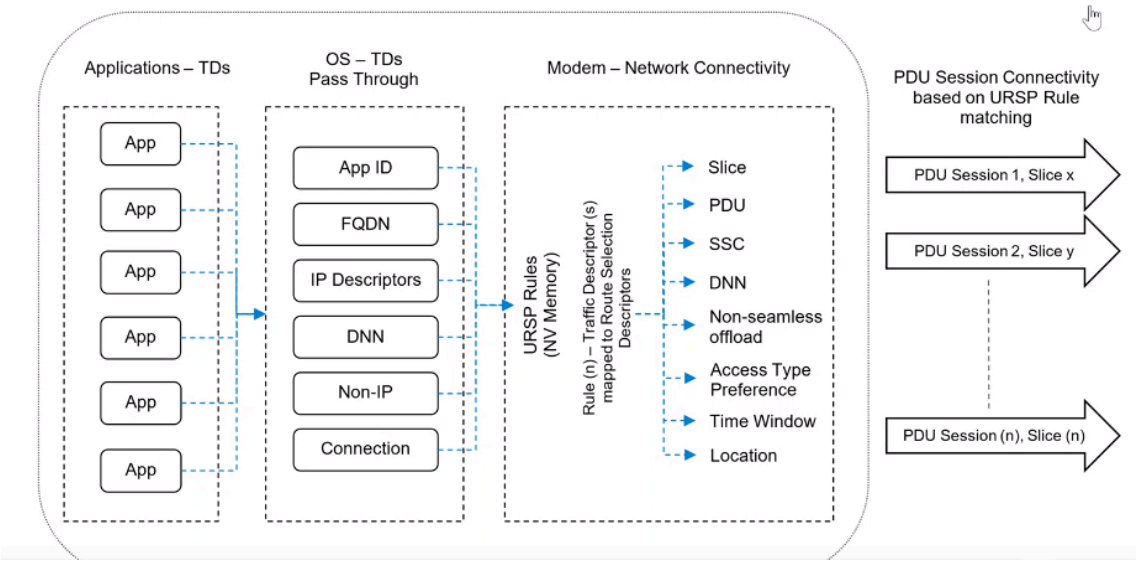


How the traffic originated in the UE is steered over the proper network slice?

As per 3GPP TS 23.501, UEs can connect up to 8 network slices simultaneously, and therefore the UE OS has to determine through which specific network slice the traffic has to be delivered. The UE Route Selection Policy (**URSP)** is a signaling capability between the network and the device composed by rules that includes information which maps the traffic flows of a client application (user data traffic) to 5G Packet Data Unit (PDU) session connectivity parameters. The URSP is used by the UE to determine if the user data traffic can be routed through an already established PDU session or there is a need to trigger the establishment of a new PDU session.

However, the way these rules are enforced in the UE is left to the OS.

URSP is delivered to the UE during the registration process in the 5G network and it is also updated in the UE when the MNO changes the URSP applying to a specific subscriber. The following picture depicts an illustration of the USRP.



A URSP rule consists of one Rule Precedence, one single Traffic Descriptor (TD) and one or more Route Selection Descriptors (RSDs).

- The TD is used by UE to evaluate whether a client application qualifies for this rule.
- The RSD is used by the UE to know which 5G PDU session connectivity parameters shall be used to route the application traffic into operator's network (among others, the network slice to be used is included here).

The URSP matching logic is usually hosted and implemented by the OS from the UE, and we refer to these devices as OS-centric devices, as are most of those currently in the market.

As can be seen, for any TD the operator wants to implement in order to build an end-to-end slicing-based service, a URSP matching logic residing in the OS is required, in the case of OS-centric devices.

2.1. Technical limitations

- App ID usage in UEs
  Currently **the OS is the sole entity deciding the routing of the application traffic towards the available slices** in the network since the URSP matching logic is implemented at OS level.

- App ID usage in USRP rules
  At this stage App IDs are mostly assigned to applications by the developers within the App store of the OS and **there are no standard mechanisms in place for MNOs to have visibility of this information to populate the USRP rule** adequately with the App ID.

- App ID authentication
  As per today **OS does not authenticate App IDs that have not been managed by the OS App store** (if an application is not installed in the device by using the App store, App ID spoofing might happen).

- App ID authorization
  At this stage **there are no mechanisms for a network or B2B customer to authorize the OS to route an App ID traffic within a slice**. The only way to do it is on OS level and thus in control of the OS provider.

2.2. Business impact

- Use cases limitations in B2B.
  Because of the limitations described in section 2.2 the operators cannot guarantee Service Level Agreement (SLA) within a slice as it could be consumed by undesired or unauthorized app. This bring important limitations in use cases where the connectivity is critical (e.g. public safety, remote maintenance in critical sites, drone, AGVs, etc.)

- Possible fraud issues.
  Due to current limitations in the level of authentication of App ID, there is a risk of fraud issues where end users could install apps spoofing the App ID to try to access non-authorized slices.

2. Possible technical approaches

3.1. Building a specific device configuration per use case

With this approach UEs would need to be capped so that they may only run the applications allowed to access the network slicing service. Such an approach would scale neither technically nor in cost, because of the following.

