



Alliance of Telecommunications Terminal Equipment Manufacturers (VTKE)
Alt-Moabit 90a ▪ 10559 Berlin
+49 173 628 62 44 ▪ info@vtke.de

**Statement of the Alliance of Telecommunications Terminal Equipment Manufacturers (VTKE)
on the
Public consultation on the definition of the Network Termination Point (NTP)**

The Alliance of Telecommunications Terminal Equipment Manufacturers (VTKE) expressly welcomes the fact that the Hellenic Telecommunications and Post Commission (EETT) wants to define the Network Termination Point (NTP) for Greece in regulatory terms.

Over the past years, the members of the VTKE have been able to gain a wealth of experience in open and more closed markets for terminal equipment, both in Europe and beyond.

We thank you for giving us the opportunity to comment.

General remarks

VTKE expressly welcomes the fact that EETT would like to create more clarity with regard to the regulation of the NTP with the present draft regulation. We clearly advocate a definition of the NTP at point A, because only in this manner the free choice of telecommunications terminal equipment can be fully (re)established for all access technologies (DSL, cable and fibre) in Greece.

We agree with EETT that point A as a NTP is fully compatible with the European regulatory framework as well as the BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies (BoR (20) 46).

In this context, we would like to note that the possibility for end-users to choose the terminal equipment at their broadband connection is already explicitly laid down in European law (cf. Art. 3(1) Regulation (EU) 2015/2120). A precise and unambiguous regulatory definition of the NTP at point A by the EETT would bring this to life in all member states of the European Union - including Greece - and make it fully applicable in practice.

A passive NTP (point A) and the resulting free choice of terminal equipment leads to a lively competition for the best terminal equipment, from which especially the end-users benefit, who could freely choose from various innovative and high-performance products the one that best meets their demands for quality and functionality. In addition, freedom of choice of terminal equipment makes it easier for end-users to change network operators, creates a clear data protection situation and contributes to greater IT security. In addition, the free choice of terminal devices - in contrast to the so-called "obligatory terminal equipment" - makes much more sense for ecological and economic reasons.

The freedom of choice of terminal equipment further promotes the innovative capacity of telecommunications terminal equipment manufacturers as well as technical progress and thus contributes to strengthening the digital sovereignty of the telecommunications terminal equipment industry in Greece and Europe. Furthermore, it enables the great potential of modern broadband infrastructure to be better exploited.

In countries such as Italy or Germany, where the free choice of terminal equipment was (re)established by a precise and unambiguous definition of the NTP as "passive" (point A) already in 2018 and 2016, respectively, it can be seen that this is technically easily achievable and a success story. Many end-users are happy to make use of the option to purchase a terminal device from a retailer and use it on their



broadband connection. The problems predicted in advance by the network operators, which in their opinion were associated with freedom of choice of terminal equipment (such as network breakdowns), have not occurred.

It can therefore be clearly stated that there are no technical reasons whatsoever that would speak against a definition of the NTP at point A and the associated full freedom of choice of terminal equipment.

On the individual questions:

1. Do you think it is necessary or not to define the Network Termination Point? Please give reasons for your opinion.

The lack of definition of the NTP in Greek regulation allows network operators to arbitrarily (re)define the NTP, which is the boundary between the public telecommunications network and the private home network, according to their needs.

Thus, the possibility exists for network operators to determine that the NTP is not the "socket on the wall" (passive NTP), but should be located at the subscriber-side interfaces of the terminal device owned by the network operator. The router, modem, etc. should therefore be an integral part of the public telecommunications network and be under the sovereignty of the network operators. On this basis, the network operators can make the use of a certain terminal device compulsory for their customers.

The definition of the NTP is to avoid that operators unilaterally determine the specifications of terminals compatible with their networks, which would enable them to transfer its market power in the area of services to the market for terminals.

A precise and unambiguous definition of the NTP as "passive" ("socket on the wall", point A) ensures that connected terminal devices have direct access to the physical transmission medium (i.e. the line or cable). Such a technology-neutral definition has the effect that the NTP can no longer be "moved" into the terminal or to its subscriber-side interfaces to prevent free choice of terminal equipment.

In this respect, we consider it necessary for EETT to define the NTP precisely and unambiguously.

2. Which point do you think is most suitable to define a Network Termination Point (A, B or C)? Document your answer.

The VTKE supports and strongly recommends a definition of the NTP at point A.

Only if there is an NTP at point A,

... **End-users can freely choose and operate the terminal device** that best meets their needs and wants when it comes to quality and functionality at their Internet connection.

... **The great potential of a high-performance network infrastructure can be better exploited** and **end-users can take full advantage of technological progress** as commercially available terminal devices often have more functionalities and are more powerful than provider terminal equipment.



... **End-users can change the network operator more easily**, because they can simply continue to use their existing, already familiar terminal device instead of renting and configuring a new mandatory device from the network operator, which is often associated with a lot of effort.

... The **end-user is in a clear situation in terms of data protection**.

If the terminal device with its local routing functions is part of the public telecommunications network, the communication previously conducted via private networks within the end users' private home networks (Wi-Fi, DECT, telecommunications systems) becomes a component of public communication under the control of the network provider. Sending a document or photos to a wireless printer via Wi-Fi would then become part of public communication, to which the network operator could theoretically have access.

The fact that the following data are stored in the terminal device for technical reasons also raises data protection concerns: A home network router is „aware of“ a list of all devices integrated in the home network (notebooks, tablets, smartphones, printers, etc.), the times at which the above mentioned devices are switched on and off, the assignment of internet traffic to certain devices in the private network, telephone books, call lists, call diversion settings, account information for other services, a list of connected USB devices, connected Smart Home devices and much more. If the terminal device continues to be defined as part of the provider's public telecommunications network and they have control over it, these data would theoretically also be accessible to the network operator.

It is doubtful that this transparency about private activities in the home network is permissible and unproblematic.

... There is a **positive effect on network security**.

The infrastructure monoculture created by obligatory terminal devices can result in security problems with one terminal device (such as a hacker attack) inevitably affecting a very large number of terminal devices and thus end-users. In such a case, the end-users have to wait until their network operator resolves the problem and they would continue to be exposed to risks during this period, which may last for days or weeks.

... **Net Neutrality** as principle of open, non-discriminatory network access **is being protected**.

On the one hand, the restriction of the right to connect no longer allows nondiscriminatory network access. On the other hand, if the terminal device is controlled by the network operator, the users can no longer decide themselves which services are transmitted and at what quality.

... There is an **open market for terminal devices, competing for quality and performance features** in order to attract customers. This is what leads to transparency and security. From an economic point of view, an open competition for the best terminal device increases the incentive for innovation by manufacturers of terminal equipment, accelerating innovation cycles for products. Here, too, end-users would benefit from innovation and technical progress.

... There are **clear economic and ecological advantages**.

“Cascading“ (connecting a mandatory terminal device to a freely chosen terminal device) is disadvantageous for ecological and economic reasons. Both devices require power, resulting in increased



and unnecessary electricity costs for the end-user. With regard to the provider's obligatory terminal equipment, the end-user thus pays the electricity costs for a device that does not belong to him or her but over which the network operator has control. Last but not least, in view of the global trend towards greater energy efficiency, the additional power consumption that is ultimately unnecessary is harmful to the environment. In addition, there are purchase costs for the terminal device prescribed by the provider, which would not have to be spent if the terminal equipment was not obligatory.

... There is a **diversity of terminal equipment from different manufacturers, vendors and providers** that are used on the networks of different network operators. This **promotes interoperability** overall.

... It is **possible for manufacturers of terminal devices to offer fully integrated terminal devices** with optimum energy consumption and performance features.

In this context, EETT correctly observes that the majority of DSL equipment cumulates the router and modem functions (see 3. of the consultation document).

... The **share of closed broadband connections ("golden bundles") decreases**. Manufacturers of network equipment link the sale of their network equipment with terminal equipment. This goes against the spirit of diversity, interoperability and freedom of choice. A free choice of terminal equipment (re-)established by an NTP at point A provides a remedy.

