NICC ND 1448 V1.1.1 (2024-01)

NICC Document

Guidance to Providers on interpretation of the terms PECN and PECS in relation to the Telecommunications (Security) Act 2021

NICC Standards Limited

c/o TWP ACCOUNTING LLP,
The Old Rectory,
Church Street,
Weybridge,
Surrey KT13 8DE

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number 6613589

NOTICE OF COPYRIGHT AND LIABILITY

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be that printing on NICC printers of the PDF version kept on a specific network drive within the NICC.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other NICC documents is available at:

http://www.niccstandards.org.uk/publications/

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary,
NICC Standards Ltd
secretary@niccstandards.org.uk

Copyright

All right, title and interest in this document are owned by NICC Standards Limited ("NICC") and/or the contributors to the document (unless otherwise indicated that copyright is owned or shared with a third party). Such title and interest is protected by United Kingdom copyright laws and international treaty provisions.

The contents of the document are believed to be accurate at the time of publishing, but no representation or warranty is given as to their accuracy, completeness or correctness. You may freely download, copy, store or distribute this document provided it is not modified in any way and it includes this copyright and liability statement.

You may not modify the contents of this document. You may produce a derived copyright work based on this document provided that you clearly indicate that it was created by yourself and that it was derived from this document and provided further that you ensure that any risk of confusion with this document is avoided.

Liability

Whilst every care has been taken in the preparation and publication of this document, neither NICC, nor any working group, committee, member, director, officer, agent, consultant or adviser of or to, or any person acting on behalf of NICC, nor any member of any such working group or committee, nor the companies, entities or organisations they represent, nor any other person contributing to the contents of this document (together the "Generators") accepts liability for any loss or damage whatsoever which may arise from the use of or reliance on the information contained in this document or from any errors or omissions, typographical or otherwise in the contents.

Nothing in this document constitutes advice. Nor does the transmission, downloading or sending of this document create any contractual relationship. In particular no licence is granted under any intellectual property right (including trade and service mark rights) save for the above licence to download copy, store and distribute this document and to produce derived copyright works.

The liability and responsibility for implementations based on this document rests with the implementer, and not with any of the Generators. If you implement any of the contents of this document, you agree to indemnify and hold harmless each Generator in any jurisdiction against any claims and legal proceedings alleging that the use of the contents by you or on your behalf infringes any legal or other right of any of the Generators or any third party.

None of the Generators accepts any liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance on the contents of this document for any purpose.

IPR and Anti-trust policy

The NICC Standards Web site contains the definitive information on the IPR Policy and Anti-trust Compliance Policy

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC. Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by NICC Security TG.

Introduction

This document aims to provide guidance to Providers to help them arrive at an interpretation of the terms ‘Public Electronic Communications Service’ (hereafter PECS) and ‘Public Electronic Communications Network’ (hereafter PECN) as defined specifically in Sections 32 and 151 of the Communications Act 2003 [1], for the purposes of the Telecommunications (Security) Act 2021 (TSA) [2] and the associated Electronic Communications (Security Measures) Regulations 2022 [3] and Telecommunications Security Code of Practice [4].

Hereafter this document refers to [2] as “the Act”, [3] as “the Regulations” and [4] as “the code” or “the code of practice".

1 Scope

The present document is intended to support Providers in making their own assessment of whether their products or services fall within scope of the regulations and code of practice supporting the TSA and – if so – whether certain elements constitute Security Critical Functions (SCFs), or Network Oversight Functions (NOFs), or Associated Facilities[4].

The document does not constitute legal advice or provide a definitive position on whether any specific service type or model is or should be included as an element of PECN and PECS – rather, it details commonalities (and – where relevant – differences) between how Providers might interpret them by detailing what criteria might be used to answer three key questions:

Q1 – Is a given element a PECS or PECN?
  Q1.1 Does the element need to comply with the Act and/or the Regulations?
Q2 – Is an element a Security Critical Function?
  Q2.1 Is the element subject to specific regulations and measures within the Code?
Q3 – Is an element a Network Oversight Function?
  Q3.1 Is the element subject to specific measures or clauses in the Code?

In common with other industry guidance, this document is intended to support Providers in delivering compliance, assurance, and reporting as required by the TSA.

The scenarios and edge cases described in Section 8 are examples provided for illustrative purposes and are not intended to be definitive or exhaustive.

NICC Standards Limited members have produced this ND which includes a process by which Providers might determine what may be in or out of scope of the TSA and any associate documentation. Each Provider should continue to take their own legal advice on compliance with all legislation, independently of this document. This document should not be used as sole justification for any Provider decisions on what should, or should not, be considered as in or out of scope.

The requirements in the TSA and Regulations come into effect over the period 01 Oct 2022 through 31 March 2028. Providers and Operators would probably prefer to have some guidance from the Regulator that decisions they are making as they make changes to their networks would lead to compliance. However, Ofcom have made it clear that they cannot provide feedback that a particular choice will be compliant. It might be prudent for Providers and Operators to share their decision-making rationale with the Regulator at their earliest convenience so that the Regulator is aware of the background and approach being taken. This does not ensure compliance; however, the transparency will be beneficial in the long term as the Regulator will understand the reasons behind the choices made.

NCSC comment
While this guidance document is published by NICC, it has been produced by and only represents the views of the industry members of NICC. It should not be inferred from the NCSC's Associate Membership of NICC that this document is in any way endorsed by or represents the view of the NCSC. The definitions in the Communications Act 2003 and The Electronic Communications (Security Measures) Regulations 2022 determine what is in scope. The Telecoms Security Code of Practice (the Code) gives guidance as to the measures to be taken by Providers. We would encourage Providers to define the scope of their cyber defence based on risk, as per section A2 of the Code, rather than based on the interpretation of the law contained in this document.

