QMUL Spectrum Sandbox

Work Package 1: Proof-of-Concept and Practical Measurements

Final Report for DSIT

24th March 2025

Table of Contents

Table of figures

1 Executive summary

In 2019, Ofcom set out two new licence products:

- **Local Access Licence (LAL)**, which enables 3rd parties to access spectrum which is licensed to the UK's Mobile Network Operators (MNOs) but is not in use now or in the foreseeable future - just 27 LALs have been issued by June 2024, mostly to Telet;
- **Shared Access Licence (SAL)**, which gives first-come-first-served access assuming non-interference with existing licensees. By November 2024 a total of 988 SALs had been issued across the four spectrum bands:
    - Band 3 - 1800 MHz, 3.3 MHz of FDD spectrum;
    - Band 40 - 2300 MHz, 20 +10 MHz of TDD spectrum for indoor use only;
    - Band n77 - 3.8 to 4.2 GHz, 400 MHz of TDD Spectrum for 5G NR use only;
    - Band n258 - 24.25 to 26.5 GHz millimetric wave.

These licensing products are fundamentally sound in principle, but in practice there are unnecessary impediments to would-be licensees, which are having a strongly detrimental effect on uptake:

- For LALs, the licence application and assessment process is far too cumbersome, time-consuming, and uncertain to be commercially viable. The process requires engagement between Ofcom and the MNOs, and optionally (but desirably) between the applicant and the MNO; this coordination has proven to be enormously difficult, and the primary licence holders are not incentivised to participate. An application typically takes upwards of 6 months, with no guarantee of success. The result is that very few LALs have been issued, and there is no reason to expect any change in uptake without a re-evaluation of the application process.
- For SALs, the licence application and assessment process is somewhat more viable but still burdensome, and it limits the use-cases the licences can be used for. While the manual *application* process is soon to be brought online [6], the *assessment* process will remain manual, and will continue to take roughly 6 weeks. This is adequate, if burdensome, for long-term deployments such as Private 5G and Fixed Wireless Access, but it precludes short-term and/or short-notice usages such as Private 5G for festivals, and TV Content Production (BBC estimate 1000 outside broadcasts per year would use Shared Access Licences if they were more readily available).

This Sandbox project has investigated solutions to these problems, of which this Work Package 1 (WP1) has designed, implemented, trialled, and demonstrated:

- **Licensed DSA**, which splits licence issue and spectrum assignment into separate processes to provide immediate spectrum access within the regulatory certainty of a licence. The initial licence authorises the licensee to operate radios within designated geographic area(s) and frequency bands, as directed by a DSA Server.
- **Collection of Radio Measurement Data from 4G/5G Infrastructure**, offering a cost effective and easily implementable way of gathering the data required to carry out the Spectrum Allocation procedure.

- **DSA Server**, which is software to automatically compute spectrum assignments for radio base-stations to use without causing harmful interference to other licensees, subject to methodologies defined by Ofcom. A fully-functioning DSA Server was built by WP1 to support both the LAL and SAL bands, and Cellica and RANSemi radios were successfully demonstrated to transmit only as directed by the DSA Server.
- **Coordinated Sense and Avoid**, which is a mechanism whereby radios - whether base-stations or their User Equipment (UEs) - periodically scan their frequency band for other base-stations, and report the results to the DSA Server. This allows the evolving usage by MNOs of their licensed spectrum to be automatically detected, and for the DSA Server to prevent any possible interference by instructing all nearby devices to immediately cease using that frequency range. This process was successfully demonstrated with the cellXica radio.
- **CBRS Extensions**; by building on prior CBRS research and investment for the multi-band, multi-jurisdiction DSA Server-Client protocol designed in this project, a TRL 6 prototype was able to be cost-effectively and efficiently created and demonstrated and shows a path to ecosystem sustainability.
- **Automated Inter-Network Interference Management,** which applies extensions to CBRS coexistence management protocols to perform TDD alignment (timing and parameters) within groups, estimates of MNO Coverage were improved with measurements, and WP2 of the project performed simulations and field measurements to improve modeling parameters.

Via the WP1 prototyping and experimenting process, the following high-level outcomes were shown:

- Licensed DSA is technically viable and enables near-real time spectrum assignment from a DSA Server, instead of the existing multi-week or multi-month process;
- Performance demonstrated includes:
  - reduction in time taken to complete the entire process of obtaining a spectrum assignment down to sub-2 minutes for both LAL (currently 6 months) and SAL (6 weeks) scenarios
  - rapid detection (about 10 seconds per MIB) and prevention of co-channel interference between Primary and Secondary licence holders in LAL.
  - incumbent MNO detection at -15 dB SNR, enabling robust protections
- Coordinated Sense and Avoid is an efficient and cost-effective mechanism for detecting and protecting evolving MNO operations;
- Extending existing CBRS protocols for new jurisdictions, bands and sharing rules is feasible and well-positioned to leverage the existing CBRS device and software ecosystem;
- Proof of concept support for DSA Server performing inter-network interference management with a limited TDD alignment capability. This is a mechanism which can enable much greater deployment densities for SAL scenarios where common waveforms are grouped together with time synchronisation (managing spectrum in **both** frequency and time domains)
- In addition to the fully automated approach, it has also been identified that a more manual approach can be adopted as an interim measure when deploying equipment that does not have the full scan, sense and remote control capability.

2 Overview

In March 2024, the UK Department for Science, Innovation and Technology (DSIT) made three awards for Spectrum Sandbox projects, one of which was made to the team of Queen Mary University of London (QMUL), Telet Research (telet), Aetha Consulting (Aetha), and Federated Wireless (FW). The goal of the QMUL-led project is to prototype and characterise the impact of a novel spectrum sharing mechanism to improve spectrum sharing performance and operations in Local Access Licence (LAL) and Shared Access Licence (SAL) using 3GPP Band 3 and n77 for prototyping, respectively.

WP1 of the QMUL Spectrum Sandbox focussed on formalising, prototyping, and experimenting with the spectrum sharing mechanism. This section of the document describes the background to this project, the problems the project seeks to address, the approach to solving those problems, and the major outcomes from the prototyping work.

2.1 Background and related work

In 2019, Ofcom [1] set out two new licence products:

1. **Shared Access Licence (SAL)**, which gives access to four spectrum bands (1800 MHz, 2300 MHz, 3.8-4.2 GHz, and 24.25-26.5 GHz) [2] assuming rule compliance and non-interference with protected systems.

2. **Local Access Licence (LAL)**, which provides a way for 3rd parties to access spectrum licensed to UK's Mobile Network Operators (MNOs) that is not currently in use nor planned for use in the near future [3].

One of the Key Performance Indicators (KPI) that can be used to assess the effectiveness of a licensing method is the number of licences issued.

By June 2024, just 27 LALs have been issued [4] with 988 SALs issued by November 2024 [5]. While the SALs are far more numerous than the LALs, SAL utilisation is multiple orders of magnitude less than in the US Citizens Broadband Radio Service (CBRS) where over 400,000 sites are active in less spectrum (150 MHz). This is generally attributed to the uncertainty and time required to receive a licence where receiving a SAL can take months and a LAL over a year. LALs in particular, have an inherent high degree of uncertainty for access and continued operation due to the requirement to protect future incumbent MNO operations.

Despite this relative underutilisation, it is already evident that SAL access in urban areas is already being "sterilised" from inefficient coordination among secondary systems. This was highlighted by Ofcom in 2024 where SAL TDD synchronisation in 3.8-4.2 GHz was required (see Fig. 1), but no automated mechanism for implementation was proposed nor appears on Ofcom's updated Licensing Platform Evolution (LPE) SAL roadmap.[6]

Ofcom's LPE program is updating and streamlining the application process (not the assignment process) across Ofcom's supported licenses, with significant current emphasis focused on supporting new SAL rule changes [5][6]. Several other sharing mechanisms have been proposed in the UK including for TVWS [7], though that framework ceased in 2024 with no active devices as the last database administrator stopped service.

Internationally, CBRS is the most widely deployed sharing protocol [8] with extensions defined for measurements [9] and automated coexistence (TDD alignment) [10].

Innovation, Science, and Economic Development Canada (ISED) is currently beta-testing its Non-competitive Local Licensing (NCLL) framework – a SAL-like variant for 3900 GHz. Sharing for WI-FI access include the distributed 802.11h protocol [12] and the Automated Frequency Controller Framework (AFC) [13] approach. In the UK in February, Ofcom issued a consultation to “authorise both [mobile and WIFI] services to use the band through sharing … [with] standard power Wi-Fi to use Lower 6 GHz (5925–6425 MHz) using an AFC database, including outdoors, if there is sufficient interest from industry” [25].

2.2 Problems being addressed

The sharing mechanism designed and prototyped in WP1 is intended to address the following problems:

2.2.1 LAL underutilisation & access time

Local Access Licences (LALs) enable small operators to use large swathes of underutilised MNO spectrum, but are **commercially unviable**

1. Ofcom assign spectrum to LALs, following consultation with the MNO Primary Licence holders. The MNOs have little motivation to complete this function, so long delays, often as long as 6-12 months are common.
2. Protections for *future* unknown operation lengthen the process

The relative underutilisation can be seen in the Band 3 coverage maps (reported and modelled) shown in Figure 1. To free up this spectrum, there is a need for a spectrum sharing mechanism with the following properties:

1. Quick and immediate determination of spectrum access
2. Automated protections for future MNO operations

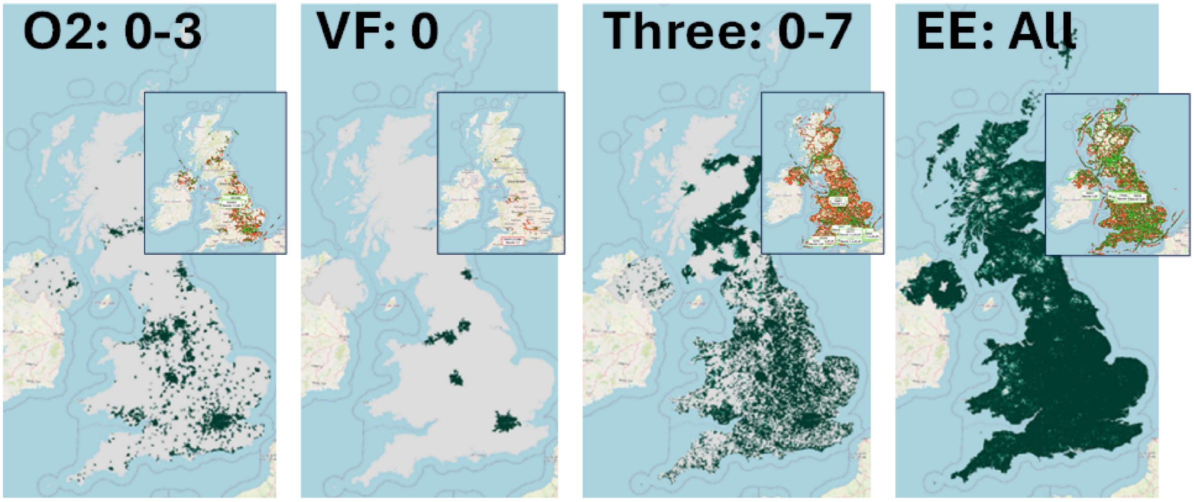


Figure 1 Illustration of Band 3 Utilised Spectrum – modelled (Green) and measured (insets, from cellmapper)

2.2.2 SAL access time

Shared Access Licences (SALs) enable non-MNO operators to use 5G spectrum for **some use-cases**, particularly long-term emplaced operations, but short-term operations are a problem.

1. Ofcom will automate SAL applications, but will still make spectrum assignments manually [6], taking around 6 weeks; this is unnecessarily burdensome even for long-term use-cases.

2. No short-term and/or short notice use:
    a. From conversations related to this project, BBC have stated that they would use for SAL spectrum for ~1000 outside broadcasts per year if they could, producing enhanced content at reduced cost;
    b. Private networks for festivals.

Ultimately, the UK could derive more economic & social benefit from its spectrum with more efficient licensing & processes.

1. Ofcom uses complex algorithms to assess whether a transmitter will cause interference to other licensees, but these can be automated (CBRS, AFC, TVWS, etc.).

2.2.3 Efficient use of spectrum

Despite relative underutilisation, it is already evident that SAL access in urban areas is already being “sterilised” from inefficient coordination among secondary systems. This was highlighted by Ofcom in 2024 where SAL TDD synchronisation in 3.8-4.2 GHz was required (see Fig. 1), but no automated mechanism for implementation was proposed nor appears on Ofcom’s updated Licensing Platform Evolution (LPE) SAL roadmap [6].

