JOINT OPERATORS TECHNICAL SPECIFICATION

OF THE

NEUTRAL HOST IN-BUILDING

SMALL CELL SOLUTION

ANNEX 4

OPERATIONAL PROCESSES

SCOPE

This Annex defines the Operational Processes specification for the JOTS Neutral Host In-Building (NHIB) solution, capable of supporting cellular services for multiple Mobile Network Operators.

This Annex sets out the roles and responsibilities across three operational domains within the Neutral Host In-Building solution. Specifically, the **Operator Domain**, the **Neutral Host Domain** and the **Retailer Domain**.

PURPOSE

This specification will be used by *Operators*, *Neutral Hosts* and *Retailers* to implement instances of the Neutral Host In-Building solution. To assist in that task the overall specification is divided into a set of annexes, each covering a key aspect of the implementation:

- Annex 1 – Architecture
- Annex 2 – Radio Requirements
- Annex 3 – Testing and Acceptance
- Annex 4 – Operational Processes (**This document**)
- Annex 5 – Fulfilment

Each annex is separately version controlled. Collectively the latest versions of all the annexes define the JOTS Neutral Host In-Building specification.



JOTS (NEUTRAL HOST IN-BUILDING)

ANNEX 4
OPERATIONAL PROCESSES

DOCUMENT INFORMATION

Document Name:	JOTS NHIB Specification – Annex 4 – Operational Processes
Brief Description:	JOTS NHIB Specification
Document Author:	Katie Pontin (Vodafone)
Owner While Current:	Katie Pontin
Owner's Email Address:	katie.pontin@vodafone.com
Issue Date:	1st June 2022
Document contributor	David Morris (Virgin Media O2)
Document contributor	Andy Mildenhall (Virgin Media O2)
Document contributor	
Document contributor	

ACKNOWLEDGEMENT

This document is created with input and contributions from the current UK mobile network operators Virgin Media O2, Vodafone, BT/EE and Three.

TABLE OF CONTENTS

PARAGRAGH MARKINGS

Throughout this specification, the following paragraph markings are used:

M A mandatory and critical requirement that must be met by the solution. Details shall be provided stating how mandatory requirements have been met within any proposed solution.

R A requirement of the specification. These are to be considered mandatory to the extent that non-compliance will require the *Neutral Host* to provide to the *Operator* (or visa-versa) specific justification as to why they are not compliant to the requirement.

I Informative statement, providing either points of clarification or a statement relating to implementation good practice.

GLOSSARY AND ABBREVIATIONS

AMF	Access and Mobility Management Function (5G core element)
b-interface	Interface between the **Neutral Host Domain** and the **Operator Domain**
BAU	Business As Usual
BTS	Base Station (e.g. picocell, eRAN cell, femtocell)
CAS-T	CESG ASSURED SERVICE (TELECOMMUNICATIONS)
CESG	COMMUNICATIONS-ELECTRONICS SECURITY GROUP
CLI	Command Line Interface
Controller	Aggregation unit (services node) for multiple BTS
CPE	Customer Premises Equipment (switches and routers)
DL	Downlink
eNodeB	4G base station
E-RAN	Enterprise Radio Access Network
ESN	Emergency Services Network
f-interface	Interface between the **Retailer Domain** and the **Neutral Host Domain**
gNodeB	5G base station
HeNB-GW	Home eNodeB Gateway
JOTS	Joint Operator Technical Specification (forum of UK MNOs)
KPI	Key Performance Indicator
LAN	Local Area Network
MEN	Metro Ethernet Network (high quality, guaranteed bandwidth)
Mgmt	Management
MME	Mobility Management Entity (4G core element)
MB	Megabyte
MNO	Mobile Network Operator
MTPAS	Mobile Telecommunication Privileged Access Scheme
NG	5G interface between gNodeB and AMF/UPF
NHIB	Neutral Host In-Building
NTE	Network Termination Equipment (backhaul provider)
PRB	Physical Resource Block
PKI	Public Key Infrastructure
S1	4G interface between eNodeB and MME/SGW
SecGW	Security Gateway (terminates IPSec tunnel end points)
SGW	Serving Gateway (4G core element)
TACACS+	Terminal Access Controller Access Control System Plus
Tier-1***b*** SecGW	***b***-interface security gateway (in **Neutral Host Domain**)
Tier-1***f*** SecGW	***f***-interface security gateway (in **Neutral Host Domain**)
Tier-2 SecGW	***b***-interface security gateway (in **Operator Domain**)
UL	Uplink
UPF	User Plane Function (5G core element)

1 INTRODUCTION

The JOTS Neutral Host In-Building (NHIB) Operational Processes Annex defines the in-life management requirements needed to support JOTS NHIB deployments.

This specification includes the mandatory Operational Processes which are necessary to sufficiently support industrialisation of an in-building multi-operator small cell solution managed from within the **Neutral Host Domain.**

Solution requirements included within this document are assigned to the appropriate domains, of which the domain areas include: the **Retailer Domain**, **Neutral Host Domain** and **Operator Domain**. The assigned requirements are to be fulfilled by the stated domains.

The Operational Processes specification should provide a framework for management of varying vendor radio solutions, whereby the operational requirements included will be agnostic to support an open volume of radio solutions and *Neutral Host* entities.

This is a working document which will be updated by the JOTS forum as and when required to cater for modernised management processes and technological advances.

2 DOMAINS

1. I The Neutral Host In-Building (NHIB) deployment is separated into three domains: the **Retailer Domain**[1], the **Neutral Host Domain** and the **Operator Domain**, with the key areas of responsibility as shown in *Figure 2-1*:

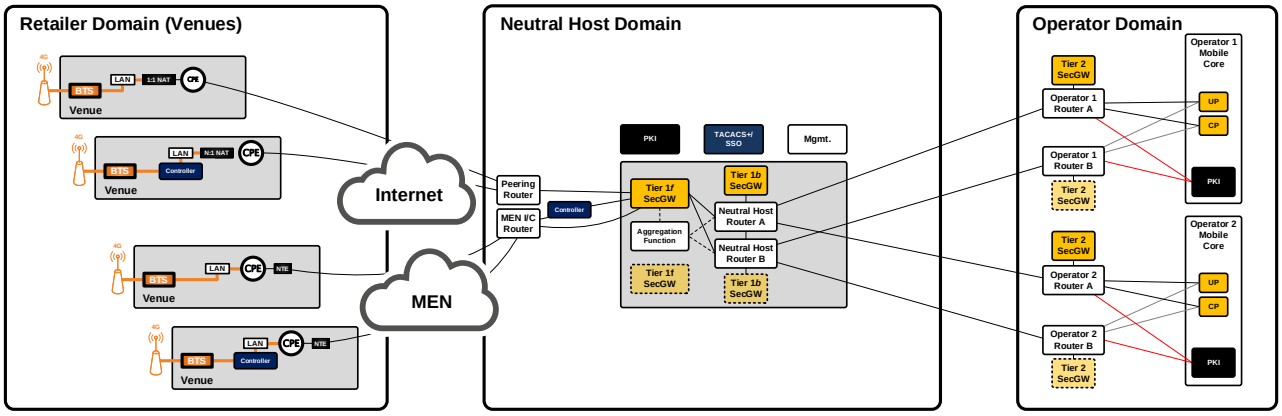

Figure 2-1 - Domain Overview

2. I The following high-level statements can be made to describe the operational processes for the *Retailer* within the **Retailer Domain**:

- The *Retailer* is responsible for maintaining and securing the BTS equipment and ***f***-interface at the venue.
- The *Retailer* is the first point of contact for the venue owner.

3. I The following high-level statements can be made to describe the operational processes for the *Neutral Host* within the **Neutral Host Domain**:

- The *Neutral Host* is responsible for maintaining, securing and operating the NHIB platform within their data centre.
- The *Neutral Host* is responsible for maintaining the ***b***-interface to the point-of-interconnect with each hosted *Operator*.
- The *Neutral Host* is the first point of contact for queries raised within the **Retailer Domain**.
- The *Neutral Host* is responsible for maintaining an inventory of BTS installations.
- The *Neutral Host* is responsible for implementing emergency BTS lock-down requests.
- The *Neutral Host* is required to follow an agreed change and fault management process with each hosted *Operator*.