Additionally, the NCSC:

- believes that the interpretations set out in this document are incorrect; and
- does not recognise the NICC as having the appropriate remit to provide comment on the Code in this way.

Ofcom comment

While this guidance document is published by NICC, it has been produced by and only represents the views of the industry members of NICC. It should not be inferred from Ofcom's observer membership of NICC that this document is in any way endorsed by or represents the view of Ofcom. The definitions in the Communications Act 2003 and The Electronic Communications (Security Measures) Regulations 2022 determine what is in scope. The Telecoms Security Code of Practice gives guidance as to the measures to be taken by Providers, and Ofcom is required to take the Code into account in our work.

2 References

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] Communications Act 2023
https://www.legislation.gov.uk/ukpga/2003/21/contents

[2] Telecommunications (Security) Act 2021
https://www.legislation.gov.uk/ukpga/2021/31/enacted

[3] The Electronic Communications (Security Measures) Regulations 2022, UK Statutory Instruments 2022 No. 933
https://www.legislation.gov.uk/uksi/2022/933/contents/made

[4] Telecommunications Security Code of Practice, December 2022
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120531/E02781980_Telecommunications_Security_CoP_Accessible.pdf

[5] Ofcom Consultation on Net Neutrality, Annex A5
https://www.ofcom.org.uk/__data/assets/pdf_file/0025/245923/net-neutrality-review-annex.pdf

[6] Product Security and Telecommunications Infrastructure Act 2022
https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted

[7] IETF RFC 6291 Guidelines for the Use of the "OAM" Acronym in the IETF dated June 2011
https://datatracker.ietf.org/doc/html/rfc6291

[8] Open Consultation – Call for Information on the uses and security of Private Telecommunications Networks within the UK
https://www.gov.uk/government/consultations/private-telecommunications-networks-call-for-information/call-for-information-on-the-uses-and-security-of-private-telecommunications-networks-within-the-uk

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply :

Provider	Provider of an ECS and/or ECN
Regulated Provider	A Provider (offering PECN and/or PECS services) regulated specifically by the Communications Act 2023 (as amended)

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BSS	Business Support Systems
CPE	Customer Premises Equipment
DOCSIS	Data Over Cable Service Interface Specification
ECS	Electronic Communications Service
ECN	Electronic Communications Network
IVR	Interactive Voice Response
KPI	Key Performance Indicators
MNP	Mobile Number Portability
NOF	Network Oversight Function
OAM	Operations Administration and Maintenance
OLT	Optical Line Terminal
OSS	Operational Support Systems
OTS	One Touch Switch
PAWs	Privileged Access Workstation(s)
PECN	Public Electronic Communications Network
PECS	Public Electronic Communications Service
PSTN	Public Switched Telephone Network
SCF	Security Critical Function
SD-WAN	Software Defined Wide Area Network
SLA	Service Level Agreement
TSA	Telecommunications (Security) Act 2021
VPN	Virtual Private Network

4 Proposed criteria for determining assessment of PECS or PECN

Provisions of the TSA apply to all PECSs and PECNs. This paper set out tests for assessing each of these below, based on an interpretation of relevant sources.

4.1 Determining whether a service is a PECS

Assessment of whether a given service can be considered a PECS requires a two-stage process to answer the following questions.

Q1 – is the product or service an Electronic Communications Service (ECS)? And then
Q2 – is the product or service available to the public?

4.1.1 Determining if the service constitutes an ECS

Identifying whether a service constitutes an ECS typically requires Providers to make four distinct assessments. These are set out in

Figure 1.

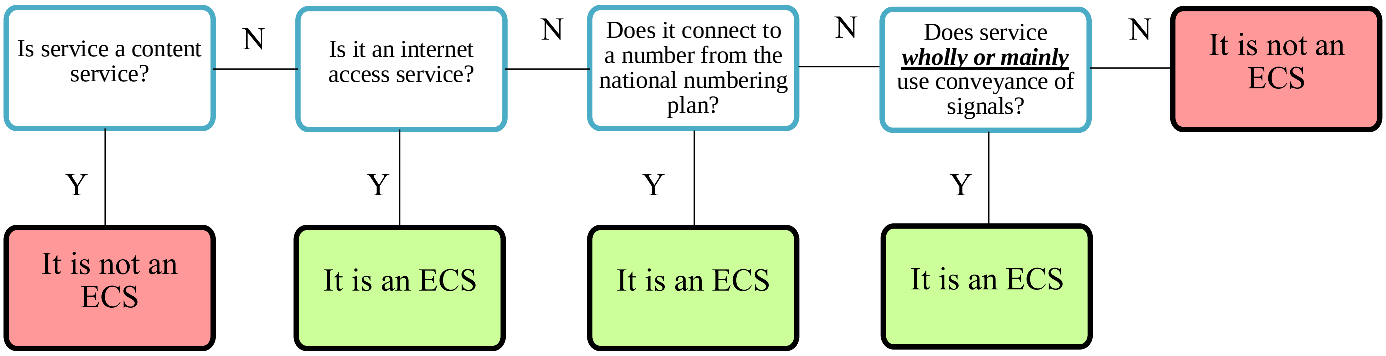
Is service a content service?
N
Is it an internet access service?
N
Does it connect to a number from the national numbering plan?
N
Does service *wholly or mainly* use conveyance of signals?
N
It is not an ECS
Y
Y
Y
Y
It is not an ECS
It is an ECS
It is an ECS
It is an ECS

Figure 1 - ECS Assessment Process

Based on experience shared amongst Providers drafting this document, there are two practical issues which might lead to diverging interpretations amongst communications Providers:

- content services are often sold together with transmission elements, so it is not always straightforward to distinguish content services from ECS;
- 'wholly or mainly use conveyance of signals' is by definition a relative measure, meaning that some subjective assessment is required by Providers when making assessments.