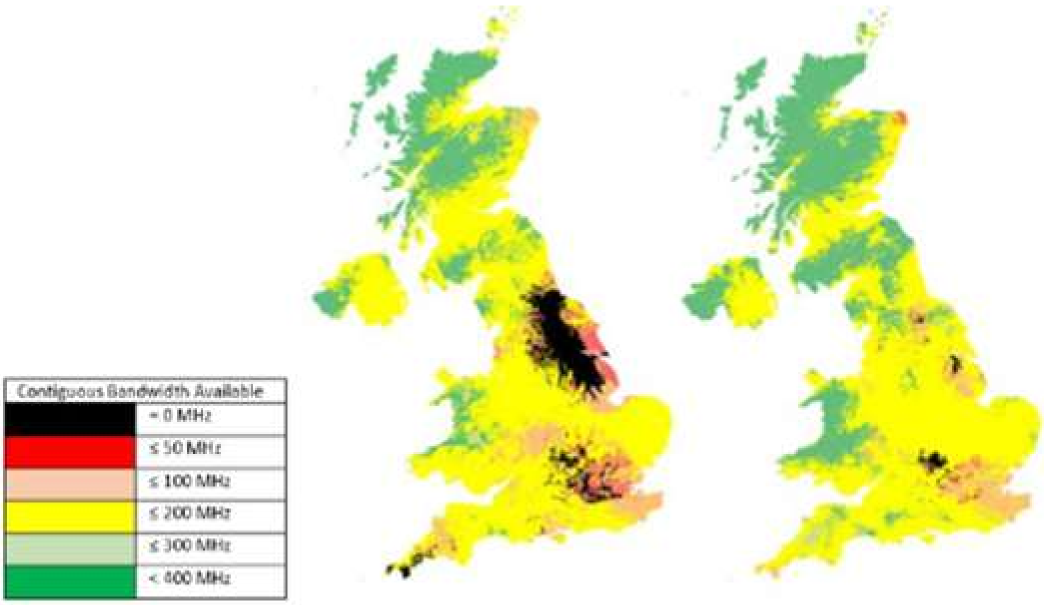


Figure 2: Despite this relative underutilisation, it is already evident that SAL access in urban areas is already being "sterilised" from inefficient coordination among secondary systems. This was highlighted by Ofcom in 2024 where SAL TDD synchronisation in 3.8-4.2 GHz was required (see Fig. 1), but no automated mechanism for implementation was proposed nor appears on Ofcom's updated Licensing Platform Evolution (LPE) SAL roadmap.[6]

2.2.4 Bootstrapping / Ecosystem compatibility

The stark contrast in uptake between TVWS and CBRS emphasises that technical solutions must have a commercially-viable ecosystem to be successful. The spectrum sharing mechanism investigated by this project leverages existing equipment and software wherever possible.

2.3 Solution overview and approach

The prototyped solution builds on the following four concepts.

1. **Licensed DSA**, which splits licence issue and spectrum assignment into separate processes to provide immediate spectrum access within the regulatory certainty of a licence. The initial licence authorises the licensee to operate radios within designated geographic area(s) and frequency bands, as directed by a DSA Server. This is summarised briefly in Section 2.3.1, more fully in Section 3.2, and in detail in [Deliverable 1.2].

2. **DSA Server**, which is software to automatically compute spectrum assignments for radio base-stations to use without causing harmful interference to other licensees, subject to methodologies defined by Ofcom. This is described in detail in Section 3.

3. **Coordinated Sense and Avoid**, which is a mechanism whereby radios - whether base-stations or their User Equipment (UEs) - periodically scan their frequency band for other base-stations, and report the results to the DSA Server. This allows the

evolving usage by MNOs of their licensed spectrum to be automatically detected, and for the DSA Server to prevent any possible interference by instructing all nearby devices to immediately cease using that frequency range. This is described in Sections 2.3.2 and 3.4.2.

4. **DRAM** - Dynamic Radio Access Management middleware has been developed to integrate between the radio unit and the DSA Server. Telete has demonstrated that radios from Cellica and RANSemi, in Band 3 and n77 can be both (a) dynamically configured to transmit the real time assigned licence and (b) can provide information based on scans of their RF environment, to update the regulatory picture about how spectrum is being utilised. This is described in detail in Section 5.7.

2.3.1 Licensed DSA

The core premise of Licensed DSA is that Licence Issue and Spectrum Assignment should be split into separate processes, with the following broad outline of steps (see [Deliverable 1.2] for full details):

1. The operator is issued a **long-term licence** via Ofcom's LPE, allowing ongoing Dynamic LAL or SAL operation as directed by a **DSA Server**.
2. The DSA Server uses Ofcom's methods to make **short-term spectrum assignments automatically** and immediately for each radio.
3. For DSALs, humans use the DSA Server's web page, and manually configure their radios accordingly – perfect for outside news broadcasts
4. For DLALs, radios automatically contact the DSA Server and transmit accordingly – protects evolving MNO usage without needing their input.

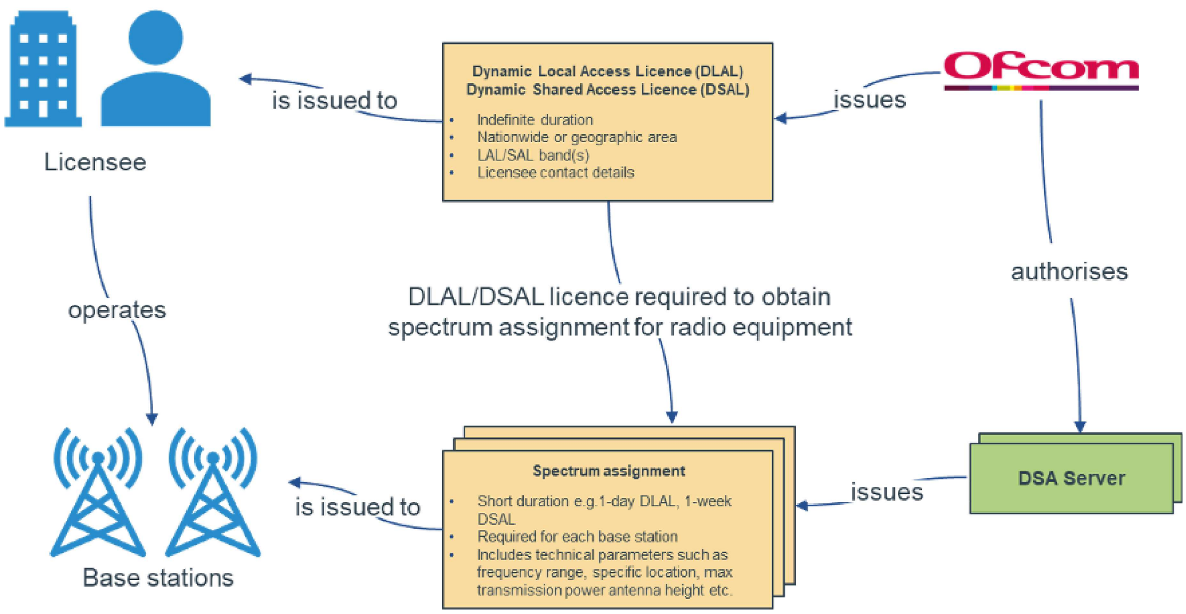


Figure 3: Overview of Licensed DSA

The proposed sharing framework assumes that secondary operators still apply for and receive licences to operate via Ofcom's existing licence management framework, thereby maintaining the existing relationship with Ofcom and its enforcement mechanisms. These licences may place restrictions on operation, e.g., areas, bands, maximum transmit power, maximum number of base-stations, but details on assignments are deferred to the DSA Server.

In various commercial bands a cloud-based DSA Server has been previously shown to perform the necessary calculations to determine availability in near real time ([14] for CBRS and AFC, [15] for SAL). The demonstration of the prototype DSA Server, hosted in AWS, again confirms this capability.

For LAL spectrum access, current processes mandate approval by the incumbent MNO. By mandating and demonstrating the success of Coordinated Sense and Avoid in LAL spectrum (prototyping in Band 3), the MNO approval step is no longer necessary, thereby enabling spectrum assignments in seconds instead of months.

This project's spectrum sharing mechanism is akin to a traditional centralised DSA solution as shown in Fig. 4 (below), with 'DSA Server' being the generic term for a SAS, AFC, Database or other centralised controller, and 'DSA Client' referring to the software that directly controls the spectrum usage for a single device or collection of devices. To this, the project adds the following:

1. First, sensed detections of changes in protected systems are primarily provided by the secondary systems (DSA Operators) rather than by dedicated sensors (e.g., ESC) - "Coordinated Sense and Avoid"; see Section 2.3.2;
2. Second, those same measurements are used to update models of MNO coverage; see [Deliverable 1.2].
3. Third, the DSA Server is intentionally multi-jurisdictional in that rules and protections enforced by the DSA Server depend on the spectrum accessed by the DSA Operators, e.g., SAL vs LAL or potentially across countries; see Section 3.4.1.

2.3.2 Coordinated sense and avoid

2.3.2.1 Overview

In the Coordinated Sense and Avoid concept, any base-station operating under DSA (and, potentially, its UEs) makes regular measurements of other spectrum users in the same band, and especially the frequency range it is using itself.

Preliminary measurement reports which confirm no nearby MNO usage in a frequency range (detected from recovering broadcast PLMNs) can be required prior to receiving a spectrum assignment in that range. Ongoing measurements are then **sensed** and reported to the DSA Server. } The base-stations will then request a fresh spectrum assignment; the DSA Server incorporates all recent measurements, so as to augment any data which it may have previously received, either from Ofcom or the MNOs themselves, on where coverage is being provided.

To detect the presence of MNO operations, recovering broadcast PLMN information is sufficient, but additional information (e.g. cell identifications) assists the DSA Server to make more informed decisions. The DSA Server is also responsible for enforcing the time-periods in which fresh measurements must be taken, and could coordinate and optimise when measurements take place between multiple devices in the same vicinity.

The mechanism by which measurements are taken is not mandated in this framework and can come from UEs, gNBs, or dedicated sensors. For 3GPP compatibility, the required measurements for access and coexistence (PLMN, cell ID, signal strength) are most easily achieved at the UEs, which already capture these fields before network attachment from broadcast MIB and SIB1 data. UEs also provide the possibility for sampling a wider variety of locations. [9] is further extended to permit any Request to include measurement capabilities or reports and any Response to include measurement requests so that non-transmitting systems can also report measurements.

2.3.2.2 Measurement and analysis of radio data

The objectives of this Work Package included investigation into methods of collecting radio use data from live mobile systems for analysis in near real time in order to produce real world spectrum models which can be used for efficient allocation of radio spectrum.

In practice, modern 4G and 5G waveforms are designed to cope with co-channel interference (CCI), and as long as the radio systems within a local area are configured so that parameters are set up for minimal interference, much higher CCI signal levels can be achieved without noticeable service degradation.

2.3.2.3 Levels of radio data capture

Within this Work Package, we have identified three main levels at which data for DFSA use can be collected. These levels are as follows:

2.3.2.3.1 Level 1 - Signal Level Reports

This is the simplest measurement that can be made and captures the signal strength as measured by the radio. Even as a basic measurement there is useful information that can be extracted as the signal strength level tells us something about the interference potential, the the spread indicates information about the occupied bandwidth:

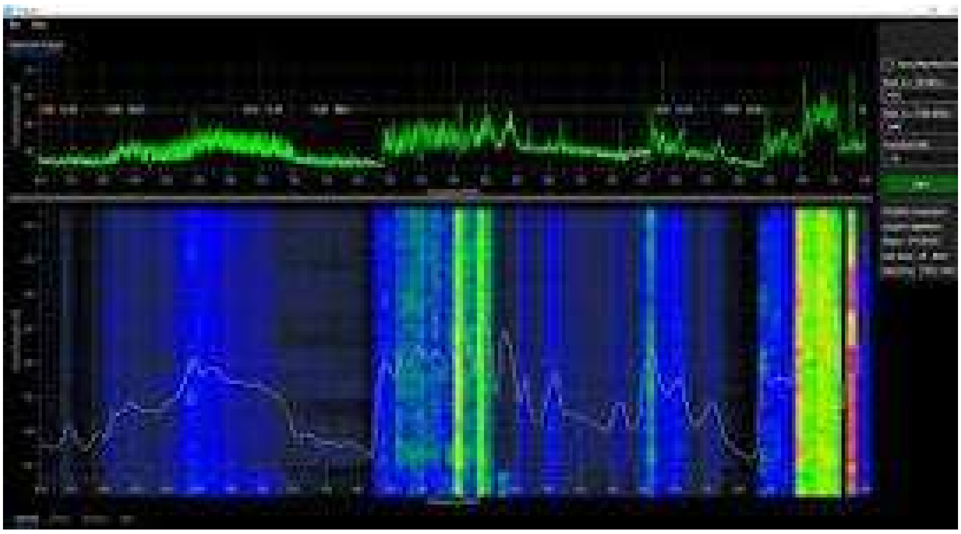


Figure 4: Typical example of a signal strength report showing relative signal strengths and occupied bandwidth

2.3.2.3.2 Level 2 - Analysis of Broadcast System Information

The MIB and SIBs are designed to enable UEs to synchronize with the network, acquire essential parameters, and access the cellular services. They contain a range of information regarding the configuration of the radio network. This information is constantly broadcast to allow UEs to synchronise, then attach to the local radio access network.