[1] For the avoidance of doubt, a *Retailer* within the **Retailer Domain**, in this context, is not a 'shop', but an entity whose commercial model is built around providing in-building coverage solutions to venues.

4. I The following high-level statements can be made to describe the operational processes for the *Operator* within the **Operator Domain**:

- The *Operator* is the contact for queries raised by the *Neutral Host*.
- Each hosted *Operator* acts as a certificate authority for the purposes of securing their ***b***-interface links to *Neutral Hosts*.

2.1 High Level NHIB Operational Process Overview

5. I It is suggested that the *Retailer*, *Neutral Host* and *Operator* align their high-level BAU operational processes to that shown in *Figure 2-2*, fulfilling reporting (including meetings between *Neutral Hosts* and *Operators*), trouble ticketing (triggered by 'issues') and upgrades (modifications/changes).

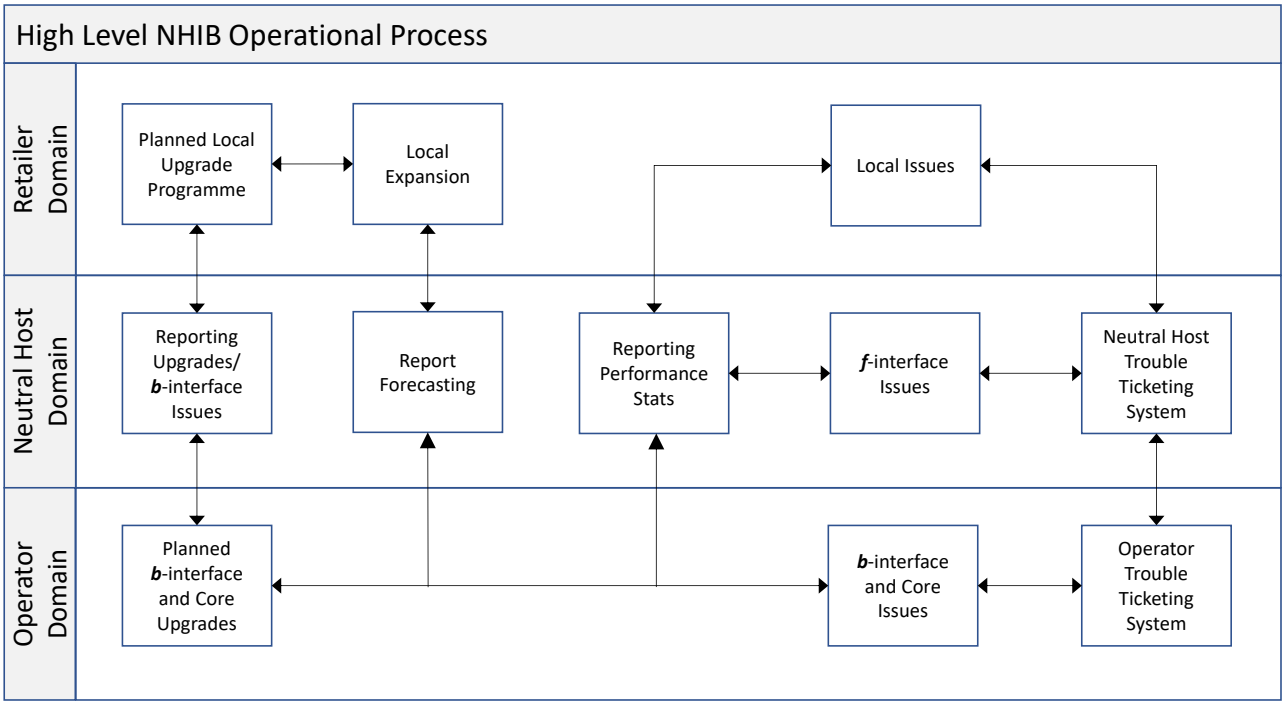

Figure 2-2. - BAU Operational Processes

6. I The operational processes within the **Retailer Domain** include local (venue) capacity planning and fault reporting towards the *Neutral Host*.