4.1.2 Determining if the service is available to the public

There is limited information available on delineating between public and non-public services. Providers can use a variety of 'proxy' tests to assess whether a given service can reasonably be considered in scope. Even where commonly applicable tests are used to assess whether a service is public or non-public, there are likely to be edge cases which require some degree of flexibility in making such assessments.

Figure 2 describes typical approaches used by Providers to examine whether a service is likely to be considered as public and, therefore, likely to be in scope.

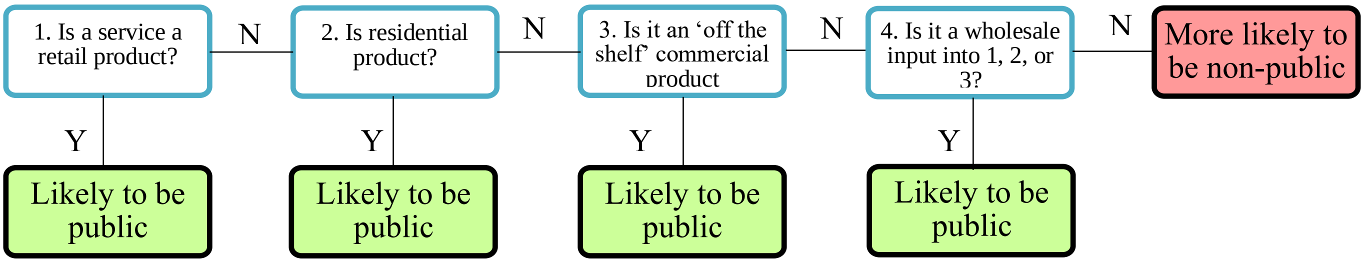
1. Is a service a retail product?
N
2. Is residential product?
N
3. Is it an 'off the shelf' commercial product
N
4. Is it a wholesale input into 1, 2, or 3?
N
More likely to be non-public
Y
Likely to be public
Y
Likely to be public
Y
Likely to be public
Y
Likely to be public

Figure 2 - Approaches used for assessing services as public

Figure 3 describes typical approaches used by Providers to examine whether a service is likely NOT to be considered as public and, therefore, likely to be out of scope.

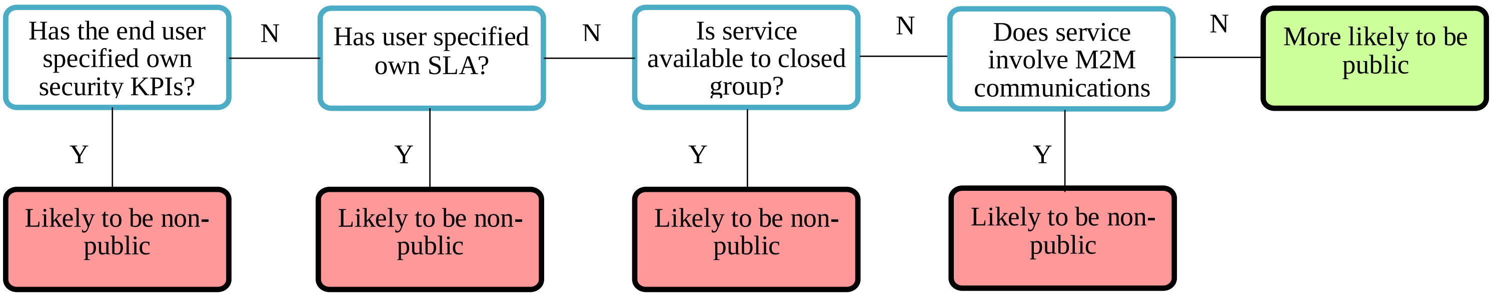
Has the end user specified own security KPIs?
N
Has user specified own SLA?
N
Is service available to closed group?
N
Does service involve M2M communications
N
More likely to be public
Y
Likely to be non-public
Y
Likely to be non-public
Y
Likely to be non-public
Y
Likely to be non-public

Figure 3 - Approaches used in assessing services as non-public

The explanation for these criteria is set out in the table 1 below:

Criterion	Reason
User has specified their own security KPIs	• Services with unique security KPIs not marketed to the public; • Specification of security KPIs may imply preferences differing from TSA 'defaults'; • Requires specialist tools/knowledge usually only available for large corporate, enterprise or public sector users
User has unique SLA	• Services with unique SLAs not marketed to the public; • Requires specialist tools/knowledge usually only available for large corporate, enterprise or public sector users

Criterion	Reason
Service available to only a 'closed group', such as: - employees of a company, - members of an organisation - network(s) within a campus - services on corporate private networks	• Cannot be accessed by public without credentials extraneous to connectivity element (e.g. corporate ID, corporate login, VPN access etc.)
Involves machine to machine communications	• Connectivity element not available to public

Table 1 – Decision Criteria

Providers may also wish to refer to [5].
Ofcom has not published any definitive guidelines on how it interprets the definitions of PECNs or PECSs under sections 32 or 151 of the Communications Act 2003 for the purposes of TSA and has signalled it does not intend to do so.
Nonetheless, it has addressed this matter to some extent in adjacent policy work in other contexts, most notably in [5] where clauses A5.18, A5.19 and A5.20 informed some of the content in this section.

4.2 Determining whether a network is a PECN

PECNs are networks used wholly or mainly to provide electronic communications services to the public. If, after following section 4.1.1 and 4.1.2, a determination is made that a service is a PECS, the network(s) used to deliver that service are PECN.