The MIB and associated SIBs are coded and broadcast in a manner that allows them to be detected and decoded at very low signal levels, which are considerably below the level required for an UE to attach. This also means that MIBs from co-channel stations can be detected well below the signal threshold required to cause interference to other mobile radio systems.

The collected MIB and SIB data can be used to uniquely identify co-channel stations, and to determine the technical configuration that they are using. This information can then be fed into the DSA system for use within the spectrum grant process. As different waveform configurations between co-channel stations can be accurately predicted if all of the relevant radio parameters are known, accurate predictions of likely interference results can be assessed. Once the configuration of each waveform within a co-channel pairing are known, appropriate interference profiles between different systems can be selected and applied in the interference assessments

2.3.2.3.3 Level 3 - Collection of Radio Management Signalling between Base Station and active User Equipment.

This represents a far more detailed set of data that can be collected in terms of not just the RF environment at the location of the base station but also across the geographic area served by the base station. Whilst this additional data presents significant opportunity for a more sophisticated analysis of potential interference it also presents challenges in terms of the processing requirements to fully utilise this data.

2.4 Summary of WP1 outcomes

The following high-level outcomes were shown:

1. The viability of Licenced DSA was implied and the benefits demonstrated
    a. Separation of licensing from assignment with license synchronisation with Ofcom emulated, but operator credential verification implemented
    b. Near-real time spectrum assignment (on the order of seconds) from a DSA Server instead of the existing multi-week process
2. The technical feasibility of the spectrum sharing concepts to the sandbox spectrum sharing mechanism were demonstrated, including:
    a. Detecting new MNO operations from PLMN broadcasts
    b. Coordinating avoidance across DSA networks from a detection
    c. Updating MNO coverage data from measurements
3. The developmental feasibility of extending existing CBRS protocols for new jurisdictions, bands and sharing rules was shown, and the potential cost savings of the approach, including:
    a. The DSA Server implemented for both LAL and SAL automation across all LAL and SAL bands
    b. Achieving TRL 6 with a limited budget and in under a year.
    c. The transparency of this approach to the DSA Client (DRAM)
4. Proof of concept support for DSA Server performing inter-network interference management with a limited TDD alignment capability

2.4.1 Solution Architecture

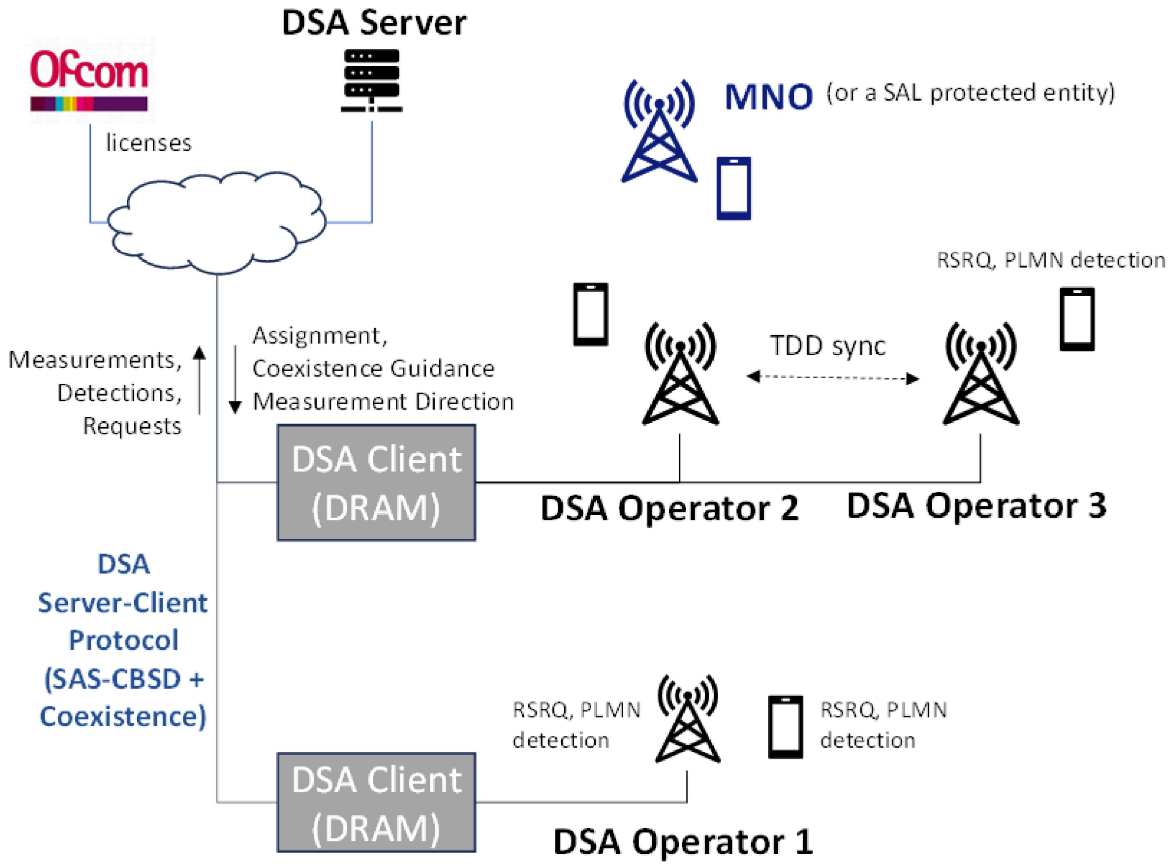


Figure 5: The DSA solution architecture. depicts the WP1 Solution Architecture which supports all of the preceding principles with components described in Table 2

Table 1: Components of the WP1 architecture

Component	Description
MNO	Protected System. Cooperative or non-cooperative
DSA Operators	Operators of RANs in spectrum unused by Protected System(s), holding a DLAL or DSAL Ofcom licence
DSA Server	• Responsible for protecting MNO operations from DSA Operators in spectrum assignments • Dynamic guidance to DSA Operators
DSA Client ("DRAM")	"Middleware" that coordinates DSA RAN operations with DSA Server
RAN / UE	RAN / UE Operations + collect measurement reports
DSA Server-Client Protocol	Messaging by which DSA Server and Clients coordinate secondary access and operation

2.4.2 Working prototype solution

Within the solution architecture in Figure 5, WP1 prototyped the following:

1. **DSA Server**
    a. Supports near real time spectrum assignment for all LAL and SAL bands
    b. Implements a Client-Server protocol, derived from the CBRS protocol, to support automated requests for LALs and SALs
    c. Implements a web-page to support human requests for SALs
    d. Implements Licensed DSA
    e. Implements Coordinated Sense and Avoid
    f. Uses Ofcom OfW590 algorithm for SAL spectrum assignments
    g. Uses a prototype algorithm for protecting MNO coverage (see [Deliverable 1.2]) in lieu of a future Ofcom algorithm, which additionally incorporates measurement reports of MNO usage
    h. Proof-of-concept TDD alignment
    i. Deployed in AWS
2. DSA Client - the **Dynamic Radio Access Manager** (DRAM). This component has the following characteristics:
    a. It sits between the DSA Server and one or more eNB/gNBs
    b. It can be owned by an Independently Operated Private Network (IONP) or provided to the IONP as a service.
    c. It directly controls the radio parameters of its subordinate radios, and configures them to operate on radio channels for which the DSA Server has issued leases
    d. Compiles and provides spectrum usage reports based on data collected from its subordinate radios
    e. Compiles Spectrum Lease Requests, based upon scan results from radios
    f. Provides 'Heartbeat' interactions with DSA server
    g. It can be implemented in a number of form factors:
        - Within the Radio Manufacturer Radio/Network Management System
        - Provided as a Hosted Service (DSA as a Service)
        - Embedded within a standalone radio
        - A 'Bolt On' application, running on a secondary platform within a deployment site.
3. **DSA Client-Server Protocol**
    a. Defined for multi-jurisdiction, multi-band operation by extending the SAS-CBSD protocol
    b. Implemented by both DRAM and DSA Server
4. **RAN and UE support**
    a. Telet has integrated the following radios: Cellica M3Q (Band 3), RANSemi PC802 Reference Design in Band 3 and Band n77, enabling a demonstration of DSA for both Local and Shared Access.
    b. User Equipment (mobile phones and spectrum analysers) were used to demonstrate that the cells were transmitting in the correct band and delivering the relevant service.

2.5 WP1 Program status review

2.5.1 Fulfilment of research objectives

As per “Spectrum Sandbox WP1 Acceptance Criteria” (DSIT, 13/03/2024), the research objectives of this work package were to undertake practical field trials to:

Table 2: Research objectives

Objective	Evidence Presented in this Document
Use network equipment and user devices to make measurements of the radio environment, including measurements and characterisation of spectrum utilisation, noise floor and interference.	Sections 5 POC demonstration [Telet]
Develop and demonstrate proof of concept solutions for sharing measurement data and associated metrics with Ofcom and DSIT.	Sections 5 POC demonstration [Telet] 3.6 [Federated Wireless]
Develop and test technical solutions that increase the level of spectrum sharing relative to current spectrum authorisation and access methods.	Sections 4 Practical Implementation [Telet] 3 The DSA Server [Federated Wireless]

2.5.2 WP1 Deliverables

The project identified the WP1 project deliverables listed in the following table.

Table 3: WP1 deliverables

Serial	Milestone/deliverable
1	Request to and approval in principle from Ofcom for necessary spectrum authorisations to cover the duration of the project in a format and with information to be specified by Ofcom. Should include, inter alia, a statement of acceptance from the affected parties of potentially increased interference during the project.
2	Where appropriate, request to and approval from the relevant government department for necessary authorisations and agreements to share, to cover the duration of the project.
3	R&D report detailing the measurement and data sharing solutions to be demonstrated in the final deliverable proof of concept.
4	R&D report detailing the design of the sharing solutions(s) to be tested including rationale for their design and expected performance in a test environment.
5	Test plan, setting out in detail the systems which will be tested, the conditions under which they will be tested, the parameters that will be varied, and the approach to assessing the performance of the systems.
6	Test report, setting out the detailed results from the testing, comparing system performance under conventional operation and under more intensive spectrum sharing. 1. preliminary test report 2. Updated test report (incorporating WP2 requirements)
7	Report and proof of concept demonstration on potential for sharing of usage and interference data for regulatory purposes, setting out the potential benefits, associated challenges, and recommendations for the future operation of such systems. This should include visualisation, such as a map-based representation of the data allowing analysis by location, frequency, and time

Serial	Milestone/deliverable
	1. Quarterly interim reports 2. Demonstration 3. Interim final report 4. Final report
8	Archive of measurement and performance data captured during testing. 1. format for archive and data agreed 2. Delivery of archive and data
9	1. Conclusions drawn, set against objectives and relevant items of the Study questions listed on Page 10 (Section, 'Policy Context to requirement') of the ITT. 2. Next steps for building on objectives and study questions and lessons learnt

2.5.3 Federated Wireless WP1 milestones

Table 4 lists the Federated Wireless Milestones and status of those milestones with all completed except for the Final Report (this document) and the Final (Q4) Briefing to DSIT to come.

