Appendix B3 – Clarifications of Appendices B1 and B2

This document is a non-binding translation to English of the Swedish appendix published 5 June 2024

Introduction

This document provides clarifications concerning the procedure for the preliminary examination of applicants for participation in the auction for licences to use radio transmitters in the 1800 MHz band. The purpose of the preliminary examination is to assess whether the radio use according to the licence application could be assumed to cause harm to the national security of Sweden, pursuant to Chapter 3, Section 6, point 7 of the Swedish Electronic Communications Act (2022:482) (LEK). The assessment is made by the Swedish Post and Telecom Authority (PTS) after consultation with the Swedish Security Service and the Swedish Armed Forces (referred to below as 'consulting authorities').

In the application, the applicant shall answer the questions in Appendix B1 and report how each principle and the criteria for assessment of actors in Appendix B2 are taken into account.

Some general clarifications

PTS and the consulting authorities have not set any special formal requirements for how the report, in the application, is to be formulated. It is desirable that the questions are answered as clearly and in the most easily accessible manner possible. The answers to the questions in Appendix B1 and the report on how each principle and the criteria for assessment of actors in Appendix B2 are taken into account can be submitted in separate documents. The report on how the 16 guiding principles in Appendix B2 are taken into account shall, in each section, refer to the relevant principle(s).

The examination of whether the radio use in accordance with the licence application could be assumed to cause harm to the national security of Sweden is carried out in accordance with Chapter 3, Section 6 of LEK. That assessment does not affect obligations that the applicant may have in accordance with other provisions, such as the Swedish Protective Security Act (2018:585), the rules in Chapters 8 and 9 of LEK

Post- och telestyrelsen
Postal address: Box 6101, 102 32 Stockholm
Visiting address: Hälsingegatan 38
Phone: 08-678 55 00
Email: pts@pts.se
www.pts.se

and in PTS regulations and general advice (PTSFS 2022:11) on security in networks and services, or future legislation. However, an applicant who follows the rules in these regulations should be well placed to submit an application that takes into account the principles and criteria for assessment of actors in Appendix B2.

In the documents submitted to PTS, applicants shall mark information that in the applicant's assessment is security-classified, along with which security classification the information belongs to. The applicant shall also state which information is covered by secrecy under the Swedish Public Access to Information and Secrecy Act (2009:400).

If PTS decides that an applicant's radio use in accordance with the application can be assumed to cause harm to the national security of Sweden, PTS will reject the application to participate in the auction.

At this point, it is not possible to determine whether there will be grounds to combine a certain applicant's licence with special licence conditions in terms of requirements that are of importance to the national security of Sweden pursuant to Chapter 3, Section 12, first paragraph, point 9 of LEK, and, if so, how such conditions may be formulated. If it becomes apparent that there are special circumstances for an individual licence holder, such circumstances could justify the introduction of special conditions for that licence holder, in order to ensure that certain measures are taken. PTS's position, however, is that the same licence conditions should generally apply for all licence holders.

Clarification of Appendix B1 to Open Invitation Part 1

Question 1 in Appendix B1: The licence in itself does not require certain specific services to be provided in the relevant frequency bands. It is up to the applicant to specify which functions are fundamental from a security standpoint. A reasonable starting point is that data communication, voice calls and messaging services can be critical services, if these services are provided to end customers, i.e., subscribers and users. Additional services need not necessarily constitute part of the critical infrastructure. Operation and maintenance networks that control network availability can be considered to be critical infrastructure. The assessment of what affects the national security of Sweden may change over time depending on how technology, services, etc. develop. Any other services needed to provide central functions shall also be presented.

Question 3 in Appendix B1: The purpose of Question 3 is to obtain information about who has influence and in practice controls and influences an applicant company. A company listed on the stock exchange can state that it is a listed company and give

the names of its largest owners at the time of the application. The names of approximately the 10 largest owners can be given.