It is extremely important to understand that network assets fulfilling this criterion are likely to be included in scope, even if they are <u>also</u> used to provide services which might be considered out of scope.

For the purposes of clarity and to avoid confusion, four specific elements are described below to aid understanding.

Further, Providers may also refer to [8] which, in the section headed "What are Private Telecoms Networks" lays out some further examples of what are considered as Private networks.

4.2.1 The Customer Termination Point

There is some ambiguity concerning where the boundary for regulatory purposes is in relation to the customer termination point. Broadly, the Regulations (4(4)(i)) and Code of Practice (3.31) provide that customer premises equipment (CPE) provided to customers "as part of the public network or service" is included within scope of the TSA, and is also part of the Providers' exposed edge. However, consumer devices generally are out of scope (broadly, such devices would be expected to fall under other legislation, for example the Product Security and Telecommunications Infrastructure Act 2022 [6]).

Figure 4 details the different scopes between the following 2 pieces of legislation in terms of 'in premise' equipment that a *typical* home may have:

- the Communications Act 2003 [1];
- the Telecommunication (Security) Act 2021 [2].

NOTE: some networks may differ slightly. For example, some Provider-provided CPE in a DOCSIS network may be considered as the Customer Termination Point.

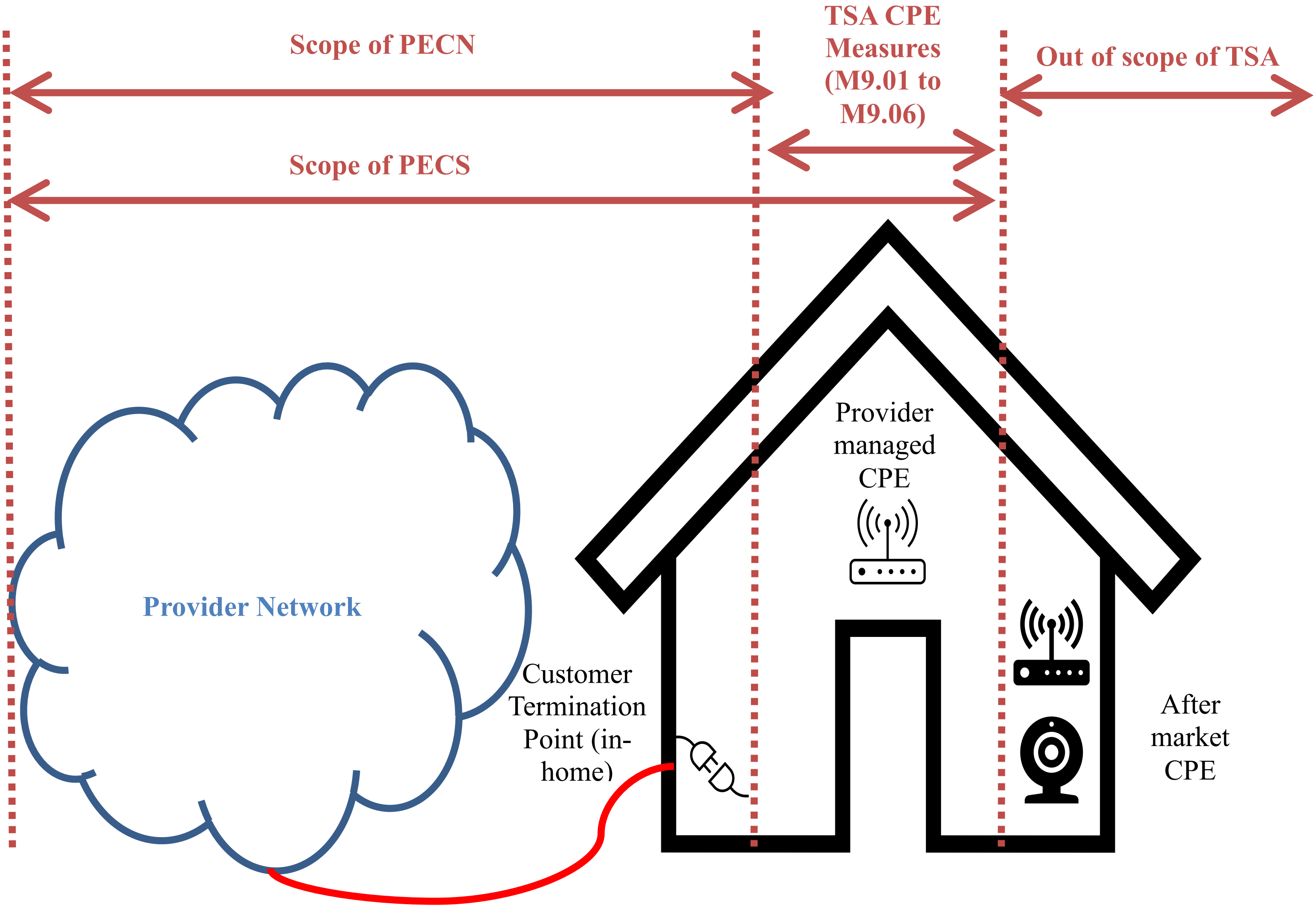

Figure 1 - Typical in-home connectivity

Figure 4 illustrates the scope of PECN/PECS and TSA Code of Practice CPE measures under the Communications Act.
However, the flowcharts in Figure 2 and Figure 3 show, the scope of TSA *may* also include residential type products in a non-residential setting.

4.2.2 Residential and business service boundaries

The boundaries between residential and business services can sometimes be thin or even overlap. Some Providers may make products available to business customers which would be considered as PECN and PECS – for example, a business utilising a 5G connected router, or provision of mobile services (e.g. all employees being issued with a 5G device).