Table 4: Federated Wireless Deliverables to Work Package 1

Date	Milestones	Description	Milestone Type	Status
05-Apr-2024	1. Kickoff Meeting	Participation in Kickoff	Minutes	Complete
30-Apr-2024	2. Server-Client DSA Protocol Requirements	Requirements for Multi-band	Document	Complete
17-May 2024	3. Deployment of LAL Tool	LAL Tool Accessible to telet	FW Test Report	Complete
24-May-2024	4. Server-Client DSA Specifications for Band 3	Design Document for subset of 1.	Document	Complete
24-Jun-2024	5. Quarter 1 Review Material	Inputs and participation in Quarterly Review	Document, Slides	Complete
30-Jun 2024	7. LAL Tool Covers Sandbox Experiment areas	MNO coverage for Band 3 extended	FW Test Report	Complete
30-Jun-2024	8. Stakeholder Workshop 1	Material for and Participation in workshop	Slides	Complete
31-Jul-2024	9. User Interface Adaptation	LAL tool supports interface protocol design for spectrum application and request (4)	FW Test Report	Complete

30-Aug-2024	10. LAL Heartbeat	LAL tool supports interface protocol design (4)	FW Test Report	Complete
25-Sep-2024	12. Quarter 2 Review Material	Inputs and participation in Quarterly Review	Document, Slides	Complete
30-Sep-2024	13. DSA Performance Assessment Report Under Varied Conditions	Leverage Server-Client implementation and simulation to assess performance	Document. FW Test Reports	Complete
30-Sep-2024	14. Long-term Spectrum Usage and Impact Study	Analysis from FW- telet experiments from integrating 10.	Document. FW Test Reports	Complete
24-Nov-2024	17. Server-Client DSA Specifications for Multi-band	Extension to 4 to cover all bands in 2	Document	Complete
26-Dec-2024	18. Quarter 3 Review Material	Inputs and participation in Quarterly Review	Document, Slides	Complete
24-Jan-2025	19. Security and Privacy Assessment Report	Document from FW self-assessment of security of DSA server and protocol	Document. FW Test Reports	Complete
31-Jan-2025	20. Draft Final Report Submission to DSIT	Inputs for Draft Report Submission	Document	Complete
28-Feb-2025	21. 2nd Stakeholder workshop	Material for and Participation in workshop	Slides	Complete
14-Mar-2025	22. Final Report	Final Report	Document	This Document
20-Mar 2025	23. Quarterly Review 4	Inputs and participation in Quarterly / Final Review	Document, Slides	Complete

These will be referenced throughout this document as, e.g., [FW-MS1].

3 The DSA Server

For this Sandbox, Federated Wireless have designed and implemented DSA Server software to implement the spectrum sharing mechanism described in [Deliverable 1.2], additionally incorporating some components which were previously developed for the 5G New Thinking project, as funded by DCMS in the 5G Testbeds & Trials project.

3.1 Concept

1. A DSA Server automatically computes spectrum assignments for radio base-stations to use without causing harmful interference to other licensees.
2. Ofcom will define the methodology and algorithms used by the DSA Server, matching their own methodologies for manually assessing frequency assignments, and using similar data describing other licensees' usage.
3. Spectrum assignments may change in real time as usage by high-priority licensees (e.g. MNOs in the LAL bands) changes, requiring the radios (or software acting on their behalf) to be in constant contact with the DSA Server, and automatically configure themselves accordingly.
4. Spectrum assignments may be on a first-come-first-served basis (e.g. in the SAL bands); if so, a human may contact the DSA Server via a web page, and then manually configure their radios accordingly.

3.2 Spectrum sharing with a DSA server

Full details of how dynamic spectrum assignment would operate can be found in [Deliverable 1.2 from this sandbox], entitled 'Proposed Spectrum Sharing Solution, Version 1.0, 31 October 2024'. A summary is given here:

At present, usage in LAL and SAL bands is licensed (as opposed to licence-exempt etc.). We propose to maintain this licensed approach and enable DSA by separating the licensing process from the spectrum assignment process. All users of dynamic spectrum access in the LAL or SAL frequency bands would require an administrative licence from Ofcom – a Dynamic Local Access Licence (DLAL) or a Dynamic Spectrum Access Licence (DSAL). These licences enable the same enforcement mechanisms and day-to-day operational relationships as the existing LALs and SALs. Unlike LALs, and SALs, however, they are not limited to specific sites, radios, technical parameters (e.g. transmit power, antenna height, etc.), or spectrum assignments. The licence permits spectrum usage only when a spectrum assignment is later obtained, for a given radio, from a Dynamic Spectrum Access (DSA) Server.

A DSA Server automatically computes spectrum assignments for radio base-stations to transmit without causing harmful interference to other licensees.

The functionality of the DSA Server is summarised as follows:

1. A DSA Server would assign frequencies to equipment (e.g. 5G radio base stations) – these frequencies would then be used for communications between the base station and connected devices (e.g. mobile handsets, fixed wireless access terminals on

homes, TV cameras). Without a spectrum assignment from the DSA Server, the radio base station would not be licensed to operate.

2. The DSA Server would determine spectrum assignments taking account of existing users using coexistence algorithms (defined by Ofcom) to determine the permissible transmit power in each frequency channel to avoid causing harmful interference.
3. Inputs on the usage of spectrum by the national mobile operators in the LAL bands would be provided by Ofcom and/or the national mobile operators directly, making timely account of ongoing changes. Inputs on existing LAL licences would come from Ofcom.
4. Inputs on the usage of spectrum by other SALs, and other licensees (e.g. fixed point-to-point links) in the SAL bands, would be provided by Ofcom.
5. It is envisaged there would be multiple DSA Servers, provided by industry[1], which may need to exchange some information to ensure consistency.
6. A base-station using an LAL band is required to immediately discontinue using a frequency channel if the licensed mobile operator begins using that channel in the vicinity. The base-station, or its controlling software, must automatically maintain contact with the DSA Server to receive instructions to discontinue, or to ‘hop’ onto a different spectrum assignment.
7. A base-station using a SAL band has no need to react immediately to ongoing changes in others’ usage. A human may obtain a spectrum assignment from the DSA Server via a web page and manually configure the base-station to use it. An automated approach may also be used if the particular devices have the capability.
8. Any radio equipment connected to the database (e.g. 5G private base station) could also be equipped with sensors to determine the nearby usage by priority users (e.g. mobile operators) and feed this information to the DSA Server. This enables a “Coordinated Sense & Avoid” mechanism, whereby the DSA Server combines measurements – from all devices from all licensees – with the inputs provided by Ofcom and mobile operators to form an accurate and up-to-date picture of nearby usage in the frequency band, and to react immediately to any changes. This could also enable the algorithms used in the DSA Server to not be overly conservative in respect of predicting interference, since there would be a further interference protection mechanism in specific locations where the existing (priority) user signals travelled further/are higher in signal strength than predicted by the algorithms.

[1] This is a similar approach to that proposed by Ofcom for introducing DSA in the 6GHz band – see Ofcom, ‘Expanding access to the 6 GHz band for mobile and Wi-Fi services: Proposals for AFC in Lower 6 GHz and mobile / Wi-Fi sharing in Upper 6 GHz: Consultation’, 13 February 2025.

3.3 DSA Server Components

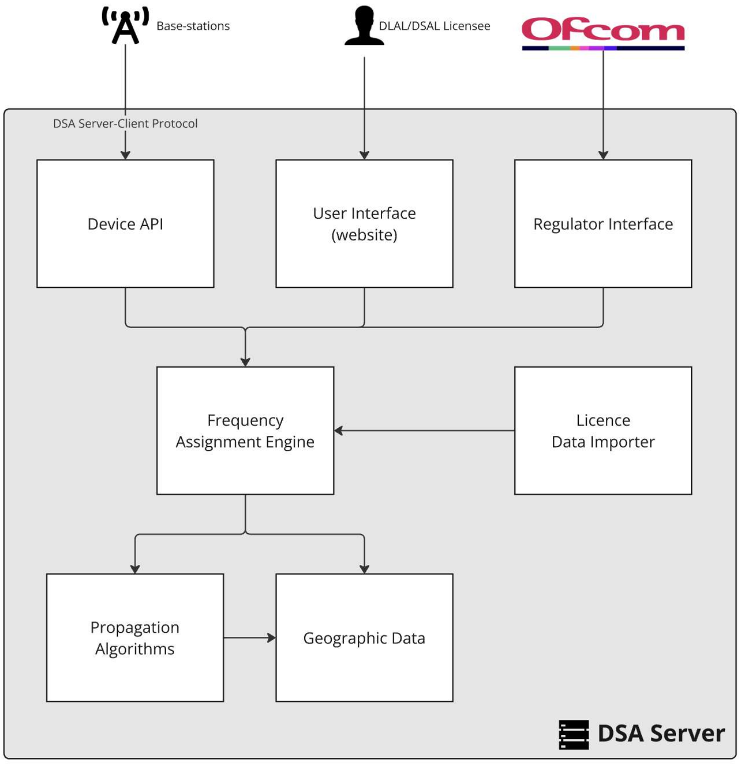


Figure 6: Schematic of DSA server components

1. The **Frequency Assignment Engine** implements Ofcom's methodologies for computing frequency assignments. For DSALs this sandbox implements Ofcom's published methodology for SALs [24]. No such method is published for LALs, so for DLALs this sandbox implements a prototype methodology described in the Spectrum Sharing Mechanism [Annex A, Deliverable 1.2], with the expectation that this will be superseded in due course by an Ofcom methodology.
2. The **Device API** provides endpoints for devices, or software acting on their behalf, to exchange automated messages with the DSA Server, according to the DSA Server-Client Protocol described in section 3.4, with the implementation and a worked example shown in section 3.5.
3. The **User Interface** allows human users to request frequency assignments (for SALs), and to onboard their radio devices with the DSA Server and obtain authentication tokens.
4. The **Regulator Interface** module provides a means for Ofcom to query the DSA Server as part of routine management processes, and to support interference investigations.
5. The **Licence Data Importer** maintains up-to-date information on other licensees and their usage. It is anticipated that Ofcom will directly provide data to an operational DSA Server; for the purposes of the sandbox, the DSA Server uses publicly-available data. For SALs, the Wireless Telegraphy Registry (WTR) is periodically imported. For LALs, MNO coverage maps are periodically imported, and augmented as described in section 3.7.

6. The **Propagation Algorithm** module implements a series of RF propagation models. For this sandbox, the ITU-R P-452 and ITM Longley-Rice models are implemented; other models can be incorporated in future.
7. The **Geographic Data** module contains data describing terrain elevation (using the SRTM dataset), geographic borders, administrative boundaries, and urban/rural classifications. Other modules query this data where needed.

3.4 DSA Server-Client protocol design

The DSA Server-Client Protocol was developed over two milestones. [FW-MS4] surveyed several protocols for DSA Server-Client interactions and were compared against the requirements for the DSA Server-Client Protocol [FW-MS2] to identify which of three different protocols ([19], [20], [21]) currently cover the requirement.

1. When one or more protocols cover the requirement, then (one of) that message, method, or data object is proposed for adoption herein.
2. When no protocol covers the requirement, then a new message, method, or data object is proposed for adoption herein.
3. When appropriate, extensions from other standards bodies are adopted and extended, e.g., [22].

[FW-MS17] built on [FW-MS4] and differs in the following:

1. [FW-MS4] focuses solely on supporting Operator access to Band 3 spectrum

2. Protocol requirements and analysis of ability of existing DSA protocols to support the requirements remain in [FW-MS4]

3. [FW-MS17] applies to any SAL or LAL band with messaging and defined responses to conditions added to address limitations of [FW-MS4] as extended to additional LAL and SAL spectrum.

4. [FW-MS17] reorganises much content in [FW-MS4] given the assumptions that licence-exempt operation is not being supported, that Ofcom is ultimately granting initial DLAL & DSAL licences, and that both DLAL and DSAL should be able to implement coexistence / TDD alignment functionality.

3.4.1 Protocol Overview

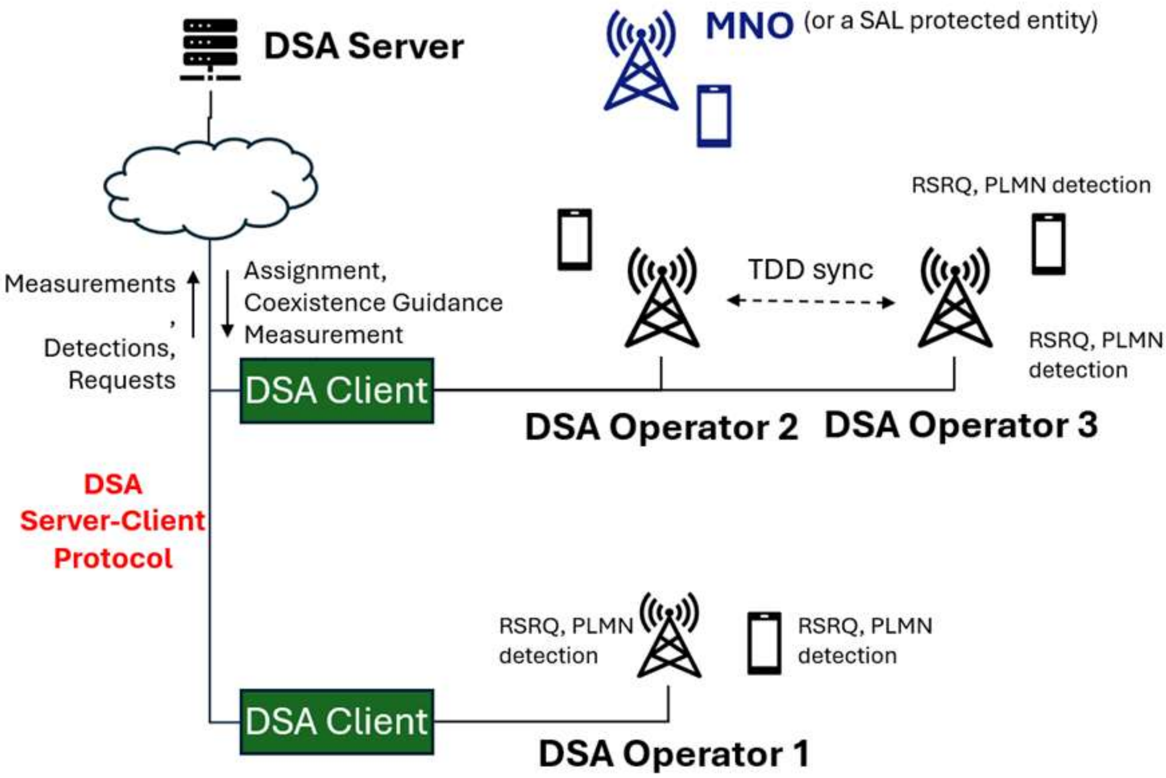


Figure 7: DSA Ecosystem where the focus of this document is the requirements for DSA Client / Server Interactions via the DSA Server-Client Protocol (red)

This project's spectrum sharing mechanism is akin to a traditional centralised DSA solution as shown in Fig. 6, with 'DSA Server' being the generic term for a SAS, AFC, Database or other centralised controller, and 'DSA Client' referring to the software that directly controls the spectrum usage for a single device or collection of devices. To this, the project adds the following:

1. First, sensed detections of changes in protected systems are primarily provided by the secondary systems (DSA Operators) rather than by dedicated sensors (e.g., ESC) - "Coordinated Sense and Avoid"; see Section 2.3.2;

2. Second, those same measurements are used to update models of MNO coverage; see [Deliverable 1.2].

3. Third, the DSA Server is intentionally multi-jurisdictional in that rules and protections enforced by the DSA Server depend on the spectrum accessed by the DSA Operators, e.g., SAL vs LAL or potentially across countries.

Key to any automated DSA is the **Protocol** by which the DSA Clients and DSA Servers communicate (highlighted in red in Fig. 6). In this section we consider this protocol in detail.

3.4.1.1 Protocol Objectives

The protocol is designed to support the following concepts and objectives:

1. Coordinated Sense and Avoid (Section 3.4.2);
2. Streamlined Access (Section 3.4.3);
3. Minimising Ecosystem Impact (Section 3.4.4);
4. Improving Sharing Capacity (Section 3.4.5).

3.4.1.2 DSA Client-Server Protocol Dialogue

It is helpful to summarise informally the sequence of messages between a DSA Client and a DSA Server as the following conversation:

Registration

Client: “My device has this location and these technical parameters” (antenna, height AGL, etc.)
Server: “Acknowledged”

Spectrum Inquiry

Client: “What spectrum is available to my device?”
Server: “You can use Channels A and B at 40dBm, or D at 20dBm, but don’t use C.”

Grant Request

Client: “Please can my device use channel B at 40dBm?”
Server: “Yes, you are now authorized to transmit for the next 24 hours, as long as you check with me every 10 minutes”

Heartbeat Request

Client: (every 10 minutes) “My device is using channel B, is this still OK?”
Server: “Yes, keep going” OR “No, stop transmitting immediately and start again.”

Relinquish Grant

Client: “My device won’t use channel B any more.”
Server: “Acknowledged.”

Requests can also include **Measurement Reports:**

Client: “My device just detected a device with PLMN 123 in channel B, with RSSI of -123dBm, etc.”
Server: “Acknowledged. Stop using channel B immediately and start again”.

3.4.2 Protocol support for coordinated sense and avoid

In Coordinated Sense and Avoid (see Section 2.3.2), the DSA Operators provide regular observations to the DSA Server as **Measurement Reports,** either within Spectrum Inquiry, Grant Request, or Heartbeat Request messages. Each message can contain many Measurement Reports, describing many other spectrum users and/or repeated measurements of the same spectrum user. If these messages indicate a change in a protected licensee, then the DSA Server adjusts or revokes the assignments of all operating base-stations in the area to **avoid** interference in a **coordinated** manner, potentially across multiple DSA Operators.

The DSA Client will send a Heartbeat Request every 10 minutes (or similar interval as defined by Ofcom). In scenarios where measurements of new nearby MNO usage are included in the Heartbeat Request, the DSA Server will reply to indicate that the spectrum assignment is no longer valid. Furthermore, in scenarios where Radio B has measured new MNO usage since the nearby Radio A's last Heartbeat, then the DSA Server will also respond to Radio A's next heartbeat (which may not include any Measurement Reports) to indicate that its spectrum assignment is no longer valid.

See Section 3.6 for real-world examples of Measurement Reports.

3.4.3 Streamlining access

In various commercial bands a cloud-based DSA Server has been shown to perform the necessary calculations to determine availability in near real time or in a handful of seconds ([5GNT] for SAL). For LAL spectrum access, current processes mandate approval by the incumbent MNO. By mandating and demonstrating the success of Coordinated Sense and Avoid in LAL spectrum (prototyping in Band 3), we believe regulatory updates could be made to eliminate the MNO approval step thereby achieving similar streamlined access.

3.4.4 Minimising ecosystem impact

The proposed sharing framework assumes that secondary operators still apply for and receive licences to operate via Ofcom's existing licence management framework, thereby permitting the continued use of backend licence handling and enforcement mechanisms. These licences may place restrictions on operation, e.g., areas, bands, maximum transmit power, but details on assignments are deferred to the DSA Server which is expected to have access to the licences to ensure spectrum assignment consistency.

The WINNF SAS-CBSD Protocol [27] serves as the starting point for the DSA Server-Client Protocol with extensions for applying TDD Coexistence [22] and extended measurement reporting capabilities. This means that the same (De)Registration, Inquiry, Grant Request/Relinquish, and Heartbeat structure is adopted with Heartbeats with adaptive timeouts used for enforcing measurement freshness. This messaging structure is extended with just a handful of field extensions specified in [CBSD Measurements] for implementation extensions that we exploit here (e.g., measReportConfig and GroupParam). A handful of fields are mapped over for band agnosticism (e.g., cbsdId to deviceId) and multi-jurisdictional endpoints are added (e.g., for SAL and LAL). For consistency with existing rules, the currently implemented DSA Server does not permit a single grant to cross jurisdictional boundaries (e.g., combining a LAL and a SAL), but a DSA Operator may have multiple grants, each under received their own specific rules, that the DSA Operator can aggregate on its end.

The mechanism by which measurements are taken is not mandated in this framework and can come from UEs, gNBs, or dedicated sensors. For 3GPP compatibility, the required measurements for access and coexistence (PLMN, cell ID, signal strength) are most easily achieved at the UEs, which already capture these fields before network attachment from broadcast MIB and SIB1 data. UEs also provide the possibility for sampling a wider variety of locations. [CBSD Measurements] is further extended to permit any Request to include measurement capabilities or reports and any Response to include measurement requests so that non-transmitting systems can also report measurements, which is implicitly required as a bootstrapping step when a DSA Operator seeking a LAL band grant is the first to operate in an area.

3.4.4.1 CBRS extensions

While CBRS was designed explicitly for the US 3.55-3.7 GHz spectrum sharing problem, it defined a number of mechanisms for open-ended extensions collectively by industry or standards bodies or by individual vendors. In particular, this project made the following extensions:

1. Measurement Reports are extended to support PLMN reporting, which the DSA Server can correlate with MNO operations
2. Coexistence Group operations are extended to support TDD alignment with non-cooperative systems (e.g., MNOs or grandfathered SAL systems)
3. Multi-band / multi-jurisdiction support is added.

The latter enables support for variation in access rules via a common DSA Server. As an example, for a multi-jurisdiction DSA Server operating behind a single base domain name *sas.example,* the jurisdiction may be provided in an HTTP header *X-Jurisdiction-Id*, and the dialect in the URL (right of the slash): *https://sas.example/techuk-gbr-sal-v1* with *X-Jurisdiction-Id: gbr-sal*.

3.4.4.2 Automated Inter-Network interference management

As noted in the preceding, TDD alignment across systems can significantly improve shared spectrum access (see Fig. 1), Ofcom stated a requirement for future SAL systems to align TDD but has not provided a mechanism [5]. Here, the DSA Server-Client protocol adopts the TDD / group management methods of [9] and [10]. This is further extended by allowing groups to align TDD information with protected MNO systems by recovering broadcast information from the MNO when they are within range. Thus, in this mechanism, spectrum availability gains come from alignment among secondary systems, with primary systems, and for both TDD LAL and SAL spectrum bands.

3.4.5 Improving sharing capacity

To improve sharing capacity, the DSA Server-Client protocol provides TDD alignment (timing and parameters) within groups, estimates of MNO Coverage are improved with measurements, and the project is performing simulations and field measurements to improve modeling parameters.

3.4.5.1 TDD alignment

As TDD alignment can significantly improve shared spectrum access Ofcom stated a requirement for future SAL systems to align TDD but has not provided a mechanism (see [Ofcom 2204]), Here, the DSA Server-Client protocol adopts the TDD / group management methods of [22]. This is further extended by allowing groups to align TDD information with protected MNO systems by recovering broadcast information from the MNO when they are within range. Thus in this mechanism spectrum availability gains come from alignment among secondary systems, with primary systems, and for both TDD LAL and SAL spectrum bands.

3.4.5.2 Improved parameter estimate accuracy

Parameters used within the DSA Server were also studied, but are covered in the WP2 section of the report.

The capacity of traditional centralised / predictive DSA solutions depends on how accurately protected and secondary system operations are modeled, which in turn influences how much interference margin is needed to achieve the desired protection assurances. Examples include accurate antenna and site modeling, propagation modeling, and setting the appropriate interference protection thresholds.

The DSA Server-Client Protocol is envisioned as operating as part of a broader ecosystem of components as shown in Fig. 6 (above) where the protocol itself is highlighted in red. The protocol is intended to support direct communications between a DSA Server and DSA Client or communications via a proxy for multiple client devices, such as may be hosted at an Operator's Network Management System (NMS).

This protocol considered herein can be complementary to existing Shared Access Licence (SAL) and Local Access Licence (LAL) processes, which has the following properties:

1. A DSA Operator acquires a "DLAL" (Dynamic LAL) or "DSAL" (Dynamic SAL) licence from Ofcom, specifying a band and a geographic region, and, optionally, ranges for other technical parameters (e.g. antenna height).
    a. The DLAL or DSAL licence confers the right to transmit within operational parameters specified by a "DSA Server", in response to requests for specific frequencies, locations, and technical parameters, within the ambit of that licence, for a specified time period.
    b. The DSA Server implements custom DLAL algorithms (using parameters derived in WP2) for:

i. Granting spectrum access to protect **current** primary licensee usage

ii. Incorporating gNBs' and UEs' spectrum measurements for "Centralised Detect & Avoid" reported via DSA Clients, to protect **evolving** primary licensee usage in real time

Milestone 4 [FW-MS4] and Milestone 17 [FW-MS17] documented protocols for the DSA Server / Client coordination where [FW-MS17] builds on [FW-MS4] and differs in the following:

1. [FW-MS4] focuses solely on supporting Operator access to Band 3 (LAL) spectrum

2. Protocol requirements and analysis of ability of existing DSA protocols to support the requirements remain in [FW-MS4]

3. [FW-MS17] applies to any SAL or LAL band with messaging and defined responses to conditions added to address limitations of [FW-MS4] as extended to additional LAL and SAL spectrum.