Question 5 in Appendix B1: The description shall concern the central system architecture. The system architecture for the transport network may also be necessary to describe. The description of network elements can be general, through a network sketch with full names of included network elements. A description at the component level, e.g. of number of servers, etc., is not necessary. If a specific standard is used, it can be referred to. The content of the standard does not need to be copied into the document.

It should be stated how the geographic expansion will take place. Geographic locations do not need to be more specific than names of cities, towns, etc.

It is mainly the network's architecture and structure at commissioning that must be reported. If an applicant already knows at the time of the application that the applicant intends to use existing infrastructure at commissioning, such as an existing core network, and then later switch to a 5G core network, such circumstances shall be stated in the application, along with when the switch might take place. Other anticipated general changes should also be stated.

If artificial intelligence (AI) will be used for the operation of the network, it should be stated who controls it and how, and a description should be given of how the use of AI takes the guiding principles according to Appendix B2 into account.

If open radio access networks (Open RAN)[1] are to be used, this must be stated, as well as a description of the special security measures that the company applies to be able to ensure availability, accuracy, authenticity and confidentiality.

Clarification of Appendix B2 to Open Invitation Part 1

General information about the document

'The overall functionality of the network' refers to general functions in radio access, core, transmission, and operation and maintenance networks, required for the network and services to end users. The functionality need not be described in precise detail, including number of servers, etc. What is referred to is how the network is built, in general. It is okay to refer to a standard, if one is used. If the applicant, for example, plans to use AI, it is important to describe how the AI functionality is to be planned, monitored and controlled. If the applicant plans to use

[1] Open RAN means a radio access network consisting of software and hardware components with open interfaces that follow common standards.

Open RAN, it is important to state when this is planned to happen and how the applicant works to identify and prevent security risks linked to Open RAN.

'Central functions' are those functions needed, on a general level, to provide communication services.

The phrase 'communication services provided by the operator to end users' refers to mobile voice, data and messaging services over 4G and 5G to end customers. Note that 'users' is broader than 'subscribers', in that it can include e.g. users of services provided in corporate subscriptions.

The term 'regulatory services' refers, for example, to requirements concerning the provision of the 112 emergency phone call service, but also to other services that an operator is obligated to provide under LEK.

The consulting authorities deem that the observance of the guiding principles in accordance with Appendix B2 is a guarantee for the national security of Sweden. A key intention of the principles is that operators should be able to use the principles as a basis to build secure networks and then be able to manage them with regard to the national security of Sweden. If the operator considers and complies with the guiding principles, it creates conditions to also be able to provide services to customers conducting security-sensitive operations. If the principles are not considered, the radio use could be assumed to cause harm to the national security of Sweden. The consulting authorities will make an overall assessment based on what is stated in the application. Non-technical vulnerabilities and risks will also be assessed. These refer, for example, to suppliers and subcontractors that are known to the consulting authorities to pose risks; exposure to another government's legal system is an example of a factor that may be taken into account.

The licence conditions concerning the national security of Sweden will apply throughout the validity period of the licence. PTS can exercise supervision to ensure that the licence conditions are met.

Guiding principles

1. Must function even if connections to other countries are broken

If the applicant has a network element outside Sweden, the network must function even if connections to other countries are broken. This is also a matter of network availability because the applicant must be able to operate the network even if the borders are closed. This also applies in relation to our neighbouring Nordic countries. The principle is that the network must function independently, without connection to foreign countries. However, there is no requirement that all equipment must, without exception, be located within Sweden's borders. If an applicant has solutions with

connections to other countries, it is important to explain in the application the exposures that could arise and how the applicant acts to address these exposures. The applicant must be able to demonstrate that such solutions do not entail any risk of harm to the national security of Sweden.

The operators must have a clear continuity plan for how the network will function should disturbances in relation to products (including components, spare parts) and suppliers arise, and be able to ensure that security incidents can be handled from Sweden and that system and user data are stored in Sweden.