... The **European Union's digital sovereignty** is being **supported**. Competition for the best terminal device within the European Union strengthens European manufacturing companies and Europe's ability to act in this area.

BEREC also clearly states the numerous advantages of an NTP at point A in Guideline 40.

Against this background, we agree with EETT that a NTP at point A does not create any market restrictions for terminal equipment, the interoperability of terminal equipment with the public network is ensured and the protection of end-user data is guaranteed.

3. If you propose point B or C, refer in detail to the criteria in section 5 that are met or to additional criteria that justify your proposal.

The VTKE is exclusively in favour of defining the NTP at point A and rejects options B and C.

4. If you propose point A, justify why you think there is no reason to apply criteria iii - vi of section 5.

As a matter of principle, we would like to state that there are no technical reasons whatsoever that speak against a passive NTP (point A).

All criteria listed in section 5 (interoperability between public network and telecommunications terminal equipment (TTE), data protection, simplicity of operation of the public network, network security, local traffic and provision of fixed-line services through wireless technology) are compatible with a NTP at point A and can be implemented without technical problems.



Interoperability between public network and TTE

The interface specification description published by the network operator is the basis for interoperability. Interoperability is best achieved by applying ITU-T or ETSI standards for transmission over subscriber lines. Therefore point A should be considered the preferred NTP.

Data protection

Data security/protection is – rightly – a very important aspect of the definition of the NTP/the free choice of terminal equipment.

As stated earlier, in the case of compulsory terminal equipment (NTP at point B or C), there is theoretically the possibility for the network operator to access personal data/local traffic of the end-user as the terminal device is a part of the public network under the sovereignty of the network operator. This ultimately leads to serious data protection and privacy issues and problems.

Simplicity of the operation of the public network

We would like to point out that the interworking between the modem at the customer premises and the modem at the central site is fully standardized by ITU or ETSI, including network management (OAM). No additional effort arises therefore to handle different modems. In addition, in practice there are only two to three chip vendors supplying the customer premises equipment (CPE) market. Those chips have proven interoperability before being used in the market. The public network does not need to manage the CPE differently. The public network does only comply with its own network interface specification.

Network security

We cannot find any difference to the obligations an end-user has for all the other connected devices that he or she owns and which can be as harmful as the router or modem discussed here.

Nowadays many connected devices make it rather easy for the end-user to install security updates or these devices, including many modems and routers, have an auto-update function that automatically installs security updates if needed – no user interaction is required at all. Terminal manufacturers are already striving to ensure that their products are as secure as possible.

Problems with regard to the security of telecommunications networks and/or equipment cannot be solved by shifting the NTP within the customer's premises. Malicious parties, security researchers or amateurs with an interest will not obey or follow any rules that tell them not to connect a device to point A. The security of a telecommunications network must not depend solely on the security of the terminal devices.

The argument of network security is repeatedly put forward by opponents of the free choice of terminal equipment. In markets where freely available terminal equipment can be used instead of a compulsory terminal device from the provider, it has been shown in practice for many years that the freedom of choice of terminal equipment does not pose any particular risks to network security.

Local traffic

A location of the NTP at point B or C would lead to a violation of the legal requirements for a network termination point (in the European Electronic Communications Code (EECC, Directive (EU) 2018/1972)). For example, the LAN interface does not provide access to a telecommunications network, but to the private network of the customer's own devices at home (LAN). Private communication between two LAN interfaces would then be absurdly routed over a public network and subject to all the requirements of the legal



requirements in this area. There would also be hardly any devices that could be connected with this LAN interface, because the network devices connected to the LAN (for example PC, printer or Smart TV) are not telecommunications terminal devices.

Fixed-line services based on wireless technology

There is no reason why the mobile network NTP (the air interface) would not apply to stationary applications as well.

Berlin, 07 April 2021

Alliance of Telecommunications Terminal Equipment Manufacturers (VTKE)



Contact:

Kira Terstappen-Richter
Coordinator

E-mail: k.terstappen-richter@vtke.eu

Telephone: +49 173 62 86 244