4. MS17 reorganises much content in [FW-MS4] given the assumptions that licence-exempt operation is not being supported, that Ofcom is ultimately granting initial DLAL & DSAL licences, and that both DLAL and DSAL should be able to implement coexistence / TDD alignment functionality.

3.4.6 Design choices

3.4.6.1 Message encoding and transport

All surveyed protocols support the same basic approach to message encoding and transport, which are adopted herein.

1. All messages are JSON objects and transported using HTTPS (HTTP plus TLS).
2. A message shall contain one JSON object, noting that [26] supports arrays for the support of multiple devices behind a proxy or multiple configuration or other scenarios where such use is advantageous to the DSA Server-Client Protocol
3. All messages are sent to a URL of the format $BASE_URL/ $METHOD where:
    a. BASE_URL is the path to the DSA Server
    b. METHOD corresponds to one of the METHODS listed below where Clients issue Requests and Server Issues Responses.

METHOD	Request message	Response message
Inquiry	Inquiry Request message	Inquiry Response message
Grant	Grant Request message	Grant Response message
Heartbeat	Heartbeat Request Message	Heartbeat Response Message

Figure 8: Supported methods

1. HTTP version number shall be 1.1 as specified in [1], or a later version using HTTP POST.
2. HTTP Request messages include:
   a. host: <DSA Server host name included in $BASE_URL>
   b. contentType: application/json
3. HTTP Request messages include the DSA Server time on which all interface timers are based.
4. TLS-v1.2 or later shall be performed for mutual authentication, prior to any communication. Subsequent to successful authentication, the Client and Server shall negotiate a ciphersuite to use for encrypting all communications between the two entities where the supported list includes:
   a. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
   b. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
5. A "character" may be one or more bytes depending on the message's string encoding as defined in the HTTP header, e.g. *Content-type: application/json; charset=utf-8* may contain characters which occupy 1-4 bytes; wherever character lengths are specified in this specification, this applies to the number of characters not the number of bytes.

3.4.6.2 Server authentication

The DSA Server must present a valid TLS certificate which has been signed by a widely-trusted public Root Certificate Authority. Each device must trust any server certificate which is signed by a widely-trusted public Root Certificate Authority (i.e. must be pre-loaded with their public keys). The device must check that the provided server certificate matches the domain name in the URL it is connecting to. It is the responsibility of the operator to ensure that the URL specified corresponds to a DSA Server which has been authorised by the relevant regulator.

3.4.6.3 Client authentication

Two alternative methods are acceptable, with the first being the more secure, the second the more convenient.

3.4.6.3.1 Client certificates

Each equipment manufacturer maintains a Certificate Authority ("CA") in its own right, along with ancillary services such as a Certificate Revocation List ("CRL"). The certificate of the CA must have been signed by a widely-trusted public Root Certificate Authority. Each device has a unique certificate which has been signed by its manufacturer's CA. The unique identifier of the device is embedded within the certificate's metadata (e.g. the Common Name). The manufacturer must provide the public key of its CA to the DSA Server, along with the means to obtain its CRL. The DSA Server must trust any certificate signed by a trusted manufacturer CA, and reject any request which either does not present a suitable certificate, or which presents a certificate which has an embedded device identifier which does not match the identifier in the body of the request.

Note that, unlike CBRS, there is no centralised Root CA which is specific to a particular Dynamic Spectrum Access ecosystem.

3.4.6.3.2 Shared secret

If the above client-certificate method is not possible for some reason, the DSA Server may elect to fall back on a Shared Secret method. The manufacturer and/or operator of a particular device agrees with the DSA Server on a unique string token for that device, by an out-of-band process. The device must present the token as a Bearer Token in the HTTP header of each request to the DSA Server. The DSA Server must reject any request which does not present a valid token, or which presents a token which is associated with a different device to that specified in the body of the request.

3.4.6.4 Coexistence management

To increase the capacity of DSA devices with secondary access rights, the messages of *GroupInfo*, *CoexMeasInfo*, and *GroupConfigInfo* from [22] are adapted for use for exchanging BroadcastInfo, coordinating timing alignment, and extending measurement capabilities. While strictly beyond the scope of this protocol document, the spectrum organisation of secondary DSA devices is assumed to follow the basic structure shown in Figure 2 of [22], which is summarised as follows:

1. A CxM groups together DSA devices (GAA CBSDs in [22]) in a CxG where all members adhere to a common coexistence policy – a TDD frame structure and an effectively common timing standard (commonly Temps Atomique International, which may be accessed via GPS< GNSS, PTP, and NL).
2. A specific set of TDD frame structures for LTE and 5G NR (both 15 kHz SCS and 30 kHz SCS) are mandated for support, though a CxG may implement any agreed to 3GPP supported frame structure
3. Within a CxG, subgroups of ICGs, normally by operator, may self-organise to facilitate further relaxed interference management amongst the ICGs
4. CxGs provide to the CxM information on the devices support and desire for specific frame structure and measurements about their environment (sometimes at the direction of the CxM), which the CxM can use to detect interference and further optimise coexistence among GAA CBSDs.

For the DSIT Spectrum Sandbox, the following changes in operation are expected, some of which are reflected in the protocol:

1. Mandated support for an U/D split of 2/1 as it’s the most common B3 configuration.
2. To facilitate closer packing with MNOs / higher capacity, the MNO’s effective interference policy is enforced in areas near the MNO’s operational footprint or anticipated footprint
3. PLMN information is added to the *SignalInfo* object in [22], which is expected to be recoverable from SIB1 fields. This supports DSA device reporting of MNO detection. A similar extension could be defined for DSA device incumbent detection in bands where the primary system transmits a non-EUTRA signal.
4. Other protocol specific fields are adapted as needed, e.g., *GroupId* in *GroupParam* is changed from CBRS_ALLIANCE to DSIT_SANDBOX.

3.4.6.5 DSAL/DLAL licence information

In a Grant Request, the DSA Client must provide licence information for the authenticated DSA Operator holding the licence.

3.4.6.6 Endpoints

3.4.6.6.1 Jurisdiction & protocol dialect fields

A particular DSA Server operator may reasonably be expected to operate in multiple jurisdictions, and have their software support multiple dialects. They may prefer to operate one ‘multi-tenant’ DSA Server which serves all such jurisdictions, or multiple ‘single-tenant’ DSA Servers which serve one jurisdiction each with the same underlying software. Independent of tenancy, they may prefer to expose distinct URLs for each jurisdiction, or the same URL for all. Internal routing decisions may depend on the jurisdiction, and how the body is parsed may depend on the dialect; defining such fields in the request body is therefore not appropriate.

Two fields describe a) which regulatory jurisdiction the request pertains to; b) which dialect of this protocol the device expects to use. The DSA Server will validate a) whether it supports this jurisdiction; b) whether it supports this dialect; c) whether this dialect is appropriate for this jurisdiction. The DSA Server will then subsequently validate the body of the request according to the given dialect, and will ensure that any geolocations lie within the bounds of the given jurisdiction.

Each dialect may impose more stringent constraints on whether a given field is Optional, Conditional, Required, or Ignored. Each dialect may apply a more specific definition to a given field. Each dialect may include its own custom fields.

This protocol does not place constraints on such choices; consequently there are deliberately no *jurisdictionId* or *protocolDialect* fields in the body of protocol requests; this information should be provided to the server in the HTTP headers and/or left-of-slash URL domain name and/or right-of-slash URL path, or left implicit if appropriate. It is left to the DSA Server operator to make the most appropriate choice according to their architecture.

As an example, for a multi-jurisdiction DSA Server operating behind a single base domain name *sas.example,* the jurisdiction may be provided in an HTTP header *X-Jurisdiction-Id*, and the dialect in the URL (right of the slash): *https://sas.example/techuk-gbr-sal-v1* with *X-Jurisdiction-Id: gbr-sal*.

For the purpose of prototyping in the QMUL DSIT Spectrum sandbox, the DSA Server supports the following dialect URLs for DSALs and DLALs, respectively:

1. *http://ec2-35-176-164-3.eu-west-2.compute.amazonaws.com:5003/techuk-gbr-sal-v1*
2. *http://ec2-35-176-164-3.eu-west-2.compute.amazonaws.com:5003/techuk-gbr-lal-v1*

3.4.6.6.2 Message endpoints

The following endpoints in the protocol are supported by the protocol where {dialect} corresponds to DSAL or DLAL paths, e.g., as described in the preceding. communications flows as requests (POST messages) from DSA Client to DSA Server and responses (payloads and REST codes) where all message payloads are JSON objects. Optional payloads are available for conveying / requesting Measurement Reports (e.g., incumbent detection) and to coordinate coexistence (TDD alignment) that can be added to any request or response.

Table 5: Endpoints exposed by the DSA server

Endpoint	Endpoint Path	Purpose
Deregistration	/{dialect}/deregistration	DSA Client removes its deployment configuration details from the DSA Server
Grant	/{dialect}/grant	DSA Client requests spectrum for use in a particular band according to its registration details
Heartbeat	/{dialect}/heartbeat	DSA Client renews spectrum grant and receives updated guidance, if available, and timing for the next heartbeat
Registration	/{dialect}/registration	DSA Client provides its deployment and configuration details (e.g., location, antenna details, SAL / LAL credentials)
Relinquishment	/{dialect}/relinquishment	DSA Client returns the spectrum in its grant(s) back to the pool managed by the DSA Server
Inquiries	/{dialect}/spectrumInquiry	DSA Client asks the DSA Client about the availability of spectrum in the specified band according to the configuration data associated with its registration.

3.4.6.6.3 Sample payload

The payloads for the protocol are defined in [FW-MS17] as hierarchical JSON objects. The following shows an example payload - SignalInfo - that can be embedded as part of several messages - and is important to realising the Coordinated Sense and Avoid concept.

SignalInfo objects are sent to describe a DSA Client's own transmitted signals and measured / detected signals in Measurement Reports. PLMN info is required for messages conveying information about the DSA Client's own signals (contained in *CoexCellInfo)* and optional in measurements (*CoexMeasInfo*).

Table 6: SignalInfo object definition

Parameter	R/O/C	Parameter Information

NAME: eutraInfo DATA TYPE: object: EutraInfo	Required	Indicates information on an E-UTRA signal or E-UTRA compatible NR signal.

Table 7: EutraInfo object definition

Parameter	R/O/C	Parameter Information
NAME: signalEarfcn DATA TYPE: number	Required	Indicates the EARFCN of the LTE signal or NR-ARFCN of the NR signal. For signalRat = LTE, permitted values are integers between 55240 and 56739 inclusive. For signalRat = NR, permitted values are even integers between 636668 and 646666.
NAME: signalRat DATA TYPE: string	Conditional	Indicates the RAT associated with the signal. When used in cellInfot, the allowed values are “LTE” and “NR”. Otherwise, allowed values are “LTE”, “NR”, and “UNKNOWN”. This parameter shall be included if used in the cellInfo parameter.
NAME: signalPci DATA TYPE: number	Conditional	Indicates the PCI associated with the signal. For signalRat = LTE, permitted values are integers between 0 and 503 inclusive. For signalRat = NR, permitted values are integers between 0 and 1007 inclusive. This parameter shall be included if the EutraInfo object carries information of the transmitted signal. This parameter shall be included if used in the cellInfo parameter.
NAME: signalEcgi DATA TYPE: string	Conditional	For signalRat = LTE, indicates the ECGI associated with the signal. It is a string of length 52, containing 0’s and 1’s. For signalRat = NR, indicates the NCGI associated with the signal. It is a string length 60, containing 0’s and 1’s. This parameter shall be included if the EutraInfo object carries information of the transmitted signal. This parameter shall be included if used in the cellInfo parameter.
NAME: signalBandwidth DATA TYPE: number	Required	Indicates the bandwidth of the signal. Bandwidth of the signal is in 100’s of kHz (E.g. number 200 indicates bandwidth of 20MHz).
NAME: plmn DATA TYPE: number	Conditional	Indicates the PLMN ID of the associated signal in a MeasurementReport message. Required when describing a DSA Client’s own signal.

3.4.6.6.4 Further design details

For further details on the design of the protocol, please refer to [FW-MS17].