- It requires the usage of device management platforms from the MNO or the B2B customer, which are complex and expensive systems.
- It supposes Specialized devices per use case, instead of leveraging generic 5G handsets. Thus, end users would have to carry several devices for each different slice.
- It is not applicable to B2C scenarios.

The increase in product costs would make the business case very difficult and thus reduce network-slicing adoption in the industry.

3.2. Traffic inspection

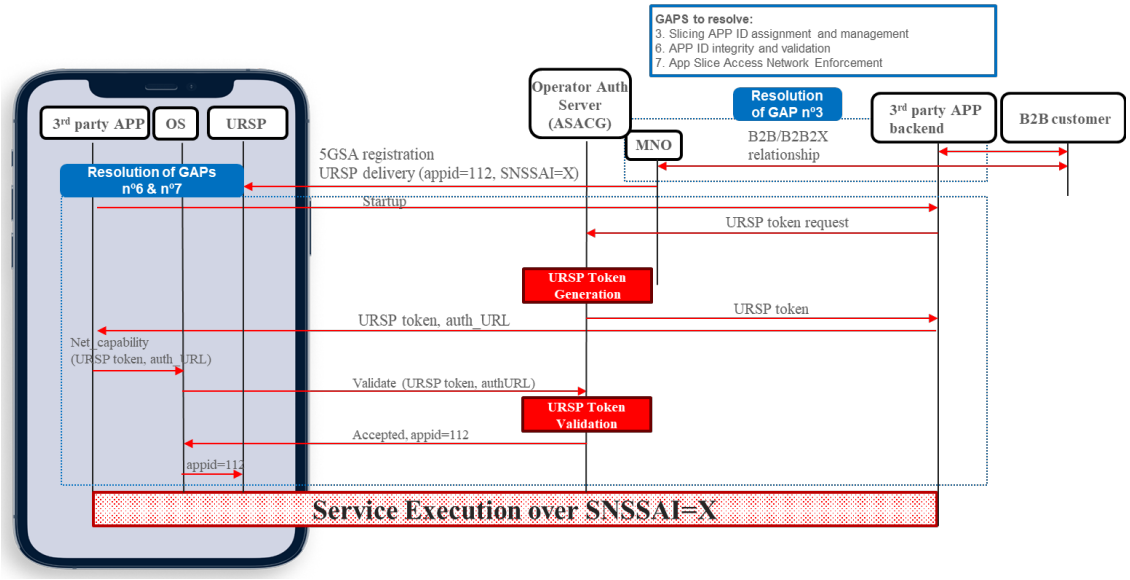
Traffic inspection (for example, Deep Packet Inspection) and enforcement could be applied in the user plane to control traffic of undesired or unauthorized app in the different slices.

However, this approach would have limitations against encrypted traffic and customer privacy. Besides, it is expensive and resource consuming, generally worsening the performance of the services. It would be very difficult to have an attractive business case with this approach, both in regulatory risk and cost terms.

3.3. Collaborative approach with developers based on token solution

A solution where MNOs could authenticate and authorize the App IDs to access a slice in collaboration with app developers could resolve the current gaps identified in this concern.

One possible solution would involve the use of a token. A token is a digital element generated by a server and delivered to a client. In this context, the token would be presented by the client to the server in successive iterations, and the server (and only the server) can validate the identity and authenticate the client. This is the principle followed in thie proposed approach. This solution could be discussed in the proper standards and adopted in the industry.



Following text explains the graphic above:

- The MNO would have a B2B/B2B2X relationship with the end customer, which is using a certain application. The 3rd party application developer would communicate its App ID to the MNO in order for the MNO to send the URSP rule properly to the customer devices (by using the App ID as TD within the URSP rule).
- The MNO generates a URSP token associated to the App ID and then delivers it to the application back-end.
- When the application starts in the device, the application back-end delivers the URSP token to the application front-end installed in the UE.
- The application front-end presents this URSP token to the OS when requesting access to the network.
- The OS validates the URSP token with the MNO, authenticating and authorizing the access for that application to the network slice. **Current versions of OS do not include this procedure, it has to be developed and implemented.**
- The service can be executed properly.

However, such approach still relies on the endorsement and correct behavior of the OS.

3. Conclusions and next steps

The following conclusions can be deduced from the technical description above.

- Operators require visibility of the IDs of the Apps accessing a slice.
- App IDs assignment cannot be limited to the APP Store of the OS.
- Operators shall have a mean to authenticate an App ID accessing a slice.

- Operators shall have a mean to authorize an APP ID to access a slice. This enforcement capability needs to be done in conjunction with the network and cannot be limited to the OS only.

As can be seen, OSs constitute a *de-facto* bottleneck in the viability of Network Slicing business case. Alternative solution not involving OSs are too costly, too intrusive and lack scale potential.

Not solving the above issues would severely limit use cases, applicability for the industry and consequently massification of the service. This erosion of business expectations would definitely put in jeopardy the considerable investments required to provide network slicing.

>>>