What is referred to here are the central functions in the network, which concerns the services provided by the applicant, not communication services provided by another party (e.g. "Vårdguiden 1177", Facebook)[2].

'System data' refer to metadata (configuration, parameters, etc.) that are directly attributable to the central function and thereby have an impact on the national security of Sweden. 'User data' refer to traffic information, location data and subscriber information.

2. Must provide functions that enable connections to and from foreign countries to be easily, quickly and selectively broken

What is referred to here are quick measures to, for example, stop cyberattacks in progress from abroad.

3. Must provide a high level of availability and secrecy

This refers to functions identified in a security analysis, but it can also include other things. Functions to e.g. generate availability in the network must be created in such a way that vulnerabilities are prevented. A development in which services move further out in the network has been considered, but the purpose of the principles will be the same. With respect to 5G, it can be generally said that the development could open up new vulnerabilities that cannot be foreseen today. It may therefore be necessary to make changes in the network architecture over time.

'Availability' refers to access control, but also availability in the network, that services work.

The word 'secrecy' does not have the same meaning as 'confidentiality', but PTS regulations and general advice (PTSFS 2022:11) on security in networks and services can be a support. To comply with the requirement for secrecy, the networks must be

[2] However, number-independent interpersonal communication services may be subject to their own security requirements according to LEK.

built to ensure that no one else than the operator (and possibly third party responsible for support) can access and control them.

For virtualised nodes for central functions, the nodes' dependence on the virtualisation platform itself must be described. This refers to the entire virtualisation infrastructure, from hardware to software.

5. Must be designed to prevent unauthorised control or manipulation

The word 'prevent' is stronger than 'guard against' or 'effectively counteract', considering that what is under consideration is the national security of Sweden, and the risks cannot be accepted in any circumstance. Applicants should describe what is done to prevent risks and vulnerabilities to the greatest extent possible. Taking security measures for more secure external routing (e.g. introduction and application of so-called RPKI) can be a measure. When vulnerabilities are discovered in e.g. stress tests, these must be remedied immediately.

Administration of the networks, traffic protection, but also the operation and maintenance network, must be separated.

6. Must be designed to prevent control or manipulation from abroad

It is important that the applicant does not build the network in a way such that it is possible to control from outside the country. The functioning of the network must not be lost if the connection to other countries is broken.

7. Must be designed to prevent unauthorised mapping of services, capacity, location or users

This point refers to information about the network and its users. 'Unauthorised mapping of services' refers to services that the operator provides to users. Access to central functions would mean that such use can be mapped. It is not the offer to provide a certain service that is considered to merit protection, but rather the users and subscribers of a certain service.

'Unauthorised mapping of capacity' refers to the capacity that customers subscribe to. This information can merit protection as it is possible to draw conclusions about what the subscription might be used for. Such information must not be available to an adversary. Information about services and capacity can, particularly in aggregated form, constitute a security risk, and such risks must be considered right from the planning stages.

'Unauthorised mapping of location' refers both to information about end customers' locations and information about the location of different network elements.

‘Unauthorised mapping of users’ refers to traffic information attributable to mobile voice, data and messaging services, location information, and communication content. It is not necessarily the same definition as in the question regarding storage of traffic data for law enforcement purposes.

Virtualisation solutions must be described to the extent that they are in place when the network is commissioned. In the event of later changes in the network, the licence holders should inform the authorities when this becomes relevant.

8. Must be designed to prevent unauthorised intervention (such as electronic attacks) and, where such prevention is not possible, to ensure that unauthorised interventions are detected and averted

The principle has a broader meaning in relation to other principles. It may, for example, be the case that there are other protective measures that can be taken, such as physical protection and protection against unintentional interference. It is desirable that other such protective measures are also reported.

10. Must have traceability for functions that can affect secrecy, availability, observation or control

‘Activities from third parties’ also includes support from manufacturers or suppliers.