3.5 Device API - implementing the protocol

Implementation, integration, and testing were reported across [FW-MS7], [FW-MS9], [FW-MS10], and [FW-MS14]. The following extracts artifacts from those milestone reports illustrating the supported endpoints, message exchanges across the protocol and internal logic within the DSA Server.

Swagger is a popular tool to create auto-documentation of REST endpoints, methods, and data objects while also providing an interface to facilitate 3rd-party integration. This is used in the following to document implementation.

3.5.1 Endpoints

Fig. 7 shows the top-level end-points for the DSA server as a screen grab of a Swagger dump of the Server endpoints. These are used in the following to further illustrate

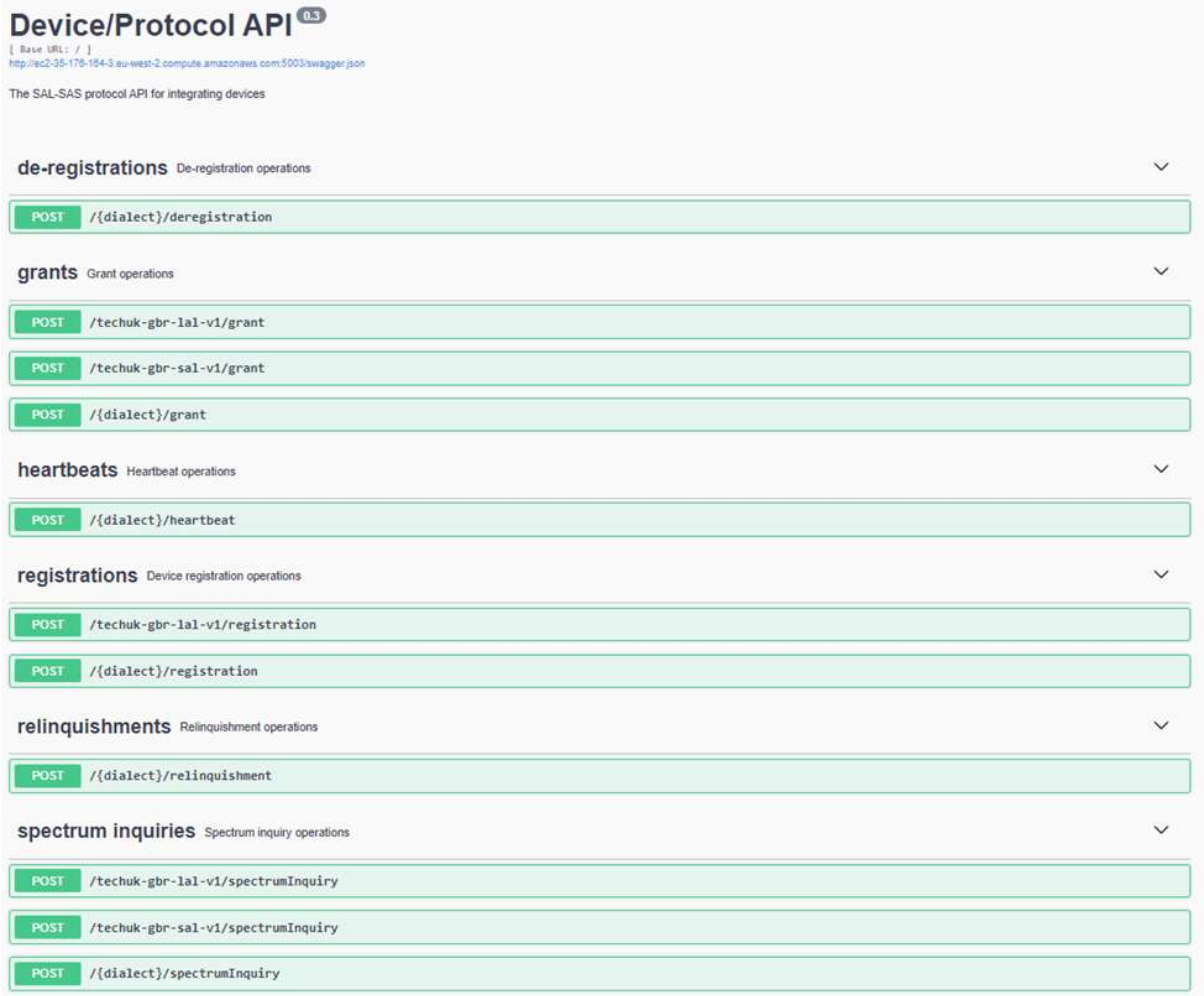


Figure 9: Top level swagger listing of server endpoints

3.5.1.1 Data object model support

As part of the development process, the auto-generated swagger implementation also hosts models of all of the data objects used in the protocol exchange including a listing of fields, types, and descriptions with a partial listing of data objects in Figure 10 and a listing of LAL-dialect specific data objects models in Figure 11. In addition to providing documentation, these models can be used by a client developer in constructing their protocols. Note that the captures below conform to the data objects in version 1.2 of the DSA protocol that was in place when documented at the time.

Figure 10: Selected Data Object Models

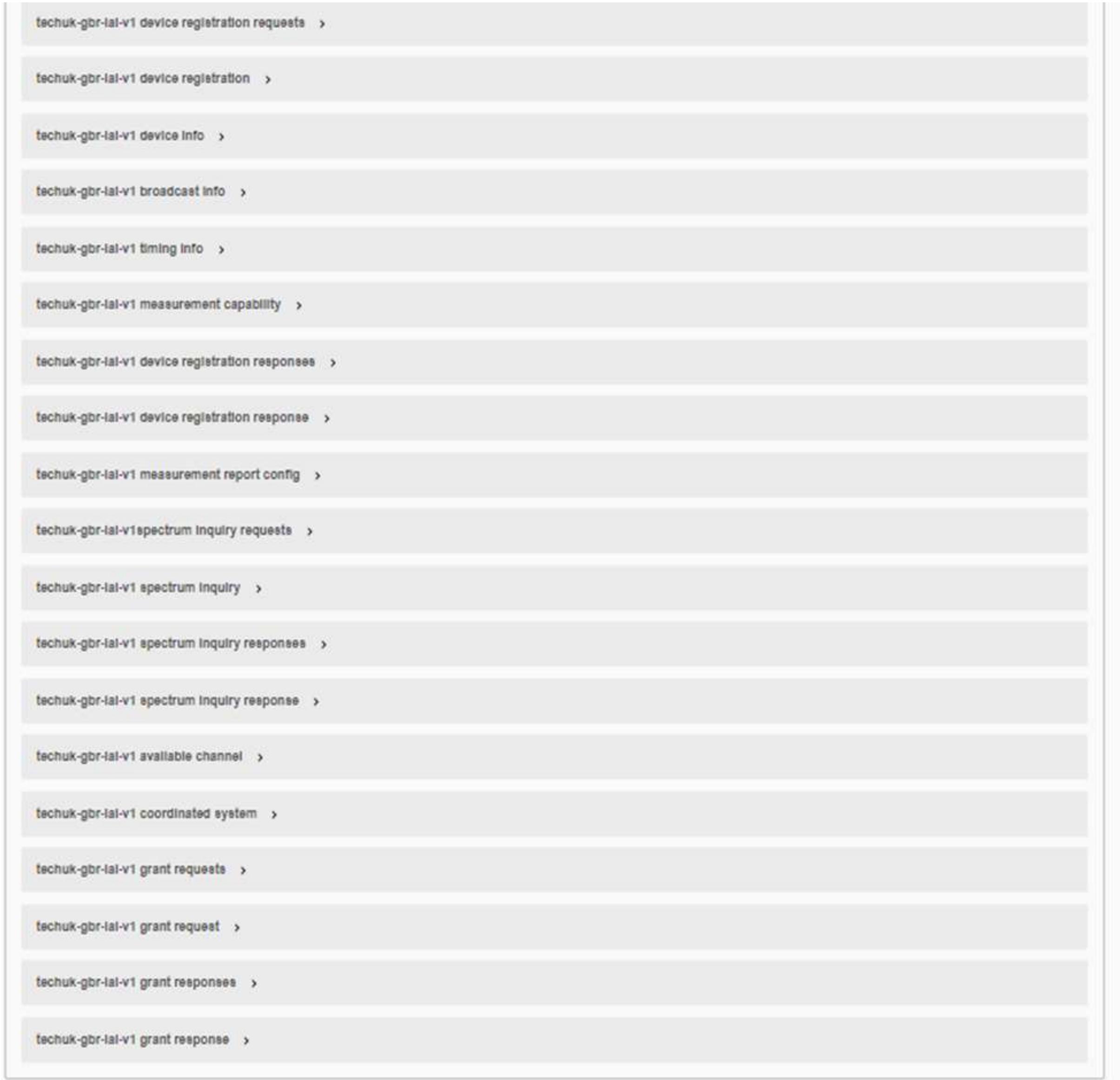


Figure 11: LAL Dialect Data Object Models

3.5.2 Captured sample message exchanges

The following are screen shots from the swagger interface of requests (from a test DSA Client) and the responses from the DSA Server for each endpoint in the protocol [FW-MS4]. Note that each swagger endpoint can be used to post test requests with varying data objects and view the DSA server response facilitating test and client development.

3.5.2.1 De-registration request and response

A de-registration request is used to remove a DSA-Client from consideration in the system.

