JOINT OPERATORS TECHNICAL SPECIFICATION

OF THE

NEUTRAL HOST IN-BUILDING

SMALL CELL SOLUTION

ANNEX 3

TESTING AND ACCEPTANCE

SCOPE

This annex of the JOTS NHIB specification covers the testing and acceptance processes for a Neutral Host In-Building solution capable of supporting cellular services for multiple Mobile Network Operators.

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 (**This document**)
- Annex 4 – Operational Processes
- 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 3
TESTING AND ACCEPTANCE

DOCUMENT INFORMATION

Document Name:	JOTS NHIB Specification Annex 3 – Testing and Acceptance
Brief Description:	JOTS NHIB Specification
Document Author:	David Morris (Telefonica UK)
Owner While Current:	David Morris
Owner's Email Address:	david.morris@telefonica.com
Next Review Date:	TBC
Retention Period:	TBC
Document contributor	
Document contributor	
Document contributor	
Document contributor	

CHANGE HISTORY

Tool Used	Microsoft Word 2007		
Version	**Date**	**Changed By**	**Changes**
0.1	05/09/19	David Morris	Original draft.
0.2	10/09/19	David Morris	Corrected heading numbering bug.
0.3	19/09/19	David Morris	Tidied up.
0.4	13/02/20	David Morris	Aligned to Annex 1 structure.
0.5	28/04/20	David Morris	Editorial changes following all-MNO review on 23/04/20.
0.6	12/05/20	David Morris	Created Advanced Draft based on feedback from all MNOs.
1.0	23/10/20	David Morris	Minor edits for final version.

ACKNOWLEDGEMENT

This document is created with inputs and contributions from the current UK mobile network operators Telefonica UK (O_2), 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

802.1p	Priority marker for (layer 2) Ethernet frames
Aggregation Function	A device capable of aggregating S1 connections
b-interface	Interface between **Neutral Host Domain** and **Operator Domain**
BGP	Border Gateway Protocol
BTS	Base Station (e.g. picocell, eRAN cell, femtocell)
CAS-T	CESG ASSURED SERVICE (TELECOMMUNICATIONS)
CESG	COMMUNICATIONS-ELECTRONICS SECURITY GROUP
CM	Configuration Management
C-NAME	Canonical Name (in a DNS system)
Controller	Aggregation unit (services node) for controlling and aggregating multiple BTS
DEV	Instance of a development NHIB platform connected to one or more Operator test core networks.
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DWDM	Dense Wavelength Division Multiplexing
eBGP	Edge BGP
f-interface	Interface between **Retailer Domain** and **Neutral Host Domain**
FM	Fault Management
FQDN	Full Qualified Domain Name
I/C	Inter-connecting (router)
IKE-SA	Internet Key Exchange – Security Association
IP	Internet Protocol (layer 3)
IPSec	IP Security protocol (encrypted packet transmission)
IPv4	Internet Protocol (Layer 3 packet switching) Version 4
JOTS	Joint Operator Technical Specification (technical forum attended by UK MNOs)
LAN	Local Area Network
LIVE	Instance of a live NHIB platform connected to one or more Operator live core networks.
MEN	Metro Ethernet Network (high quality, guaranteed bandwidth)
Mgmt	Management
MME	Mobility Management Entity (4G core element)
MNO	Mobile Network Operator
MSC	Mobile Switching Centre (4G core element)
NAPT	Network Address and Port Translation
NAT	Network Address Translation (IP layer 3)
NHIB	Neutral Host In-Building
NTE	Network Termination Equipment (backhaul provider)
OSS	Operations Support System
PKI	Public Key Infrastructure
PM	Performance Management
QoS	Quality of Service
RBAC	Role Based Access Control (management interface)
ROADM	Reconfigurable Optical Add Drop Multiplexor
S1	4G interface between eNodeB and SGW
S1-AP	S1 Application Protocol (carries user plane traffic)
S1-CP	S1 Control Protocol (carries signalling traffic)

S1-U	S1 User Plane
SA	Security Association
SCTP	Stream Control Transmission Protocol
SecGW	Security Gateway (terminates IPSec tunnel end points)
SGW	Serving Gateway (4G core element)
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
Tier 1b SecGW	***b***-interface security gateway (within **Neutral Host Domain**)
Tier 1f SecGW	***f***-interface security gateway (within **Neutral Host Domain**)
Tier 2 SecGW	***b***-interface security gateway (within **Operator Domain**)
TS	Traffic Selectors (within IPSec flow)
VLAN	Virtual Local Area Network
VRF	Virtual Routing Function
VSO	Vendor Specific Option (in DHCP protocol)
xDSL	Digital Subscriber Line (generic)

1 INTRODUCTION

The JOTS Neutral Host In-Building (NHIB) architecture specification sets out the central principles of the NHIB concept.

The JOTS NHIB architecture is split into the **Retailer Domain**, **Neutral Host Domain** and **Operator Domain**. Testing and Acceptance responsibilities within each domain are defined in this Annex.

The aim of this Annex is to provide a testing framework to enable a *Neutral Host* to move a 'development' platform into a 'live' platform configuration, which can then subsequently carry commercial traffic for one or more *Operators*.

The JOTS NHIB specification is expected to be an evolving specification which will be updated as and when required (by the JOTS forum) to maintain alignment and relevance with new technologies and developing vendor capabilities.

This specification provides guidance from UK MNOs as to how testing and acceptance procedures should be undertaken to provide an ongoing NHIB solution. It should not be taken as a commitment from the *Operators* that such facilities will be available at the time of publication. Additional *Operator*-specific requirements will need to be discussed with UK MNOs individually. Those looking to operate a NHIB solution (either in the **Retailer Domain**, **Neutral Host Domain**, or both) should engage with all *Operators* with this guideline as a starting point.

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*:

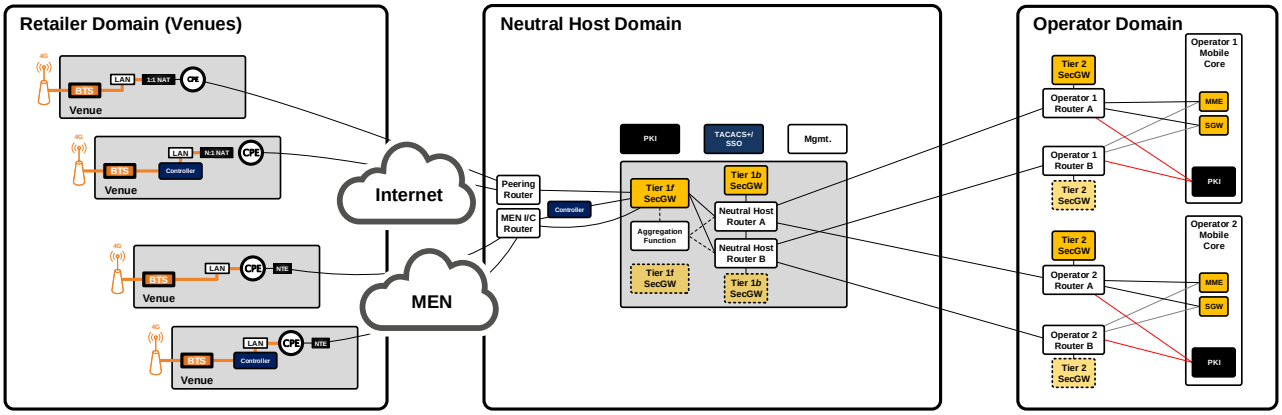

Figure 2-1 - Domain Overview

A number of possible radio architectures are achievable depending on the needs of the selected radio solution and on the aggregation requirements of the **Operator Domain**. Example radio architectures are shown in *Figure 2-2*, *Figure 2-3*, *Figure 2-4*, *Figure 2-5* and *Figure 2-6*. For illustrative purposes, the wavy line depicts the traffic path adopted for each radio architecture option.

A *Neutral Host* would select and operate one or perhaps multiple radio architectures, however it is not necessary for a *Neutral Host* to implement *all* types of radio architecture.

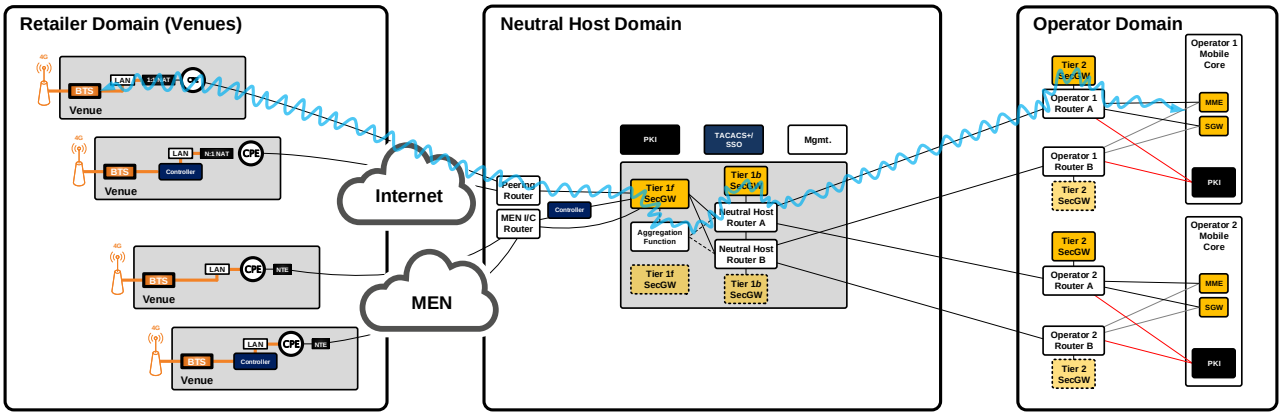

Figure 2-2. Internet f-interface with traffic aggregation in Neutral Host (Aggregation Function) Domain only.

[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.

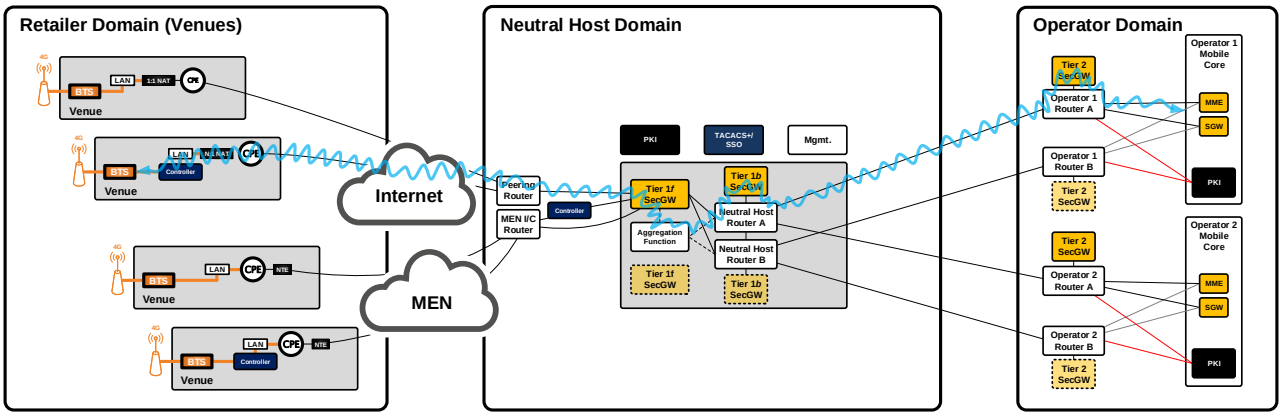

Figure 2-3. Internet f-interface with traffic aggregation in both Retailer (Controller) and Neutral Host (Aggregation Function) Domains.

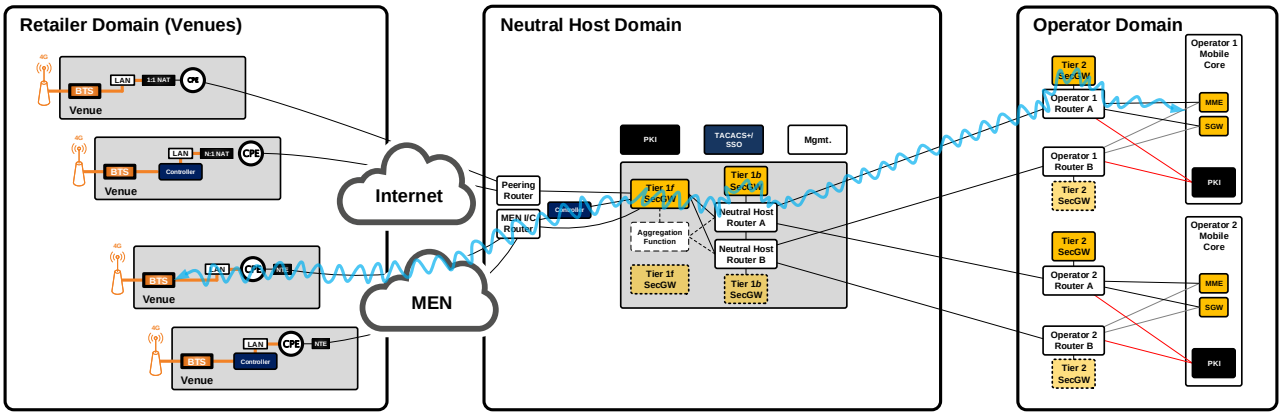

Figure 2-4. MEN f-interface with traffic aggregation in Neutral Host (Controller) Domain only.

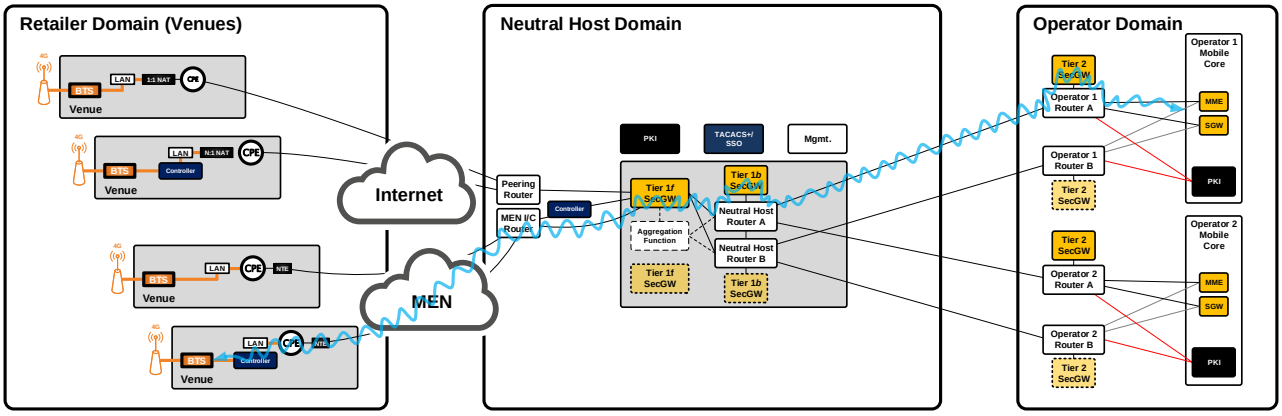

Figure 2-5. MEN f-interface with traffic aggregation in Retailer (Controller) Domain only.

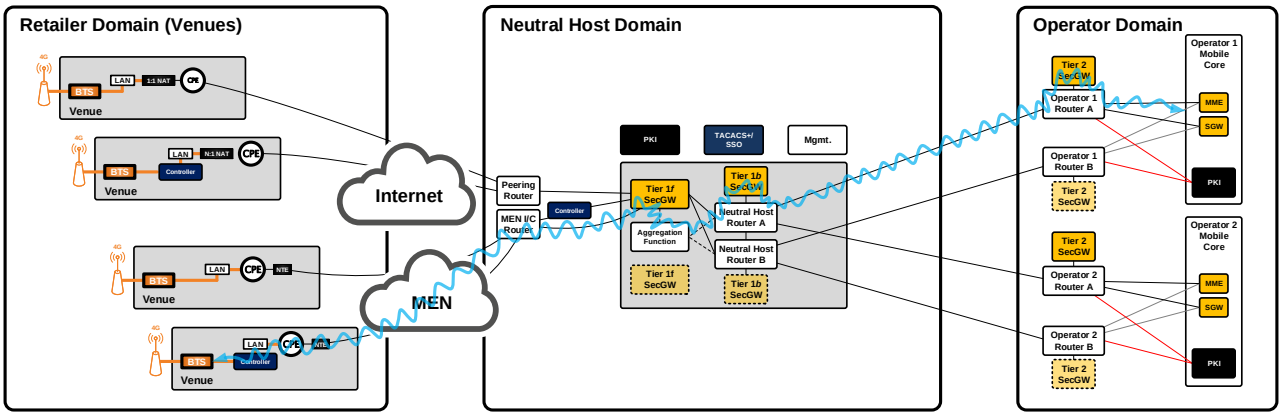

Figure 2-6. MEN f-interface with traffic aggregation in both Retailer (Controller) and Neutral Host (Aggregation Function) Domains.

2. I The following high-level statements can be made to describe the testing and acceptance responsibilities of the *Retailer* within the **Retailer Domain**:

- The *Retailer* is responsible for any testing carried out on BTS equipment within the **Retailer Domain** (i.e. venues). Testing within the **Retailer Domain** is specified in Annex 2.

3. M The following high-level statements can be made to describe the testing and acceptance responsibilities of the *Neutral Host* within the **Neutral Host Domain**:

- The *Neutral Host* is responsible for providing sufficient equipment and resources to be able to operate a development (DEV) platform and a live (LIVE) (customer supporting) platform;
- The *Neutral Host* is responsible for providing ***b***-interface connectivity, including in-band and out-of-band management connectivity, to the point-of-interconnect which provides onward connectivity to the test facilities of each hosted *Operator*;
- The *Neutral Host* is responsible for carrying out feature testing and compatibility testing on the development (DEV) platform and associated Controllers, BTS equipment and their associated management platforms prior to deployment on the live (LIVE) platform;
- The *Neutral Host* is responsible for testing PKI functionality towards the BTS;
- The *Neutral Host* is responsible for compiling a test exit report which shall, where necessary, highlight to the *Operator* any issues or concerns relating to the system's performance or functioning;
- Where workarounds of identified issues are proposed, the *Neutral Host* must highlight the underlying faults or defects, identify the root-cause and the limitations imposed by each and state for how long these will likely impact overall system performance (if at all) before resolutions have been implemented;
- That appropriate ISO27001 and CAS-T[2] governance measures are evaluated and shown to not compromise those requirements within the overall deployment of each *Operator*;
- The *Neutral Host* is responsible for maintaining documentation relating to any *Operator* specific test and acceptance requirements in respect of design decisions or architectural principles which must be adhered to.

[2] CAS-T is being closed in January 2020 and being replaced with a set of Telecoms Security Requirements under a new regulatory framework operated by Ofcom. At such point as these TSRs are published, these should be used as the basis for compliance requirements.

4. M The following high-level statements can be made to describe the testing and acceptance responsibilities of the *Operator* within the **Operator Domain**:

- Each hosted *Operator* is responsible for maintaining a Tier-2 SecGW (or equivalent IPSec capable device/function[3]) within their test environment in order to terminate the tunnels from the *Neutral Host* Tier-1***b*** SecGW;
- Each hosted *Operator* is responsible for maintaining an appropriate PKI within their test environment to support authentication of Tier-1***b*** to Tier-2 SecGW tunnel instantiation;
- Each hosted *Operator* is responsible for maintaining a test core network against which the *Neutral Host* can test their NHIB platform;
- The *Operator's* test core network must be representative of the *Operator's* live core network and include all components and capabilities required to validate the correct operation of the NHIB platform;
- The *Operator* is responsible for accepting connections from NHIB test platforms and routing those connections to their relevant test core components.
- The *Operator* is responsible to testing PKI functionality towards the *Neutral Host*.

[3] The term 'SecGW' is used for the Tier-1***b*** and Tier-2 perimeter functions within this annex, given the expectation that this function will typically be served by a dedicated context on an existing SecGW device within the **Operator Domain**. However, these functions do not need to be a SecGW in the formal sense, they simply need to be devices capable of adhering to the IPSec requirements outlined within this annex.

3 PLATFORM TESTING

3.1 Platform Configurations

5. M Within the **Neutral Host Domain** the *Neutral Host* must deploy a *development* (DEV) platform configuration connected to the test facilities of each hosted *Operator*. The DEV platform is used to carry out end-to-end testing against each hosted *Operator*.

6. M When the *Neutral Host* begins carrying commercial traffic for the hosted *Operators*, a *live* (LIVE) platform configurations must be deployed and operated within the **Neutral Host Domain**.

7. I The DEV and LIVE platform configurations together enable the testing and implementation of the NHIB platform through a process of testing and acceptance that occurs between the *Neutral Host* and each hosted *Operator*. The testing and implementation process is assumed to broadly follow the steps illustrated in *Figure 3-1*.