7. I The operational processes within the **Neutral Host Domain** include monitoring and managing capacity upgrades within the **Retailer Domain** and reporting those capacity upgrades to the *Operator*. The *Neutral Host* is also responsible for forward capacity planning and reporting those forecasts in a timely manner to the *Operator*. Where faults are identified by the *Neutral Host*, either within the **Neutral Host Domain** or **Retailer Domain**, these faults should be registered on their trouble ticketing system and, if necessary, also registered on the *Operator's* trouble ticketing system (where the *Operator* is required to take remedial action). Generally, the *Neutral Host* will regularly report performance and availability (potentially caused by faults) to the *Operator*.

8. I The operational processes within the **Operator Domain** include planning core and ***b***-interface upgrades according to the forecasts received from *Neutral Hosts*. The *Operator* will register faults within the **Operator Domain** on their internal trouble ticketing system. Where a fault is detected in the **Neutral Host Domain** or **Retailer Domain** then a fault ticket will be raised on the *Neutral Host* trouble ticketing system also. Performance stats collected within the **Operator Domain** might be shared with the *Neutral Host*, particularly if there are shortfalls in meeting KPIs where the *Operator* is requesting the *Neutral Host* to rectify.

2.2 Site Termination Process

9. I It is suggested that the *Retailer*, *Neutral Host* and *Operator* align to the site termination process shown in *Figure 2-3* to deactivate and decommission sites.