To help explain this further, see the following fictitious case study of Customer A and their retail outlets, which illustrates the potential issues and complexities concerning differentiation between public and non-public services.

Figure 5 below shows a fictitious example of Customer A and their Pie Shop Empire to show the concept of public and non-public services.

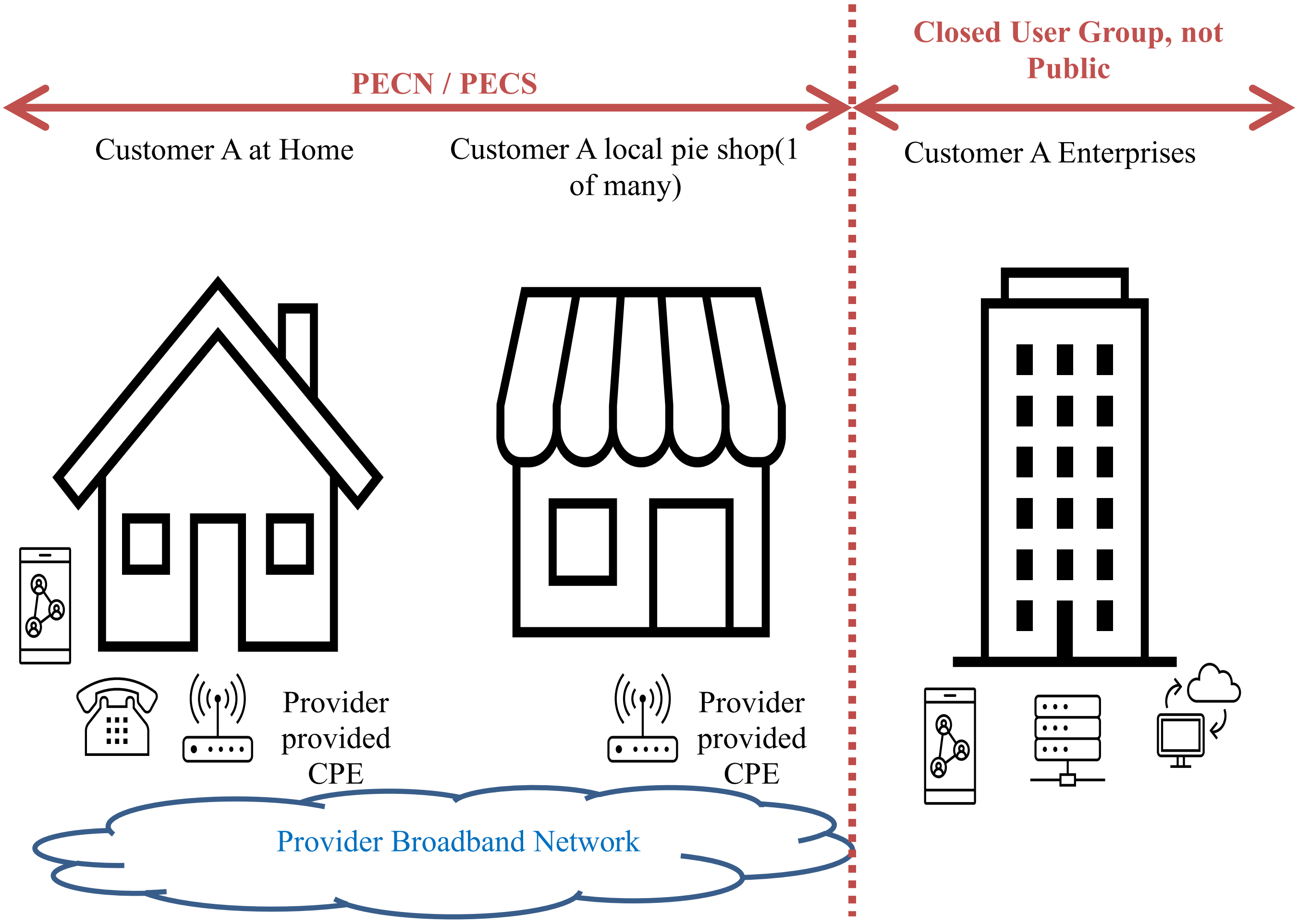

Figure 5

Case study: Customer A

In Figure 5, consider the example, firstly, of Customer A as a single residential customer at home. Customer A might have a broadband service, a home phone line and a mobile contract. In this case, services would likely be categorised as public and in-scope (although may be subject to legacy conditions in some cases, e.g. PSTN and 2G or 3G, depending on the Provider).

Now consider the middle part of Figure 5, where Customer A owns and operates a series of retail outlets in their local county. In each shop, they have the same router as they might have at home which they might use to provide wi-fi connectivity to customers and connectivity for their point of sale and card acquisition. In this instance, it is likely that Customer A is consuming the service via a commercial tariff as opposed to a residential one, but technically, it’s the same equipment on the same network and, again, services would likely be in scope.

Now consider the final part of Figure 5 in which Customer A Enterprises has a wholesale distribution business supplying national supermarkets. In this case, Customer A Enterprises might be consuming services such as SD-WAN or a managed and hosted IVR which would not be in scope as they are only available to the closed group of Customer A Enterprises employees. Some business services MAY be in scope, so this should not be considered a hard differentiation. For example for Customer A enterprise:

1. If they use a private video conferencing solution, which may not be in scope; however, the ability to make inbound and outbound calls via a telephone number (from the National Telephone Numbering Plan) may be in scope from the point where it leaves the private network.
2. Public mobile services to employees through issuing of managed handsets and subscriptions will be in scope.