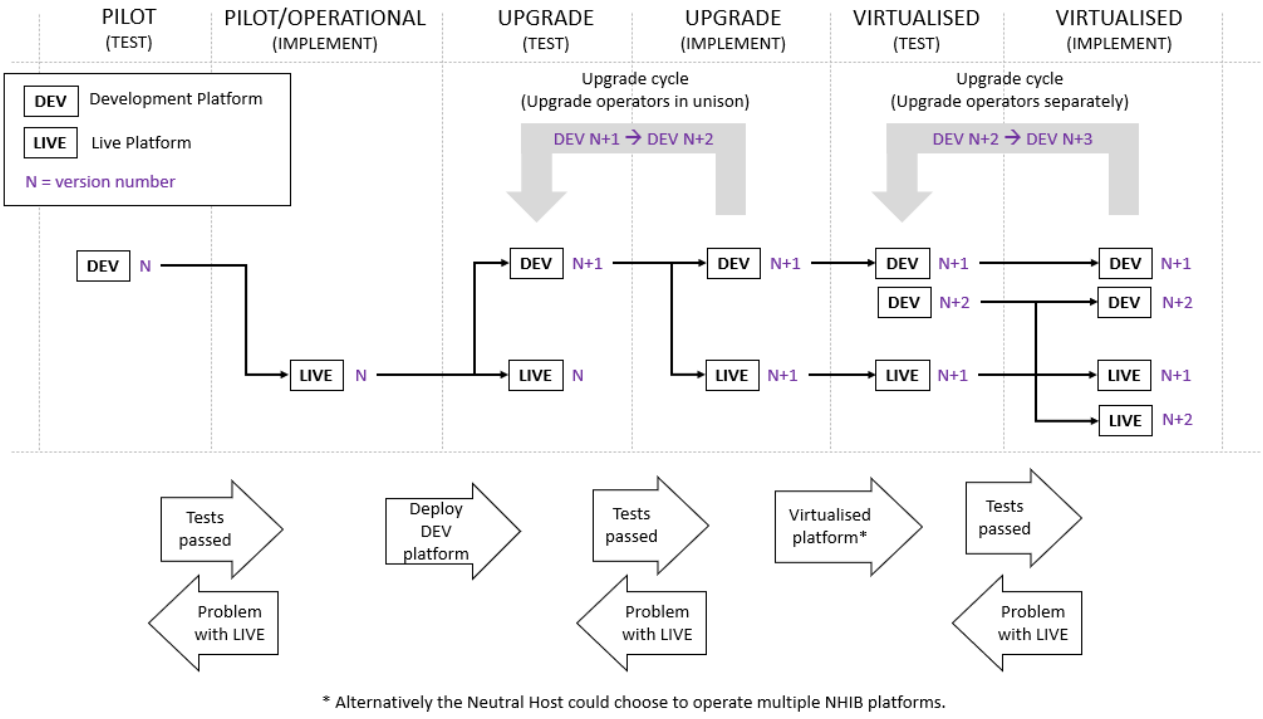

Figure 3-1. NHIB platform testing and implementation steps.

8. M **PILOT (TEST)**: This represents the initial stage of interaction between the *Neutral Host* and the *Operator(s)*. A DEV (N)[4] platform is deployed within the *Neutral Host's* datacentre and is connected to the test core of one or more *Operators*. End-to-end testing is carried out between the DEV (N) platform and the *Operator's* test core(s), and between the DEV (N) platform and the **Retailer Domain**,

[4] '(N)' refers to 'Version: N' of the NHIB platform. Likewise (N+1) refers to an increment to the NHIB platform version.

until all required test cases have been passed. The *Neutral Host* must separately complete testing against the test core network of each *Operator*.

9. M **PILOT (IMPLEMENT)**: When the testing against the *Operator's* test core is complete the DEV (N) platform is reassigned to become the LIVE (N) platform[5] and is connected to that *Operator's* live core network. If required, further 'live' call testing can occur, thus completing the full suite of tests required by the *Operator*. Once all tests have been completed, the LIVE (N) platform can be used to carry commercial traffic for the *Operator*. If, however, a problem arises during 'live' call testing, the LIVE (N) platform may be reverted to the DEV (N) configuration and further testing against the *Operator's* test core carried out. The *Neutral Host* exits the PILOT phase via demonstration of stable platform performance over a time period agreed separately with each hosted *Operator*.

10. M **OPERATIONAL (IMPLEMENT)**: The *Neutral Host* enters the OPERATIONAL phase following the successful completion of the initial PILOT phase. The *Neutral Host* has the option at this point to expand the capacity of the LIVE (N) platform without recourse to further testing, so long as the functional configuration of the platform is not altered (i.e. it runs the same software versions and supports prior tested BTS equipment). During this first OPERATIONAL phase the *Neutral Host* is not required to maintain a DEV (N) platform configuration.

11. M **UPGRADE (TEST**): In order to enable platform upgrades the *Neutral Host* must create a new DEV (N+1) instance of the NHIB platform (i.e. a new upgraded version of the platform). The DEV (N+1) platform must be connected to the test core networks of the hosted Operators and exists to enable end-to-end testing against the new DEV (N+1) platform version. Where a single instance of the LIVE (N) platform connects to multiple hosted *Operators*, the testing of the DEV (N+1) platform must be completed against all hosted *Operators* before the LIVE (N+1) upgrade can be implemented.

12. M **UPGRADE (IMPLEMENT)**: Once all tests are passed, the LIVE (N) platform is migrated to LIVE (N+1) and this becomes the new operational platform configuration for the *Neutral Host*. If, however, a problem occurs following the upgrade, then the LIVE (N+1) platform will be reverted to LIVE (N) and further testing against the *Operator's* test core(s), using DEV (N+1), will be carried out whilst commercial traffic continues to be carried on the LIVE (N) platform.

Where the *Operator* requires testing of the NHIB platform against a new core element or feature then the *Operator* will deploy those upgrades onto their test core network and the *Neutral Host* will use their DEV platform (assumed to be permanently connected to the *Operator's* test core) to run tests against that new test core functionality.

13. M **VIRTUALISED (TEST)**: When the *Neutral Host* gains greater scale it may be necessary or prudent to operate multiple NHIB platform instances, either on a common 'virtualized' platform or on physically separate platforms. Either way, the *Neutral Host* will potentially be faced with managing multiple versions of platform instances. In this case each platform instance version must be tested separately.

In the example illustrated in *Figure 3-1*, the *Neutral Host* is assumed to operate a platform instance at LIVE (N+1), but is wanting to introduce a new platform instance at DEV (N+2) (which, for example,

[5] Note that further platform hardware need not necessarily be acquired at this initial stage since the DEV platform can be reassigned to be the first (potentially low capacity) LIVE platform.

might be introduced to meet the requirements of one specific *Operator*). Note that the *Neutral Host* is required to maintain a DEV (N+1) platform instance alongside the new DEV (N+2) instance, in order that testing and debugging can continue on the N+1 platform configuration, if required.

14. M **VIRTUALISED (IMPLEMENT)**: Once end-to-end testing is complete, the *Neutral Host* can deploy the new LIVE (N+2) instance[6]. The *Neutral Host* must, in parallel, maintain a DEV (N+2) instance connected to the appropriate *Operator's* test core network. Again, if problems are detected with LIVE (N+2), then the *Neutral Host* reverts to testing using DEV (N+2) whilst commercial traffic continues to be carried on the pre-existing LIVE (N+1) platform instance.

15. I The *Neutral Host* could opt and is encouraged to deploy and manage a virtualised test core within the **Neutral Host Domain** to carryout initial platform testing prior to connecting the DEV platform to the *Operator's* test core networks.

16. M The *Operator* must maintain a test environment which is accessible to the *Neutral Host* from the **Neutral Host Domain** and which contains test instances of all relevant core network components.

17. M The *Operator's* test core components must be logically separate from their live core components and the live core components must not be reachable (routable) from within the test core domain.

18. M The test core within the **Operator's Domain** must be sufficiently provisioned and configured so that upon fault-free and correct operation of the connected NHIB platform the *Operator* is able to certify the NHIB platform for connection to their live core network.

3.2 Testing Procedures

19. I To begin the process of testing a new NHIB platform, or testing an upgraded version of an existing NHIB platform, the *Neutral Host* should contact each hosted *Operator*, separately, to request that test resources are allocated within each hosted **Operator's Domain**.

20. I The *Neutral Host* should liaise with with each hosted *Operator* on a bilateral basis to agree the tests to be carried out, the schedule for the testing (the test window) and the resources required within the hosted **Operator Domain** to carry out the testing.

21. M The *Neutral Host* is responsible for drafting a *Test Plan* which specifies the test strategy and the environments to be tested and is responsible for agreeing that Test Plan with the relevant hosted *Operator*(s). The *Neutral Host* will clearly set out which tests are lab tests and which are non-lab tests. At no point shall testing impact live user traffic or LIVE platform performance.

[6] Note that it is possible for *Operators* to be upgraded separately (i.e. it is possible that different versions of platform instances are supporting different *Operators* concurrently).

22. R The *Neutral Host* is required, on request, to furnishing the *Operator* with all relevant ***f***-interface, ***b***-interface, Controller and Aggregation Function configuration data for the planned tests.

23. R The *Operator* is required, on request, to furnishing the *Neutral Host* with all the relevant radio, core network and transport parameters for the planned tests.

24. R When testing is complete, the *Neutral Host* is required to provide to the hosted *Operator* a **Test Exit Report**. The format of the Test Exit Report shall be agreed between the *Neutral Host* and the hosted *Operator*.

25. R The Test Exit Report shall contain, as a minimum, the measured outcome of all planned tests and, most importantly, should highlight any issues or problems or workarounds that were identified during the testing phase and include visibility that workarounds have successfully been implemented via pre and post implementation testing.

26. R The *Operator* is required to review the Test Exit Report and respond by:

- Signing-off the DEV platform for LIVE deployment;
- Signing-off the DEV platform for LIVE deployment, but with caveats;
- Requesting further testing to be carried out on the DEV platform.

Where further testing is requested, the *Operator* should provide clear guidance as to why the DEV platform has not achieved LIVE certification and should set out what further steps the *Neutral Host* needs to take.

27. M Following the testing phase, the *Neutral Host* is required to draft a Method of Procedure (MoP) for each planned LIVE platform deployment, which must include a time-bounded roll-back procedure (in the event that the LIVE platform deployment is unsuccessful).

28. M The *Neutral Host* is required to alert all the existing hosted *Operators* and supported *Retailers* when the planned LIVE platform deployment will occur and to check that all necessary outages within the **Operator Domain** and **Neutral Host Domain** have been booked so that the LIVE platform deployment can proceed.

29. M The *Neutral Host* is responsible for monitoring alarms and checking that the new LIVE platform meets all agreed *Operator* KPIs. The *Neutral Host* must alert the hosted *Operator(s)* immediately of any detected faults or performance issues.

30. M When a new *Operator* is added to an existing NHIB platform, this introduces a risk of impacting the performance of existing hosted *Operators* (since, for example, capacity is shared on the ***f***-interface links). In this case, the *Neutral Ho*st must demonstrate, by example of proactive capacity planning,

that any hosted *Operator* agreed performance metrics are maintained after the new *Operator* is added.

31. I The *Neutral Host* should aim to make the platform deployment (whether a new deployment or an upgrade of an existing platform) as seamless as possible and with a minimum of impact from the end customer's perspective. System downtime should be minimised and it is recommended engineering work is scheduled during quiet traffic periods.

32. R Where a new BTS product or DEV(N)/DEV(N+1) platform, with new features and functionality, is deployed, the *Neutral Host* shall, on request, provide a complete set of factory acceptance test results with the design. The factory acceptance tests are the responsibility of the *Neutral Host* and are carried out in order to support the design of the NHIB solution, support the end-to-end testing and the acceptance of the design by *Operator* and confirm the NHIB solution meets the design requirements of this specification and also the 3GPP's specifications and Ofcom's requirements.

33. R The test methodology for the factory acceptance test shall be provided in the same report.

4 Connectivity Testing

4.1 Venue and *f*-interface Testing within the Retailer Domain

34. R The NHIB test configuration can either include the **Retailer Domain**, meaning the BTS and Controllers that form part of the end-to-end test configuration reside in the venues, or it can exclude the **Retailer Domain**, meaning the BTS and Controllers are located (for test purposes) within the *Neutral Host's* datacentre or test-house, but are representative of what will be deployed in the venue.

35. I Components of the NHIB system that can be tested within the **Retailer Domain** include the BTSs, the Controllers, local DNS servers and the ***f***-interface connectivity, which may also include local networking elements within the venue.

36. R Alternatively, where testing excludes the **Retailer Domain**, the *Neutral Host* is responsible for implementing the test ***f***-interface connection and required local DNS servers as a proxy for what will be (or is) deployed in the **Retailer Domain**. The test ***f***-interface connection can be a local network connection between the Aggregation Function and BTS and/or Controllers under test.

37. I The test ***f***-interface connection could include a network emulator (which degrades the local network connection by introducing additional delay, jitter and packet loss) in order to test the robustness of the overall solution under non-ideal ***f***-interface connectivity. The use of such of a network emulator and its configuration would be by agreement between the *Neutral Host* and the hosted *Operator*.

38. R Where testing includes the **Retailer Domain**, the *Retailer* is required to provision BTSs and Controllers as instructed by the *Neutral Host* to establish a suitable operational environment at the venue.

39. R Where testing includes the **Retailer Domain**, the *Retailer* is required to provision ***f***-interface connectivity at the venue. Additionally, the *Retailer* is responsible for delivering an appropriate ***f***-interface bandwidth, latency, jitter and packet loss performance aligned to the technical requirements of the radio solution adopted by the *Neutral Host*.

40. R Where testing includes the **Retailer Domain**, the *Retailer* is required to either provision and configure local network elements (i.e. switches, routers, local DNS servers) within the venue or will liaise with the venue owner to reuse their networking facilities at the venue.

41. I In larger venues, a representative partial deployment of the solution (e.g. a deployment on one floor of the building only) would be acceptable for testing the NHIB solution at that venue, so long as the remainder of the deployment replicates that tested in the partial deployment.

42. R The *Retailer* is responsible for configuring and testing the local network 802.1p QoS handling, demonstrating that an appropriate IP subnet address range has been allocated and (optionally) a VRF

has been deployed and tested for the NHIB solution and that local DNS capability able to resolve FQDNs (if required) is working correctly.

43. M The *Retailer* is responsible for demonstrating that an appropriate synchronisation solution has been deployed such that BTSs demonstrably synchronise to the *Operator's* network and that time-of-day clock signals are provided to all components required to provide time-stamped events or which rely on time-stamped certificates.

44. R Where the ***f***-interface is provided by a shared Internet connection or xDSL line, the *Retailer* shall demonstrate that the performance of that ***f***-interface connection can be monitored.

45. M Where testing includes the **Retailer Domain**, the *Retailer* must demonstrate concurrent connectivity between all BTS supporting all hosted *Operators*.

46. R Where the **Retailer Domain** is included in the test configuration, the *Retailer* should prove by demonstration that introducing (plugging in) or removing (unplugging) a BTS for one hosted *Operator* does not impact services provided to other hosted *Operators*.

47. R Where the solution operates with one hosted *Operator* per BTS, the *Neutral Host* is required to demonstrate that locking and unlocking the BTS of one hosted *Operator* does not impact the operation of BTSs supporting other hosted *Operators*.

48. R Where the solution operates with two or more hosted *Operators* per BTS, the *Neutral Host* is required to demonstrate that locking and unlocking the carrier of one hosted *Operator* does not impact the operation of either the other hosted *Operator* on the same BTS or other hosted *Operators* on other BTSs.

49. M When test calls are made against the DEV platform, *Operators* provided 'test' SIM cards must be installed into test devices[7].

50. M When test calls are made against the LIVE platform, *Operator* provided 'live' SIM cards must be installed into the test devices[7].

51. R The *Neutral Host* is responsible for providing, configuring and testing synchronisation sources (grand masters) within the **Neutral Host Domain**.

52. R Where the *Neutral Host* has implemented BTS auto-configuration (plug-and-play), the testing shall demonstrate the correct operation of the BTS auto-configuration feature.

[7] Test devices, with *Operator* specific carrier builds, may optionally be provided by the *Operator* for the purpose of testing.

53. R If required by the hosted *Operator* or the *Neutral Host* a pen test should be carried out against all exposed ports on all relevant equipment in the venue to check that *Operator* core elements and NHIB platform elements are not reachable. A pen test report should be provided following this activity and any identified issues should be resolved between the *Neutral Host* and *Operator*.

4.2 *b*-interface Testing within the Neutral Host Domain

54. R The *Neutral Host* is responsible for providing ***b***-interface connectivity between the DEV platform and the point-of-interconnect with each hosted *Operator*.

55. M The *Neutral Host* must deploy a DEV platform incorporating a resilient (dual) ***b***-interface connection to the *Operator's* test core network.

56. R The following options are available to the *Neutral Host* in respect of the resilient (dual) ***b***-interface connection:

- it can be instantiated on separate physical hardware deployed in a geo-resilient configuration (equipment located in two physically separate sites);
- is can be implemented on separate co-located physical hardware;
- it can be implemented using a twin (independent) chassis on the same hardware platform;
- it can be implemented via two logically independent and separate instances on a common virtualised platform.

57. I It is not necessary for the *Neutral Host* to provision physically separate geo-resilient circuits between the DEV platform and the point-of-interconnect (i.e. a common circuit, logically configured with an A-side and B-side path, can be used to connect the DEV platform to the *Operators* test core network).

58. R The *Neutral Host* is responsible for provisioning at least one of the following ***b***-interface connectivity options to the *Operator's* point-of-interconnect:

- A Dense Wavelength Division Multiplexing (DWDM) connection ('DWDM transmission');
- A Metro Optical Network connection ('Metro transmission');
- A dedicated Point-to-Point Layer 2 Service connection ('E-LINE transmission');
- An Internet connection via Private Peering, Public Peering or Transit Peering ('Internet transmission').

59. M The bandwidth of each provisioned test ***b***-interface circuit shall be sufficient to meet the throughput and latency requirements of the DEV platform configuration.

60. R The *Operator* is responsible for defining the BGP prefixes, autonomous system identity and IP subnets and end-point addresses for the S1 (S1-U, S1-AP) connections to the *Operator's* test core network.

61. R The *Operator* is responsible for defining the SCTP parameters for the test core network.

62. I The low-level details of the connectivity arrangement between the **Neutral Host Domain** and the *Operator*'s test core network will ultimately be defined through a bi-lateral agreement between the *Neutral Host* and the *Operator*.

63. I To complete the testing of the b-interface the Neutral Host shall demonstrate error free bidirectional end-to-end connectivity from the BTS, in the Retailer Domain, through to the Operator's core network in the Operator Domain.

4.3 Routing and Resilience Testing

64. R The *Neutral Host* is responsible for testing and proving that the reachability towards the **Operator Domain** aligns to the NHIB architecture principles, and most importantly it is demonstrably not possible to route between *Operator's* cores.

65. R The *Neutral Host* is required to demonstrate that only the agreed core network elements within the **Operator Domain** are reachable from within the **Neutral Host Domain** and **Retailer Domain** and that the routing policies and advertised BGP prefixes align to the NHIB architecting principles.

66. M The *Neutral Host* is required to demonstrate that there is no routing or reachability to any destination from any *unused* port on any switch, router or Aggregation Function element residing within the **Neutral Host Domain** and the **Retailer Domain** (i.e. a thorough pen test of all system components must be carried out).

67. I The *Neutral Host* may include one or more virtual Enhanced Packet Core (vEPC) elements within their **Neutral Host Domain** test environment to be used to emulate (to reasonable degree of accuracy) the core network elements of multiple hosted *Operators*. The general point here is that vEPCs can be used to accelerate multi-*Operator* testing prior to full integration testing against all hosted *Operator* test core networks.

68. I Where the *Neutral Host* wishes to test features which impact a single *Operator* only, a vEPC could be used to emulate the impacted *Operator* (in test) whilst connections to unimpacted (not in test) *Operators* test cores remain untouched.

69. I Alternatively, the unimpacted *Operators* could be emulated using multiple vEPCs and a single connection is made to the test core network of the impacted *Operator*.

70. R The *Operator* is responsible for certifying that any vEPC used by the *Neutral Host* to emulate their test core network is acceptable for emulating the *Operator's* core network functionality and capability.

71. R Where a *Neutral Host* operates both an A-side and B-side Aggregation Function (i.e. a fully resilient configuration), the *Neutral Host* will temporarily, for the purposes of failover testing, break the link between the BTS and the A-side SecGW or take down the A-side SecGW or the A-side Aggregation Function and confirm that the alternative B-side path re-establishes end-to-end connectivity.

72. R Where the BTS has the capability to select a B-side path, it should be demonstrated, on loss of the connection to the A-side SecGW, that the BTS reconnects automatically to the B-side SecGW and regains an operational state (i.e. is able to carry traffic again). Additionally, it should be demonstrated that the complete B-side transmission path is used to achieve the end-to-end connection (as per the NHIB architecting principles). Note that it is acceptable for ongoing calls to drop when the connection to the A-side SecGW is broken.

73. R The *Neutral Host* shall temporarily break the link between the Tier-1***b*** and the Tier-2 SecGW and separately take down the A-side ***b***-interface interconnect router to test failover. It should be demonstrated that the ***b***-interface path is re-routed to the B-side via the A-side router and the BTS regains an operational state (i.e. is able to carry traffic again). Note that it is acceptable for ongoing calls to drop when the A-side path is broken.

74. R The *Neutral Host* should establish that the convergence time for the A-side to B-side failover is slower within the **Neutral Host Domain** than the convergence time for core network components within the **Operator Domain** for each hosted *Operator*[8].

75. R Where a *Neutral Host* has opted to deploy both a ***f*-interface-internet-context** (for Internet ***f***-interface connectivity) and a ***f*-interface-private-context** (for Metro Ethernet private ***f***-interface connectivity) then it shall be demonstrated that there is no interconnection between these contexts.

76. R The *Operator* is required to deploy a test configuration which accepts a resilient (dual) ***b***-interface connection from the **Neutral Host Domain**.

77. R The *Operator* is responsible for checking that all BTS and Controller end points are reachable from the **Operator Domain** and that each end point address aligns to the test configuration design.

78. R The *Operator* is responsible for checking that the reachability of IP end points is limited to those which are relevant and allowed to be accessed by the *Operator* from within the **Operator's Domain**.

[8] This is to allow failovers within the *Operator's* network to converge prior to the NHIB platform taking its own failover action. Meaning that failures within the *Operator's* network, which cause a short interruption of service, do not impact the NHIB platform (apart from a short disconnection) and race conditions between competing failover mechanisms is avoided.

79. R The *Operator* is responsible for checking that all advertised BGP prefix ranges from within the **Neutral Host Domain** are correct, that the IPSec tunnel end points are valid IP addresses and that the traffic selectors limit connectivity according to the NHIB architecting principles.

80. R The *Operator* is responsible for testing that there is no reachability towards anything other than the **Neutral Host Domain** end points associated with that *Operator*.

4.4 IP Address Testing

81. R The *Neutral Host* is responsible for configuring IP outer and inner loopback addresses on the ***f***-interface links of the DEV (and subsequently LIVE) platform configurations.

82. R The *Operator* is responsible for defining the outer and inner (test core network) IP loopback addresses for the ***b***-interface link.

83. R The *Neutral Host* shall check that test core network (and subsequently live core network) end point inner addresses of hosted *Operators* do not clash when they exist within a common subnet address range (as might be the case in a non-virtualised implementation).

84. R The *Neutral Host* shall demonstrate that each BTS is able to obtain its outer IP address via a DHCP server located at either the venue or within the **Neutral Host Domain**, as appropriate.

85. R The *Neutral Host* shall demonstrate that any required Vendor Specific Options or other DHCP options are working correctly within the NHIB solution.

86. R The *Neutral Host* is responsible for providing and testing any local DNS servers within the **Neutral Host Domain** or the venue where private ***f***-interface connections are deployed and can demonstrate that DNS resolution is available within public DNS servers for Internet based ***f***-interface connections.

87. R The *Neutral Host* shall demonstrate that all A-NAME FQDNs, either within a public DNS or held on a local DNS server within the **Neutral Host Domain** or venue, resolve to valid C-NAME FQDNs using the round-robin method.

88. R The *Neutral Host* shall demonstrate that all Tier-1***f*** tunnel end point addresses, resolvable by a C-NAME within the DNS lookup, are valid tunnel end point IP addresses.

89. R The *Neutral Host* is responsible for defining Aggregation Function end point IP addresses.

90. R The *Neutral Host* is responsible for aligning both the DEV and LIVE platform configurations to the MME pooling capability of each hosted *Operator*.

5 Security, Control Measures and PKI Testing

91. M The *Neutral Host* is required to demonstrate that physical security is established through restricted access to the NHIB equipment and interconnecting cables[9]. Access to the *Neutral Host's* datacentre, where the platform is assumed to reside, is assumed to be limited to authorised personnel only. Any racked equipment should be installed into lockable cabinets. Only a restricted number of authorised personnel should be provided with cabinet keys. An access log should be maintained, recording who accessed the equipment, their time-in and time-out, and the reason for their access.

92. R The *Neutral Host* is required to check that appropriate physical security measures are put in place within the **Retailer Domain**.

93. M All unused Ethernet ports should be locked down.

94. R The *Neutral Host* is required to demonstrate that the IPSec tunnel between the Tier-1***b*** and Tier-2 SecGWs can only be initiated from within the **Neutral Host Domain** towards the **Operator Domain**, and not visa-versa.

95. R The *Neutral Host* is required to check that the ***f***-interface links between the Tier-1***f*** SecGW and the BTS under test are secured as per the PKI ***f***-interface design.

96. R The *Neutral Host* is responsible for checking that the ***b***-interface links between the Tier-1***b*** SecGW and each hosted *Operator* Tier-2 SecGW are secured as per the PKI ***b***-interface design. The *Neutral Host* is required to demonstrated that the public certificates provided by each hosted *Operator* are correctly installed onto the Tier-1***b*** SecGW.

97. R For the purposes of testing certificate re-authentication, the *Neutral Host* is required to check that new certificates load correctly onto the Tier-1***b*** SecGW and subsequently secure the ***b***-interface link.

98. R The *Neutral Host* is required to demonstrate that the tunnel is automatically closed (on re-authentication) if the certificate used to re-authenticate the IPSec tunnel is revoked. The *Neutral Host* should demonstrate that ***b***-interface links for other *Operators* are not affected by the revoking of one *Operator's* certificate.

99. R For the purposes of testing re-keying, the *Neutral Host* is required to demonstrate that the Tier-1***b*** SecGW operates in a make-before-break mode (thereby ensuring the IPsec tunnel is not torn down during the re-keying procedure).

100. R The *Operator* is responsible for providing the public certificates for securing the ***b***-interface links.

[9] Further details relating to each of the security domain requirements can be found by reference to ISO 27001 and CAS-T (see also footnote [2]).

101. R The *Operator* is responsible for revoking the certificate (for test purposes) that is used to secure the ***b***-interface link. The *Operator* should subsequently check that within a defined re-authentication period the IPsec tunnel on the ***b***-interface link is torn down.

102. R The *Operator* is responsible for checking that the child Security Associations on the ***b***-interface link egress/ingress only the traffic they are designed to transmit/receive.

103. R The *Operator* (with assistance from the *Neutral Host*) is required to demonstrate that a mismatch of policy between each end of the IPsec tunnel stops traffic flowing through the affected child Security Association.

104. R The *Operator* is required to check that any access control lists applied at the *Operator* end of the ***b***-interface link only allow valid layer-3 and layer-2 traffic to traverse the ***b***-interface link.

105. R The *Operator* is required to confirm that only multi-hop BGP traffic within the correct prefix range traverses the ***b***-interface link.

6 Quality of Service Testing

106. M The *Operator* is required to check that QoS markings sent and received on interfaces facing the **Neutral Host Domain** and QoS re-marking actions carried out in the *Operator's* edge routers aligns to the design mutually agreed between the *Neutral Host* and the *Operator*.

7 End-to-End Management Testing

107. R The *Neutral Host* is required to provide *Operator* connectivity to the management platform of the DEV platform either via an in-band or out-of-band connection path.