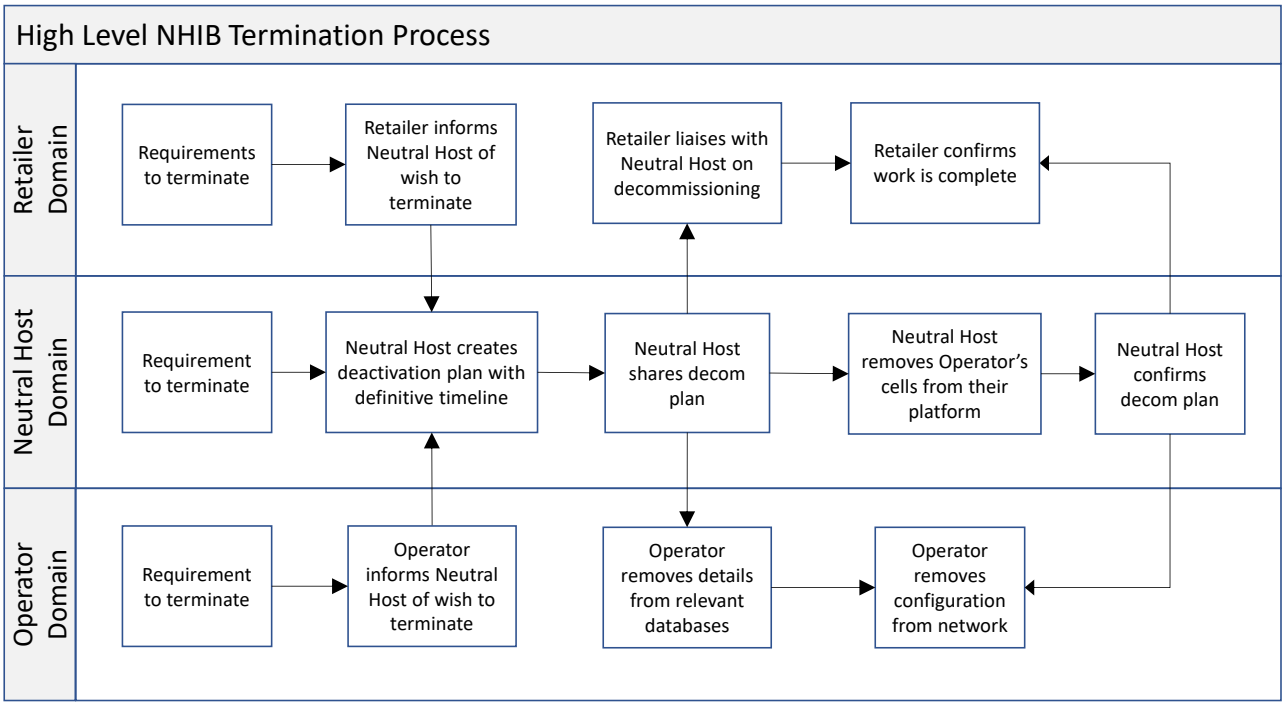

Figure 2-3. Site Termination Process

10. I The termination processes within the **Retailer Domain** requires the *Retailer* to either trigger a site termination or liaise with the *Neutral Host* who is requesting a site to be terminated. The *Retailer* confirms to the *Neutral Host* when the site is decommissioned and removed from the venue.

11. I The termination processes within the **Neutral Host Domain** requires the *Neutral Hos*t to either trigger a site termination or liaise with either the *Retailer* or *Operator* who is requesting a site to be terminated. The *Neutral Host* builds a decommissioning plan and collaborates with the *Retailer* to execute that plan. The *Neutral Host* informs the *Operator* when the site is decommissioned and removed from the venue.

12. I The termination processes within the **Operator Domain** requires the *Operator* to either trigger a site termination or liaise with *Neutral Host* who is terminating a site. Once the *Neutral Host* has decommissioned and removed the site from the venue the *Operator* removes the site from their network configuration and databases.

3 OPERATIONAL AREAS

3.1 Roles & Responsibilities

13. M The *Retailer* must maintain all equipment at the venue, which will typically include NTE, switches/routers, Controllers, BTS and antenna systems.

14. M The *Retailer*[2] must maintain the ***f***-interface between the venue and **Neutral Host Domain**.

15. M The *Neutral Host* is responsible for operating the HeNB GW or S1/NG aggregation function.

16. M The *Neutral Host* is responsible for operating the Tier-1***b*** SecGW (resilient pair).

17. M The *Neutral Host* is responsible for operating ***b***-interface (resilient pair) to the point of interconnect with the *Operator*.

3.2 Points of Contact

18. M The *Retailer* is the point of contact for queries raised by the venue owner.

19. M The *Neutral Host* is the point of contact for queries which arise within the **Retailer Domain**.

20. M The *Neutral Host* is the point of contact for queries raised by the *Operator* for both the **Retailer Domain** and **Neutral Host Domain**.

21. M The *Operator* must be provided with a point of contact by the *Retailer* for each venue within the **Retailer Domain**.

[2] It is recognised that the *Retailer* could, and often will, be the same commercial entity as the *Neutral Host* (i.e. a single commercial entity will operate as both *Retailer* and *Neutral Host*). In this case the *Retailer* responsibilities transfer to the *Neutral Host*. Likewise, if a 3rd party *Neutral Host Provider* is employed to work in the **Retailer Domain** on behalf of the *Neutral Host* then, again, the *Retailer* responsibilities transfer to the *Neutral Host*.

22. I The *Operator* is the point of contact for queries arising within the **Neutral Host Domain**.

3.3 Regulatory Obligations

23. M The *Neutral Host* and the *Retailer* are responsible for providing a process such that the NHIB deployments provided by the *Neutral Host* remains TSCoP[3] compliant and supports MTPAS, zone-code shutdown and provides the capability to complete Access Class Barring when exercised.

3.4 Physical Security

24. R In instances where a BTS Controller is deployed at the venue, the *Retailer* is required to ensure it remains hosted in a secure (lockable) room or within a lockable cabinet and access to the secure location is sufficiently managed.

25. M The *Neutral Host* will only allow permitted staff to access secure buildings and locked cabinets.

26. M The *Retailer* will ensure only permitted staff are able to access the secure room or locked cabinet.

27. M The *Operator* must only allow permitted staff to access secure buildings.

3.5 Kit Inventory

28. M The *Operator* must maintain a database/inventory covering all *Neutral Host* providers and the location of all BTS. The inventory must include: equipment type, frequency/operating bands, ***b***-interface bandwidth used and sites noted as decommissioned.

29. M The *Neutral Host* must continually maintain a list of all BTS locations per *Operator*, including (as a minimum): equipment type, frequency/operating bands deployed and ***b***-interface bandwidth used.

30. M The *Retailer* must maintain an inventory of all BTS and switch gear deployed at each venue, including kit type and ***b***-interface provided.

31. M The *Retailer* must agree all relocations of BTS equipment within a venue with the *Neutral Host*.

[3] Draft Telecommunications Security Code of Practice and Telecommunications (Security) Act 2021 (legislation.gov.uk).

32. M The *Neutral Host* must inform and obtain agreement from each hosted *Operator* for any proposed relocations of BTS equipment within a venue.

3.6 Site Numbering

33. M The *Neutral Host* is responsible for maintaining a common site name for each venue deployment (as defined in Annex 5 - Fulfilment) and will, within their internal databases, associate that common site name with the internal naming convention used (and provided to the *Neutral Host*) by each hosted *Operator*. The common site name and associated *Operator* name must be used to uniquely identify each site for the purposes of reporting, change or fault management or decommissioning.

3.7 *f*-interface

34. M The *Neutral Host* must proactively plan HeNB-GW capacity, S1/NG aggregation and Tier-1***f*** SecGW capacity through forward planning. The review period for capacity planning will typically be agreed between each hosted *Operator* and the *Neutral Host*, however in the absence of any agreement the *Neutral Host* must declare their forward capacity plans on an annual basis as a minimum.

35. M The *Neutral Host* must reactively alert the *Retailer* of detected shortfalls in ***f***-interface capacity when first identified.

36. M The *Retailer* must inform the *Neutral Host* of any planned or implemented ***f***-interface capacity upgrades.

37. M The *Neutral Host* must inform the *Operator* of any planned or implemented ***f***-interface capacity upgrades.

38. M The *Retailer* must proactively and reactively manage ***f***-interface capacity.

39. M The *Retailer* must install ***f***-interface capacity regrades as and when required.

3.8 *b*-interface

40. R The *Operator* will proactively manage ***b***-interface connectivity from the point of interconnect with the *Neutral Host* and Tier-2 SecGW capacity.

41. R The *Operator* will reactively manage ***b***-interface connectivity from the point of interconnect with the *Neutral Host* and Tier-2 SecGW capacity as and when required.

42. M The *Neutral Host* is responsible for proactively managing ***b***-interface from the point of interconnect with the *Neutral Host* and Tier-1***b*** capacity through forward planning. The review period for capacity planning will typically be agreed between each hosted *Operator* and the *Neutral Host*, however in the absence of any agreement the *Neutral Host* must declare their forward capacity plans on at least an annual basis.

43. M The *Neutral Host* must inform the *Operator* of any planned or implemented ***b***-interface capacity upgrades.

4 Operational Management

4.1 Management Platform

44. R The *Operator* will maintain a list of authorised personnel who are approved to access the *Neutral Host* platform from the **Operator Domain**.

45. M The *Neutral Host* is responsible for maintaining a registered list of authorised tenants which have been issued by each *Operator* (tenant), of which these users have been approved to access the management platform. For each personnel approved to access the platform the associated *Operator* will be assigned to control the roles each individual can fulfil.

46. M The *Neutral Host* will authorise and maintain access for specified users and assign their roles to manage the actions each user can complete, as defined by the *Operator*.

4.2 BTS Shutdown

47. M Where the *Neutral Host* is responsible for locking cells for the hosted *Operator*, the *Operator* will instruct the *Neutral Host* as to when an emergency BTS lock-down must be executed.

48. M On completion of an emergency BTS lock-down the *Neutral Host* will inform the *Operator* that the request was executed successfully.

49. M If the *Neutral Host* fails to carry out or fails to confirm a cell lock within an agreed time period following the issuing of the instruction from the hosted *Operator*, that *Operator* may opt to disconnect the *Neutral Host* (and thus take cells off-air) by tearing down the ***b***-interface (aggregated S1/NG) link.

50. M Where the *Operator* has direct management access to the NHIB platform for the purposes of locking their cells immediately by CLI command then the *Operator* will inform the *Neutral Host* of their intent to lock cells or will inform the *Neutral Host* within an agreed time period that cells have been locked.

51. M The *Neutral Host* must ensure a locking feature is available to facilitate locking of specific bands on a BTS or the entire BTS. Band locking will be available on a per *Operator* basis when *Operators* share BTS equipment.

52. M The *Operator* will provide zone-code information as part of any emergency lock-down requests that are initiated.

53. R The *Neutral Host* will carry out a non-emergency BTS lock-downs according to an agreed change management process as agreed separately with each hosted *Operator*.

54. R The *Operator* is to provide the *Neutral Host* with a justified reason for initiating a non-emergency lock-down request.

55. M For non-emergency BTS lock-down operations which are scheduled the *Neutral Host* will inform the **Retailer Domain** of the plans to complete the activity.

4.3 Certificate Management

56. M The *Operator* will distribute Tier-1***b*** certificates to the *Neutral Host*.

57. M The *Operator* will act as a Certificate Authority for certificates used to secure the ***b***-interface links between Tier-2 and Tier-1***b*** SecGWs.

58. M The *Operator* will operate a PKI able to authenticate/re-authenticate certificates used to secure ***b***-interface links.

59. M The *Operator* will revoke compromised or out-of-date certificates accordingly.

60. M The *Neutral Host* will load *Operator* certificates on to Tier-1***b*** SecGWs.

61. M The *Neutral Host* will remove revoked certificates from the Tier-1***b*** SecGWs when required.

62. M The *Neutral Host* will operate a PKI to secure ***f***-interface connections to BTS and/or BTS controllers.

4.4 Change Management

63. M The *Operator* is required to inform the *Neutral Host* of Service Protection periods (no change period) which are planned.

64. M The *Operator* is required to inform the *Neutral Host* of any foreseen or planned parameter changes on either the core network, transport layer or radio layers. Where the changes of NHIB RAN parameters for an individual *Operator* are required, subject to the condition that the other hosted *Operators* sharing the same BTS equipment are not affected by the changes, the *Neutral Host* will be responsible for implementing the change request.

65. M The *Operator* will inform the *Neutral Host*, according to an agreed notice period, of any relevant outages planned for the 4G and/or 5G core network, including a description of the outage.

66. M The *Neutral Host* must inform *Operators*, according to an agreed notice period, of any outages planned on the HeNB-GW or S1/NG aggregation functions or outages planned at the venue, whereby the *Neutral Host* will provide a description of the outage and agree the outage with all impacted hosted *Operators*.

67. M The *Neutral Host* must outline all sites which will be impacted by the outage.

68. M The *Neutral Host* must state the start and end time of a planned outage.

69. M The *Neutral Host* must inform the *Operator* of any parameter changes to the transport or radio layers.

70. M The *Retailer* must inform the *Neutral Host* of any planned outages, either per BTS, per BTS controller or per venue.

71. M The *Neutral Host* must inform the *Operator* of any planned outages within the **Retailer Domain**.

4.5 Configuration Management

72. R The *Operator* is required to configure core network parameters.

73. R The *Operator* is required to inform the *Neutral Host* of any changes or updates to the *Operator* defined NHIB RAN parameters.

74. R The *Operator* may optionally monitor filters and alarms to identify significant changes which have been made to the *Neutral Host* system.

75. M The *Neutral Host* is responsible for maintaining NHIB RAN parameters on their deployed BTS kit.

76. M The *Neutral Host* will maintain a Configuration Management platform for all components controlled by the *Neutral Host*.

77. M The *Neutral Host* must manage BTS certificates via their PKI.

78. M The *Neutral Host* must issue the syslog feed from the Tier-1***b*** SecGW to the *Operator*.

79. M The *Retailer* must ensure on-site equipment can either be managed via a local comms port or via a remote access method.

4.6 Fault Management

80. M The *Neutral Host* will monitor alarms on all components controlled by the *Neutral Host* within the **Neutral Host Domain** and **Retailer Domain** and triage faults when identified.

81. M The *Operator* will monitor alarms on all components controlled within the **Operator Domain** and triage faults when identified.