4.2.3 Providers’ corporate networks and systems

Providers’ corporate networks (e.g. the internal network that carries corporate email, instant messaging, internal document storage, HR systems, etc.) would generally not be considered PECNs as they are available to a closed user group only.

Providers’ own corporate IT networks are therefore considered as out of scope for TSA but should, of course, be subject to effective security risk management. It is noted that the requirements on PAWs will overlap with Corporate IT systems - users will need to 'browse down' to corporate IT within the PAWS architectural model.

4.2.4 Intra-industry solutions

When collating this paper, those Providers involved have concluded that services for either mobile number porting (MNP) or migration between broadband Providers (e.g. the One Touch Switch process (OTS)) should likely be considered as not in scope of the TSA.

5 Proposed criteria for determining assessment of Security Critical Functions (SCFs)

The Regulations [3] define an SCF as follows (**emphasis added**):

"*…in relation to a public electronic communications network or a public electronic communications service, means any function of the network or service whose operation is likely to have* ***a material impact on the proper operation*** *of the* ***entire network or service or a material part of it****.*"

The Code of Practice, in section 2, goes further by saying:

"*1.4 Security critical functions will therefore make up different proportions of networks or services, the specific details being dependent on the unique operating mode of each individual network. However, security critical functions will include a broad range of essential functions within the network that could impact its proper operation* ***and not simply those whose primary function is security****. The guidance in this code of practice sets out specific protections targeted at different functions of networks and services that may be considered critical. It does not seek to exhaustively define components as critical.*

1.5 When deciding which functions of the network or service could not be considered as security critical, providers should be able to demonstrate that individual functions ***do not have a material impact*** *on the proper operation of the* ***entire network or service, or a material part of it****,"*

However, there is no guidance in the Regulations or the Code of Practice on the definition of "materiality" and, therefore, there is no single or simple test that Providers can use to determine if that threshold is met.

Providers will therefore need to conduct their own risk assessment to undertake a sufficiently robust analysis of their own PECSs and/or PECNs in order to understand whether an individual function or component is, or is not, likely to create *"material impact on the proper operation of the entire network or service, or a material part of it"*, i.e. be a Security Critical Function.

Relevant factors to consider when undertaking such an assessment are:

i. **Methodology** – using a robust and repeatable methodology;

ii. **Network and architecture** – truly understanding the Provider's network and architecture (especially in networks where a Provider may rely on equipment provided by another Provider);

iii. **Key functionality** – considering the key functionality of any function or component as well as other typical security factors of confidentiality, integrity and availability – Providers need to be able to show they understand what a given component actually does in order to understand how it may create impact;

iv. **Documentation** – keeping a robust trail of what has been done, how it has been approached and the decisions taken is pivotal and demonstrates the robustness of the approach taken;

v. **Consistency** – being consistent in the methodology across all that is assessed is key so that the same criteria is commonly used across different situations.

Some questions that may help Providers determine whether to categorise and element as an SCF are:

- If visibility of this element were lost, would a security compromise be a likely reason for this (i.e. in the case of an L3 CPE that were accessible via the Internet, arguably yes)?
- If the function/component experienced substantial dysfunction, would the network/service continue to operate without "adverse effects"?
- Do we regard the PECN or PECS or a material part of it as meaningfully provided without this element operating correctly?

6 Proposed criteria for determining assessment of Network Oversight Functions (NOFs)

The concept of a NOF is not defined within the Regulations but is described in Annex 2 of the Code of Practice (emphasis added) as:
"Network oversight functions are the components of the network that ***oversee and control the security critical functions****, which make them vitally important in overall network security. They are essential for the network provider to understand the network, secure the network, or to recover the network."*

Assuming a Provider has identified its SCFs in some way, determining NOFs should be a case of understanding what architecture is used to oversee and control those SCFs.

Section 2 1.18 of the Code of Practice states "*Because of their importance to overall network security, all network oversight functions should normally be expected to fall within the definition of 'security critical functions' set out in the regulations."*

There are some examples of what are considered NOFs provided in Section 2 clause 1.8 [Ref] of the CoP:

"Network oversight functions include, but are not limited to, the following components of the network where such components oversee and control security critical functions:
• element managers;
• virtualisation orchestrators;
• management systems (e.g. jump boxes);
• security functions (e.g. firewalls at the edge of a security zone);
• root authentication services (e.g. active directories (ADs));
• multi-factor authentication services;
• security gateways (e.g. supporting the management plane);
• audit and monitoring systems (including network quality monitoring of speech and data); and
• Operational Support Systems (OSS)."

Note: OSS as defined in the above list may have different meanings to different Providers. An important consideration is whether the system has a material impact on the operation of the PECN/S; for example, element managers (listed in bullets above) are generally considered OSS platforms and would be a NOF due to their function; however, a network planning tool may also be considered an OSS platform but may not be a NOF or even considered in scope of TSA, if it has no material impact on the operation of the network.

While the list in the CoP is not exhaustive it does provide an indication on the type and function of platforms considered to be a NOF. The general principle is that a NOF is considered to have a higher security risk than an SCF, as its compromise would have a greater impact on a Provider PECN/S. This view is reflected in the CoP where additional mitigating measures are specified over and above those for a SCF.
NOFs could be classed as being:

- Operational NOFs – An operational function managing SCFs and/or lower order elements within the PECN or PECS;
- Security NOFs – Providing a security function primarily to protect the management plane of SCFs or other NOFs (e.g. multi-factor authentication services or Active Directory);

- Audit/Monitoring NOF – OSS tools used for security and signal monitoring, and audit log management.