108. R Where the *Neutral Host* provides management interface IP end-point address connectivity to each hosted *Operator*, the *Neutral Host* shall demonstrate error-free bidirectional connectivity towards each hosted *Operator*.

109. R Performance Engineering (PE) data exported towards each hosted *Operator* will be in a format that is mutually agreed between the *Neutral Host* and *Operator*. In the absence of any specific formatting agreement, the *Neutral Host* should, as a minimum, present PE data in comma separated variable (CSV) format.

110. R Fault Management (FM) data exported towards each hosted *Operator* will be in a format that is mutually agreed between the *Neutral Host* and *Operator*. In the absence of any specific formatting agreement, the *Neutral Host* should, as a minimum, present FM data in text format, with each fault identified by a unique reference and tagged with a date and time stamp.

111. R Configuration Management (CM) data exported towards each hosted *Operator* (e.g. via a syslog feed) will be in a format that is mutually agreed between the *Neutral Host* and *Operator*. In the absence of any specific formatting agreement, the *Neutral Host* should, as a minimum, present CM data in text format tagged with a date and time stamp.

112. R The *Neutral Host* will agree with each hosted *Operator* a sequence of test calls, forced call failures and handover actions which will enable the *Neutral Host* to check that the PE counters are pegging correctly. The results from those test calls, forced call failures and handover actions will be shared with the *Operator* in the agreed PE export format.

113. R The *Neutral Host* is required to carry out tests to confirm that alarms are working correctly and should send evidence of those alarms to the *Operator* in the agreed FM export format.

114. R The *Neutral Host* is required to carry out tests to confirm that the CM interface (syslog) is working correctly. Testing should include (as a minimum): changing the configuration of the Tier-1***b*** SecGWr, changing the configuration of the ***b***-interface router within the **Neutral Host Domain** or any change to the Aggregation Function which relates to its security design.

115. R The *Neutral Host* is required to log (for audit purposes) all system accesses (valid or invalid) and the configuration actions undertaken on all components within the **Neutral Host Domain**. This log shall be made available to the *Operator* on request.

116. R Where the *Neutral Host* has provided a portal (web interface) into their management platform, the *Operator* is required to checked that the portal is reachable from the **Operator Domain**.

117. R Where the *Neutral Host* has provided a portal (web interface) into their management platform, the *Neutral Host* is responsible for testing that the portal provides all capabilities mutually agreed between the *Operator* and *Neutral Host*.

118. R The *Neutral Host* is required to check that all (pre-agreed) read-only data items/records are visible and not changeable and all read-writeable data items/records are visible and can be altered via the management interface according to the privilages defined in the RBAC.

119. R The *Neutral Host* is reponsible for checking that access to restricted areas via the management interface are policed according to the privilages defined in the RBAC.

120. R The *Operator* is reponsible for checking that information flows and allowed configuration actions via the Northbound interface align to the agreed specification between the *Neutral Host* and the *Operator*.

121. R The *Operator* is required to check that the PE counters are correctly read into their internal Performance Engineering toolsets.

122. R The *Operator* is required to check that the FM alarms are correctly read into their internal Fault Management toolsets.

123. R The *Operator* is required to check that the syslog data is correctly read into their internal syslog toolsets and that any filters and alarm triggers within the **Operator Domain** work as designed.

8 Service Testing

124. I Service testing is assumed to be carried out on the LIVE platform configuration (i.e. the NHIB platform should be able to support traffic originating from devices with 'live' SIMs). Live traffic service testing is assumed to be carried out under controlled conditions prior to commercial traffic being carried.

125. I The test configuration should, as much as is possible, mirror a typical radio deployment in a venue, in terms of power settings, mobility parameters and handovers to and from external macrocells. Functional testing of the handsets and their mobility interactions with the *Operator's* live macrocells should be carried out.

126. M The *Neutral Host* is responsible for ensuring the *Operator* provided RAN parameters for the BTSs are correctly set and maintained (e.g. MCC, MNC, eNodeB ID, LTE band, EARFCN DL, EARFCN UL, system bandwidth, TAC, cell-id range, PCI range and Reference Signal power).

127. R The *Neutral Host* is required to check that the correct PLMN ID or PLMN ID list is radiating from each BTS under test.

128. R The *Neutral Host* is required to check that the correct test device camping behaviour occurs for each hosted *Operator*.

129. R The *Neutral Host* is required to check that the upon network registration the correct Network Name is displayed on the test device (furnished with a test SIM).

130. R Where calls fail to register on the hosted *Operator's* network, the *Neutral Host* is responsible for investigating the underlying issues. If the issues are related to the *Operator's* core, traces should be provided to the *Operator's* support team for further investigation.

131. R The *Neutral Host* shall demonstrate to the *Operator* that roaming users registering onto the LIVE platform configuration select hosted *Operators* randomly (i.e. there is no preferred hosted PLMN ID for roaming devices).

132. R Where service testing is carried out within the **Neutral Host Domain** voice and data test calls should be made to check voice equality and data throughput speed, packet loss (UDP transfer) and latency (ping resonse time) performance.

133. R For failed call set ups, blocked calls or dropped calls the *Neutral Host* should investigate the underlying root-cause. Where the issue is believed to be not related to the NHIB solution the *Neutral Host* should provide call traces to the *Operator's* technical teams to help them identify the underlying fault.

134. R The *Operator* is responsible for checking that voice and data call data records (CDR) are generated correctly within their core network such that calls made on the NHIB platform will be correctly billed.

135. R The *Neutral Host* should carry out call tests using non-VoLTE capable devices to check circuit switched fall-back (CSFB) behaviour (i.e. 3G voice set up where there exists good external 3G coverage).

136. R The *Neutral Host* should attempt at least one emergency call attempt using a non-VoLTE device and one emergency call attempt using a VoLTE capable device on the LIVE platform configuration. The *Neutral Host* should confirm emergency call routing and that location based services are implemented correctly.

137. R The Neutral Host should demonstrate basic handovers and idle mode reselection between the NHIB solution and surrounding macrocells on the LIVE platform configuration.

138. R The *Neutral Host* shall demonstrate, under agreed test conditions, that MTPAS actions result in selected BTS within a defined zone code being locked down.

139. R The *Neutral Host* shall demonstrate that MTPAS BTS lockdown applied to one *Operator* does not impact other hosted *Operators* on other BTSs. Where two or more *Operators* share a single BTS (in MORAN mode) then the *Neutral Host* should demonstrate that a cell lockdown for either or both *Operators* aligns to the agreed design.

140. M The *Neutral Host* shall demonstrate that Geolock functionality locks the BTS when it detects that its location has changed.

141. R The Neutral Host shall demonstrate (if CELL_ID Geolock is enabled) that the BTS is locked when it detects that its location with respect to the local macrocells has changed (i.e. the BTS detects that the local macrocell CELL_IDs have changed).

142. R The BTS shall support the Cell Broadcast Service (CBS)[10] and, where requested by the hosted *Operator*, the *Neutral Host* will verify that CBS messages transmitted by the BTS are successfully received and displayed on the connecting UEs.

--- End of Document ---

[10] See 3GPP TS 23.041 v16.4.0 (2020-06), Technical realization of Cell Broadcast Service (CBS) (Release 16).