4.7 Trouble Ticketing

82. M The *Operator* will raise a trouble ticket towards the *Neutral Host* when a fault is detected within the **Neutral Host Domain** or **Retailer Domain**.

83. M The *Operator* will ensure to keep an up-to-date contact telephone number for immediate trouble ticket registration/response/query.

84. M The *Neutral Host* will raise a trouble ticket towards the *Operator* when a fault is detected within the **Operator Domain**.

85. M The *Neutral Host* will maintain a process where both the *Operator* and *Retailer* can register trouble tickets within the **Neutral Host Domain** for investigation and resolution.

86. M The *Neutral Host* will ensure that the NMC contact telephone number for expediting trouble tickets or when an emergency or non-emergency BTS lock-down is kept up to date.

87. M The *Retailer* must raise a trouble ticket towards the *Neutral Host* when a fault is detected within the **Neutral Host Domain** or **Operator Domain**.

4.8 Spare Parts

88. M The *Neutral Host* will provide or advise on BTS/BTS controller/switch gear replacements to the **Retailer Domain** as and when required.

89. M The *Retailer* will replace faulty BTS, BTS controllers and/or switching at the venue as and when required.

4.9 Performance Monitoring

90. M The *Neutral Host* will report, as a minimum, separately to each hosted *Operator*, at an agreed frequency (e.g. hourly) and at an agreed level of aggregation (e.g. venue level, controller or BTS level), the following stats:

- Voice traffic [Erlangs].
- Data traffic [downlink MB].
- Data traffic [uplink MB].
- Number of voice calls attempted.
- Number of voice calls connected.
- Number of voice calls dropped.
- Number of data calls attempted.
- Number of data calls connected.
- Number of data calls dropped.
- Number of outgoing (to macro) handovers attempted.
- Number of outgoing (to macro) handovers successes.
- Number of inter-BTS (in-building) handovers attempted.
- Number of inter-BTS (in-building) handovers successes.
- Number of connected and active users.
- Average and Peak DL/UL cell and user throughput.
- Average and Peak DL/UL PRB usage.

91. R Any additional aggregated performance stats provided by the *Neutral Host* are to be mutually agreed by the *Neutral Host* and each hosted *Operator*.

4.10 Key Performance Indicators

92. R Where a hosted *Operator* has not specified and agreed KPI targets (which could be venue specific) for the *Neutral Host*, the *Neutral Host* must, as a minimum, meet the KPI target levels as set out in Table 1.

Table 1 – *Minimum Performance Metrics*

Performance Metric	Acceptance Threshold
Availability	> 98%
Data Call Dropped Rate	< 2%
Voice Call Dropped Rate	< 2%
Data Call Setup Success Rate	> 98%
Voice Call Setup Success Rate	> 98%
Handover (outgoing to macro) Success Rate	> 95%

93. R The *Operator* is responsible for requesting any additional KPIs to be provided by the *Neutral Host*.

94. M The *Neutral Host* will continually provide the *Operator* with specific KPIs as per the agreement between the *Neutral Host* and each hosted *Operator*.

4.11 Site Decommissioning

95. I If a site is identified as causing interference issues or its performance is not meeting the desired thresholds, the *Operator* will request the *Neutral Host* investigate the issue and if resolution is not possible the *Operator* will issue a site lock-down and termination request.

96. I As and when a site follows the decommissioning process the *Operator* will delete the locked-down site from their internal databases.

97. M The *Neutral Host* will collate a per *Operator* Decommissioned Site list and distribute to all impacted *Operators*.

98. M The *Operator* will request (as and when required) to lock-down sites to be decommissioned, whereby this could be defined for completion on a specified date.

99. M The *Neutral Host* will delete specified sites following lock-down.

100. M If a lock-down decommission request is received from the *Operator* relating to poor BTS performance the *Neutral Host* will review the site and decide to either resolve performance issues or decommission the site.

101. M The *Retailer* will identify BTS/BTS controller/venues which are required to be decommissioned and alert the *Neutral Host*, providing a 1-month notice period. Following site deletion, the *Retailer* will arrange for the onsite kit to be recovered from the venue.

--- End of Document ---