6.1 Operational NOFs

For operational NOFs the relationship between the Provider's overall scope, NOFs, SCFs and lower order elements is largely hierarchical as shown on Figure 6. There are some broad principles to consider:

- Within any given PECN or PECS there will likely be a minimum of one, and often, multiple NOFs;
- A NOF will manage or oversee at least one SCF and/or multiple lower order elements;
- A NOF may manage functions supporting different vendor SCFs or lower order elements (e.g. Cloud Orchestration);
- Not all SCF or lower order elements will have or need a NOF. Particularly in the case of a small-scale deployment. However, as there is no Operational NOF careful consideration may be needed when addressing automation and management plane measures in the CoP.

There may also be cases where other OSS platforms, not primarily managing SCF or Lower order elements become an Operational NOF or even a SCF:

- Platform has privileged access to a NOF or SCF that can make material changes that could impact the operation of the PECN/S. For example, automated fault management, network healing, vulnerability and patch management solutions

Providers will therefore need to conduct their own risk assessment to undertake a sufficiently robust analysis to determine whether these platforms are in scope of TSA.

Figure 6, below, additionally introduces the concept of *"lower order elements"*. These are elements within scope (part of the Providers PECN) that would typically not be considered as an SCF, but which may, for various reasons, be managed or overseen by something which could be considered as a NOF.

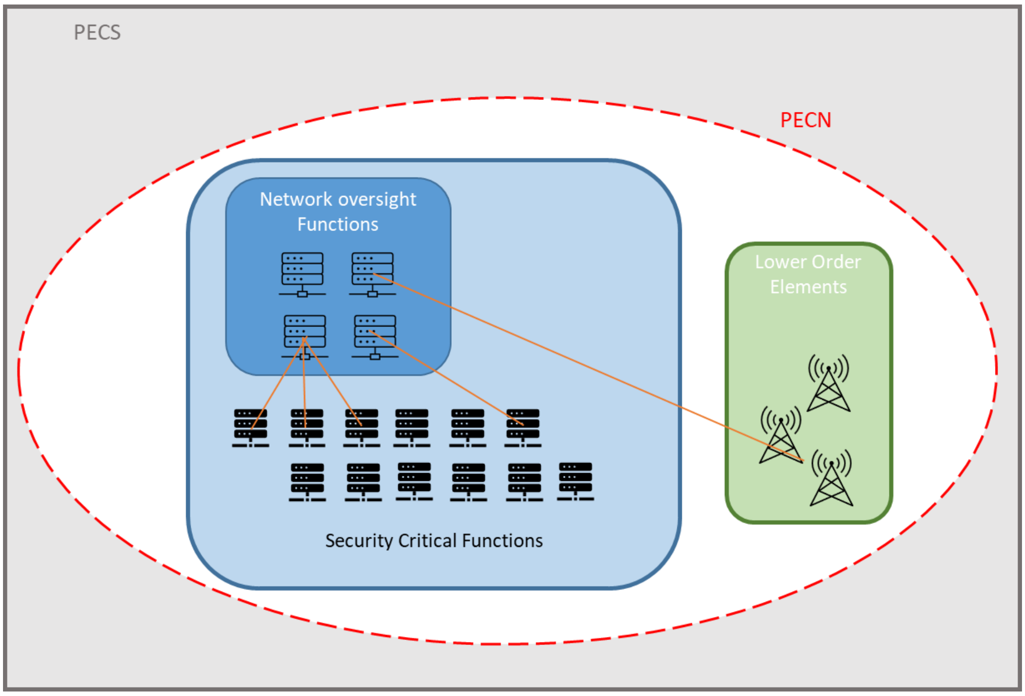

Figure 6 - Relationship diagram between Operational NOFs, SCFs and Lower Order Elements

The following is also a useful (but non-exhaustive) checklist. An element is likely to be an operational NOF if it meets any of the following criteria:

- It is essential for visibility and understanding of a PECS or PECN; **or**
- It is essential to recover, in any way, a PECS or PECN; **or**
- It enables a user to stop/degrade a PECS or PECN; **or**
- It enables a user to breach confidentiality, integrity or availability of a PECS or PECN.

6.2 Security NOF

To maintain the security of the PECN/S a number of security appliances, systems and tools will be deployed. As they are protecting the NOFs and SCFs, there is a high risk that if compromised there would be a material impact on the network. There is no hierarchy for these tools, but careful consideration should be taken to how they are deployed, and the Provider is recommended to follow the guidance in Section 2 - Key Concepts of the CoP [4].

6.3 Audit/Monitoring NOF

These could include a broad collection of OSS and security tools primarily used for security event monitoring and storage (e.g. SIEM), and detailed customer communication traffic (Signals) analysis. Provider will need to complete their own risk assessment to determine whether any platforms come into scope.

7 Proposed criteria for determining assessment of 'lower order elements'

It has been identified that there are elements of a Providers PECN/S, that may be considered within the scope of the TSA but may not be considered an SCF, as individually these elements may not have a material impact on the operation of the network; however, when aggregated the overall security risk to the PECN/S is increased causing any centralised management or oversight function to be considered a NOF (See Figure 6).

Generally, 'lower order elements' are designed to be deployed in large numbers often in the exposed edge and could include elements like Mobile eNodeBs and Broadband OLTs. However, the determination as to whether an element is considered a 'lower order element' or SCF is dependent on the security architecture deployed in the Provider.

Example 1: A single eNodeB in a mobile network may be considered as either a 'lower order element' or an SCF and determining this classification will be heavily dependent on how the Provider has architected their network and if any security compromise could enable an attacker:

- To materially impact the overall network or service (or a material part) where it would be considered an SCF; or
- If the security model deployed means there are no or limited risks to a material part of the network or service then it may not be considered an SCF.