11. Must be designed in such a manner that equipment for which there is a risk of unauthorised observation, control or manipulation, through physical access, is located on Swedish territory in order for Swedish legislation to be applicable

With respect to traffic data stored for law enforcement purposes, such information may be stored outside Sweden, provided it is stored within the EU. (See Swedish Government Bill 2018/19:86.) In principle, there is a requirement that ‘system and user data must be stored in Sweden’ for information that concerns the national security of Sweden. All information stored for law enforcement purposes does not necessarily concern the national security of Sweden, but information that could be used to harm Sweden must be stored in Sweden. In many cases, however, this will be the same information. If an operator chooses to store data in another country, the operator must show that this storage cannot harm the national security of Sweden. If the operator can describe solutions that, while storing data in another country, still follow the principles and protect the national security of Sweden, such solutions may be acceptable.

The Swedish Security Service considers it important that information that the authority needs in order to investigate crimes against the national security of Sweden, including stored traffic and user data, is available even if connections to other countries are broken.

12. The operator must continuously provide information to designated recipients at the sector-responsible authority concerning measures taken, in the communication networks, that could affect secrecy, robustness, availability, observation or control

The term 'communication networks' has the same meaning as the previously mentioned 'central functions'.

13. The operator must provide information in sufficient time that the sector-responsible authority can determine the risks entailed in such measures taken in the communication networks, and if corrective measures are needed

14. The operator must actively facilitate the sector-responsible authority's observation and control

Points 12–14 are aimed at ensuring that operators who are awarded licences communicate significant changes in the networks. This may concern, for example, new automation solutions or changes with respect to third-party suppliers, for which the security authorities may have valuable information about issues that could pose significant risks. Changes that are small for an individual operator can, notwithstanding, have major consequences.

Operators must themselves assess whether such changes occur and inform the authorities. The legislation does not contain any obligatory prior approval for changes in the networks, however, what is stipulated in these points must be continuously considered. An operator is not prevented from taking immediate measures that are necessary, e.g. due to a security incident.

In the case of planned measures that could have a greater impact, e.g. procurement of new suppliers or contracting a third party for network operations, it is valuable if PTS and the consulting authorities are given the opportunity to provide support and information concerning potential risks before the change is carried out. The consulting authorities may have valuable information about issues that could pose significant risks.

PTS will, in its capacity as licensing and supervisory authority, check and follow up on operators' information regarding measures and changes. In this context, PTS may also request detailed information from operators and specify the periodicity at which such information must be provided.

It is important to point out that information that an operator provides to PTS in accordance with these points does not affect any obligation to also provide information pursuant to other legislation, e.g. the Protective Security Act (2018:585), or Act (2018:1174) on information security for services that are vital to the functioning of society and digital services.

15. The operator shall develop, implement, operate and maintain adequate security measures

16. The operator shall ensure that personnel who obtain access to information that could affect confidentiality, accuracy, robustness and availability, are authorised and trained in security and are aware of the secrecy of the information

Principles 12–16 contain requirements on measures that, in addition to principles 1–11, may also concern protection in a broader sense. In this context, operation and maintenance also refers to continuous skills development, ensuring that there is the appropriate staffing, etc. The requirements in the previous principles remain in principles 12–16 through the way in which the licence holders are assumed to work with these issues.

The requirements in points 15 and 16 may go beyond the requirements of the Protective Security Act (2018:585). This may concern, for example, protective measures for vital locations with vital equipment and other operational protection. Point 16 refers to central functions, including vital services. 'Robustness' refers to the stability in the network, resistance to operational disturbances, redundancy, etc., to avoid system collapse.

Miscellaneous

The reference to the so-called EU Toolbox (EU toolbox for 5G security[3]) is for information purposes only. The toolbox is aimed at the EU's internal security, while the guiding principles are aimed at the national security of Sweden. However, some of the principles in the toolbox may be useful also at the national level. The guiding principles are based on what is required for the national security of Sweden, and are therefore not given the same grading as in the toolbox.

[3] NIS Cooperation Group. CG Publication 01/2020. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures