BEREC Guidelines on common approaches to the identification of the network termination point

21 November 2019

Consultation response

We would like to thank BEREC for inviting input to its draft Guidelines on common approaches to the identification of the network termination point in different network topologies (BoR (19) 181)[1] and would like to offer the suggestions below.

Express a preference for the NTP at location A

We consider that the current draft identifies the relevant criteria as to how to assess the consequences of particular choices of the network termination point (NTP) in various network topologies. However, in order to give effect to the purpose of Directive 2008/63/EC of facilitating user choice in telecommunications terminal equipment (TTE), BEREC should not only provide for this categorisation, but express a preference for the NTP to be located at point A as the default option. Consequently, the choice of NTP should also be periodically reviewed in order to assess whether reasons not to choose point A (or point B, in case point C was chosen) remain valid.

Placing the NTP at point A allows end-users to operate their networks with the maximum autonomy. It facilitates a large market in TTE (in particular, TTE that combines modems and routers as opposed to an NTP at point B), minimises the trust end-users need to place in IAS providers' security and data protection practices, and allows end-users to switch IAS providers with as little friction as possible. The experience of Germany, where national law stipulates an NTP at point A for fixed-line access, shows that it is possible to provide end-users with these benefits and thereby facilitate end-user choice in TTE and in operation and use of their internet access service (IAS) as stipulated by Directive 2008/63/EC and Regulation 2015/2120.

Clarify what does not constitute objective technological necessity

In the context of virtual unbundling, there may exist contractual relationships between IAS providers that make stipulations as to the type of customer-premises equipment (CPE) that may be provided by the virtually unbundled IAS provider which are meant to resolve responsibility questions arising from potentially incompatible CPE with the public network. The draft Guidelines touch on the issue of responsibility in paragraph 62.

Existing contractual relationships however are not technical by themselves, and therefore do not constitute objective technological necessity regarding the location of the NTP. We suggest that BEREC clarify this issue by adding a new paragraph 62a:

62a. (new) However, existing contractual relationships, including contractual relationships between IAS providers, shall not be considered to establish objective technological necessity by themselves.

1 https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/8821-berec-guidelines-on-common-approaches-to-the-identification-of-the-network-termination-point-in-different-network-topologies

Similarly, the draft Guidelines consider simplicity of network operation to be a factor in assessing possible locations for the NTP. IAS providers may design access products that incorporate specific, proprietary functionality on CPE. BEREC should clarify that such product design is not to be considered inherently simpler for the purposes of establishing *objective* technological necessity (rather it is the IAS provider's subjective necessity). We therefore suggest the following amendment of paragraph 84:

> 84. The NRA assessment whether there is an objective technological necessity of equipment to be part of the public network shall include the criterion 'simplicity of the operation of the public network'. **However, IAS product design incorporating proprietary functionality on customer-premises equipment should not be considered simpler in terms of objective technological necessity.**

Security and data protection

In view of the fact that Regulation 2015/2120 allows IAS providers to make use of traffic management measures to temporarily resolve security issues arising in its network, including security issues arising from insecure CPE, and that such measures should not be in place permanently, we consider that it is more appropriate to refer to measures that can be put in place to mitigate security issues, rather than measures that are (already) in place.

We therefore propose the following amendment of paragraph 105:

> 105. This assessment shall take into account in particular the following:
>
> a. The measures that ~~are~~ **can be put** in place which allow the network operators to protect their networks against security incidents caused by abuse of modem, router, media box etc.
>
> b. If these measures are sufficient, then it would not be likely that there is an objective technological necessity that the modem, router, media box etc. at the customer premises need to be part of the public network from the perspective of network security.

The draft Guidelines refer to the danger for the privacy of end-users' communications caused by an NTP in location C in paragraph 108 and makes reference to the prohibition of interception of end-users' communications by IAS providers.

However, the choice of CPE by end-users that is possible when the NTP is in locations A or B protects them to a greater extent against *unauthorised* access to the CPE, in cases where the legal prohibitions prove ineffective. BEREC should clarify the seriousness of restricting end-users' abilities when the NTP is chosen to be at point C, particularly in view of the fact that certain metadata (such as data on the acquisition of DHCP leases in the private network) cannot be protected by end-users by means such as encryption.

Additionally, when unauthorised access to the CPE is possible, this access can be abused to access further devices in the end-user's private network.

We therefore propose the addition of the following paragraph:

108a. (new) In case the NTP is at location C, by the nature of the communications protocols involved, certain metadata is exposed to the network operator through access to the CPE, such as which and how many devices are connected in the private network, and when they connect. In addition, access to the CPE can be used for further unauthorised access to devices in the private network, potentially compromising communication that the end-user has taken measures to protect, e.g. by encryption.

Sincerely,

epicenter.works