However, there are many different network architectures and deployment models (e.g. lateral movement between eNodeBs or aggregation via relay modes) that need to be taken into consideration, so it's recommended that Provider always completes a risk assessment before making a final decision.

Providers will need to make their own decisions based on the considerations above.

Example 2: A switch through which a service is running is likely to be in scope, whereas the rack or building where the switch sits is likely to be an Associated Facility [4].

8 Scenarios and edge cases

The following (non-exhaustive) list of example and edge cases were discussed by Providers during the collation of this paper and are included to provide illustrative examples of considerations that Providers should make when determining whether something is an SCF or a NOF.

8.1 Is vulnerability management system a NOF or an SCF?

The answer is "it depends" and Providers will need to make their own determinations. However, data in a vulnerability management system should typically be considered as sensitive and appropriate protections given.

Part of the answer depends on the level of privilege given to the authentication scanners - the higher the privilege, the more likely it is that a Provider should consider a vulnerability management system as an SCF or even a NOF. By providing a system privileged access to an SCF or NOF, that system becomes in scope of TSA.

The answer also depends on how the Provider is using vulnerability management system – if automatic patching is enabled, then arguably a decision to view it as NOF is more compelling; whereas if a vulnerability management system is used to initiate further work (e.g. through automatic raising of a ticket) then it could be considered as neither an SCF nor a NOF.

8.2 What does OSS and BSS mean in the context of the TSA?

These terms have been and still are widely used in the Telecoms industry with a number of definitions available online. However, the terms originated from the ITU-T who developed the TMN (Telecommunications Management Network) series of standards (M.3000-M.3599) in 1988, allowing OSS and BSS vendors to standardise functionality (e.g. M.3703 - Managing alarms). Further work and promotion across the industry came from the Tele Management (TM) Forum's Telecoms Applications MAP (TAM).

Some Providers prefer to use the term Operations Administration and Maintenance (OAM), as defined in [7].

Some Providers may take a view that the OSS items to be considered as in-scope are only those element(s) that can provision services directly on the network itself.

There should be clear security boundaries between BSS and the trusted network functions, and it is recommended that risk-assessment based controls are applied to prevent and detect any abnormalities from BSS platforms that could impact PECS (e.g. mass/bulk provisioning events).

In this context, systems that provide elements like customer care or billing (may also be referred to as BSS) could be considered as out of scope, but it could be considered an Associated Facility [4]. Providers should evaluate whether there is separation from the PECN or PECS (of some logical and/or physical form or via a controlled interface, with some form of anomaly detection and recovery). The reasoning here being that technically a Provider can operate the PECN/PECS without billing, even if it may be commercially challenging over an extended period.

8.3 Further scenarios

These scenarios/edge cases are examples provided for illustrative purposes and are not intended to be definitive or exhaustive. Providers are encouraged to find ways to discuss edge cases and scenarios collaboratively through appropriate industry engagement. See table 2 below.

Service	Is it an ECS?	Is it Public?	Is it in scope?	Further clarification
Wi-Fi available in a consumer environment (e.g. coffee shop, train, retail store)	Yes	No if available only to closed user group/own SLA specified Yes if 'off the shelf' commercial offering	Subject to how it is accessed by users ('members of the general public')	Providers need to consider how the service is intended to be used (e.g. wi-fi on trains is only intended to be available to the closed user group of passengers on that train even if the signal MAY be available to others in the vicinity)
'Private' Services running over 'Public' Networks	Yes	No - closed user group and own SLA	No	
5G private networks	Yes	No	No	

Table 2 – Edge Case examples

8.4 Wholesale provision between regulated Providers

Where Provider A and Provider B are in a commercial relationship for provision of wholesale services in support of a PECN and PECS, four scenarios exist and are shown in table 3 below.

The following matrix tries to demonstrate where contract and compliance controls would be needed for each possible scenario.

		Wholesale service Provider	
		Non-TSA Regulated	TSA Regulated
Provider using wholesale service	Non-TSA Regulated	• N/A	If providing a PECN/S: • Compliance provided • Ofcom oversight • No evidence of compliance provided to non-TSA regulated Provider
	TSA Regulated	• Contract clauses (e.g. CoP M2.06) • How a regulated operator provides or demonstrates compliance, needs to be determined by each Provider	• No action unless different tiering levels where highest tiering level will have to be applied • Each party provides independent compliance submission to Ofcom

Table 3 - Contract and Compliance controls

Definition of regulated used in the above table:

- Regulated: A UK Operator who is providing PECN and PECS that require compliance under the Comms Act and more specifically the Telecoms Security Act.
- Non-TSA Regulated: Means a private network or service provided as a wholesale service (e.g. Managed private IP network or a Public Cloud Provider). Note: these could also be provided by TSA regulated Providers.

Note: Operators and Providers should note that the relative tiering of the Provider and consumer must be considered due to the difference in the tiering and the implementation dates of the CoP.

9 Future updates

This version of the document is specifically focused on helping Providers understand and interpret the terms PECN, PECS, SCF, NOF, and lower order elements in relation to the TSA, associated Regulations and the Code of Practice. It also introduces the concept of lower order elements.

It does not address issues related to:

- Installation (i.e. when does network equipment being installed come into scope and therefore TSA controls apply)
- Associated Facilities
- Exposed Edge.

These issues may be returned to at a later date and this document revised by NICC, subject to greater clarity around Ofcom's approach to monitoring and enforcement and/or further input to the discussion from Government stakeholders.

This ND will be re-issued when further information on Associated Facilities [4] and 'exposed edge' is available.

History

Document history		
Version	Date	Milestone
1.1.1	17th January 2024	Initial publication.