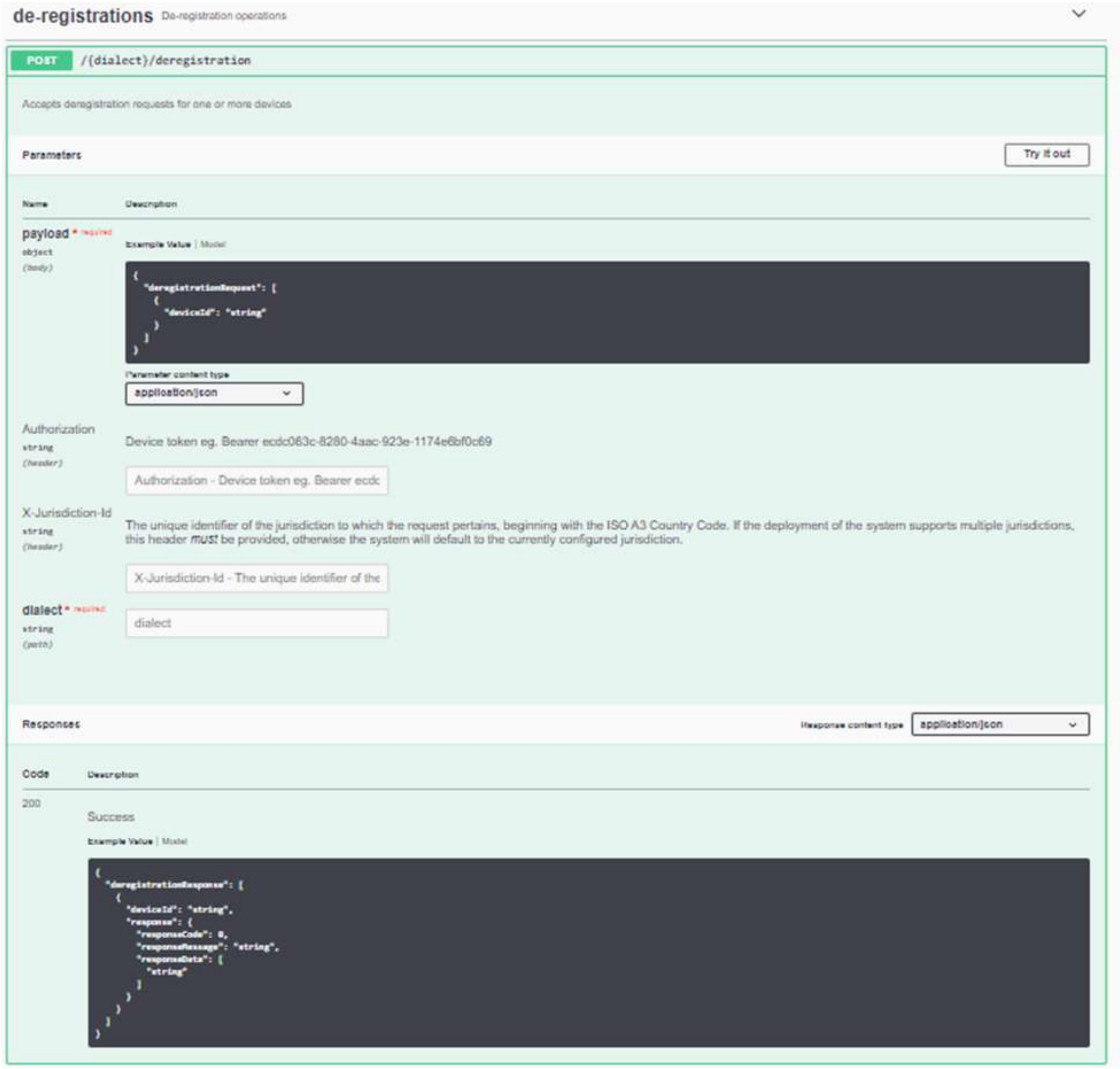


Figure 12: De-registration Request and Response Swagger Dump

3.5.2.2 Grants request and response

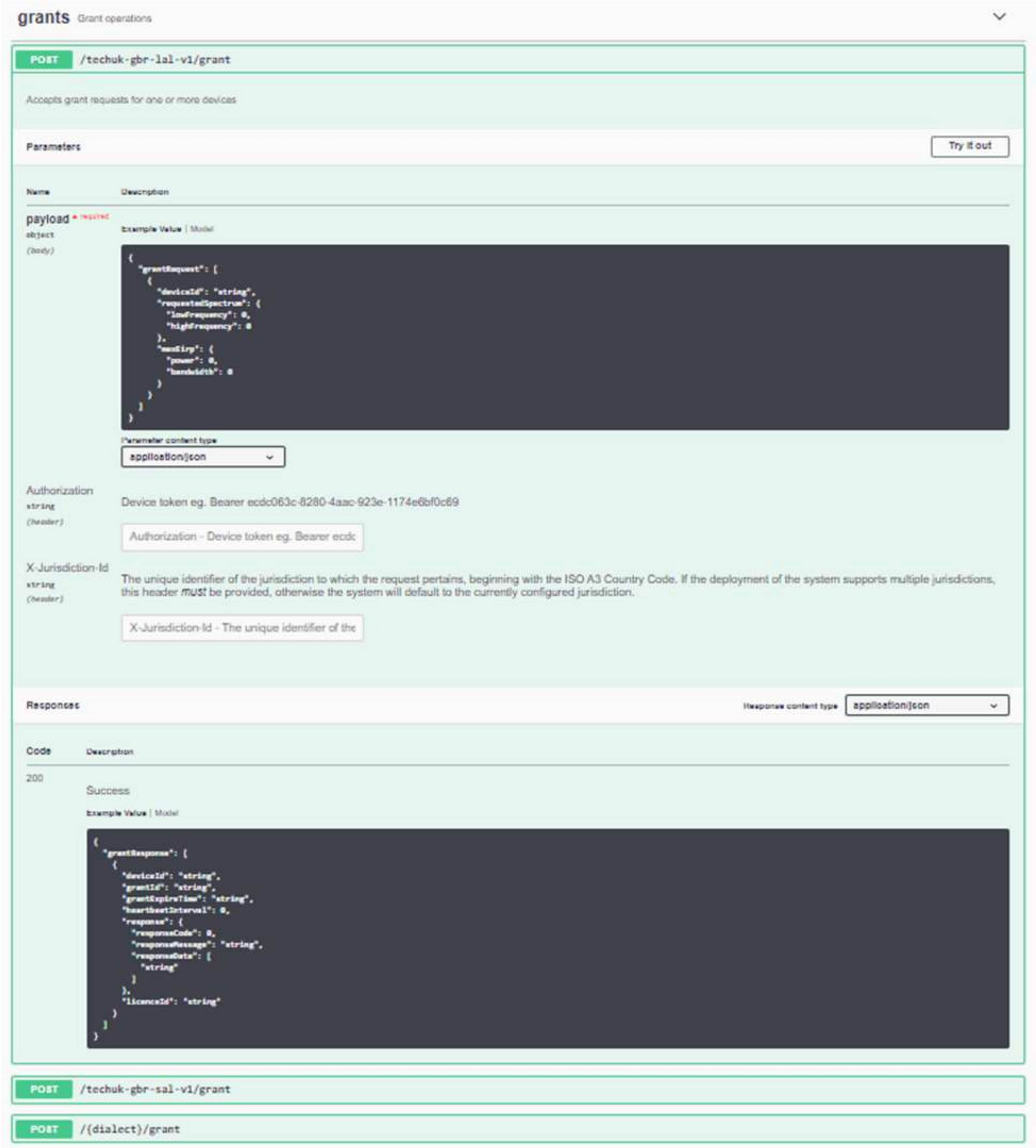


Figure 13: Spectrum Requests Swagger Dump for LAL dialect

3.5.2.3 Heartbeat request and response

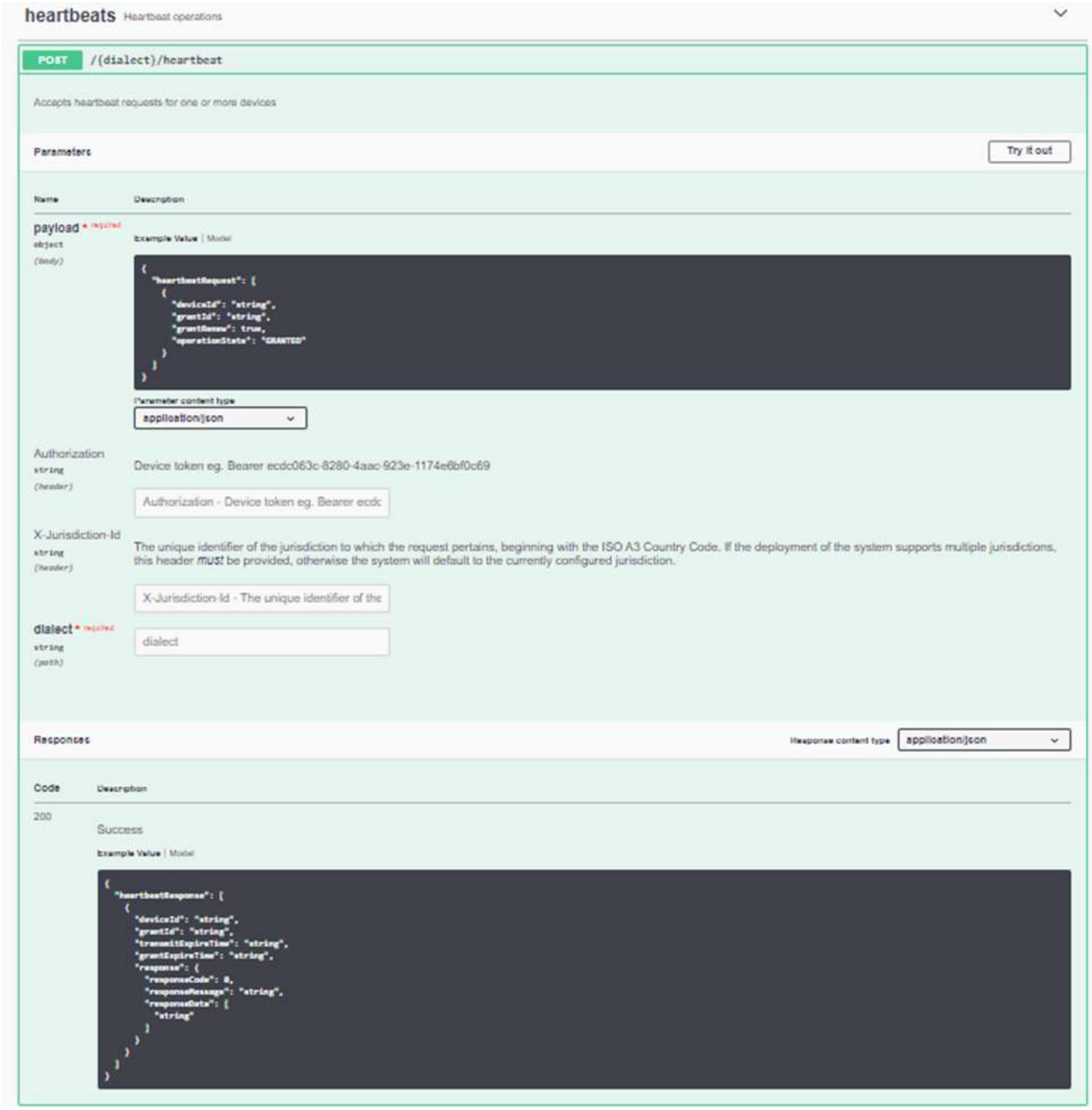


Figure 14: Heartbeat Requests Swagger Dump for LAL dialect

3.5.2.4 Registration request and response

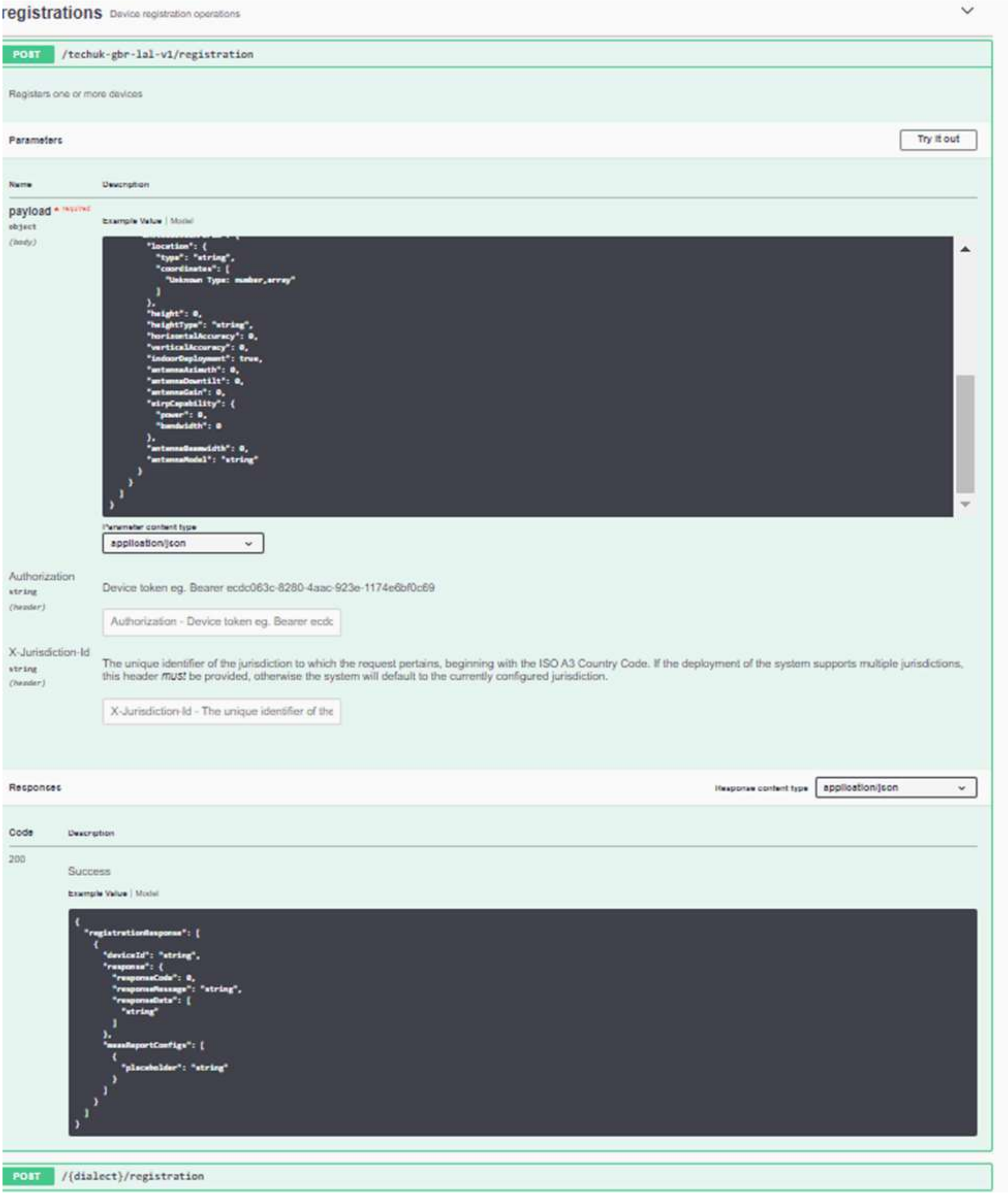


Figure 15: Registration Requests Swagger Dump for LAL dialect

3.5.2.5 Relinquishment request and response

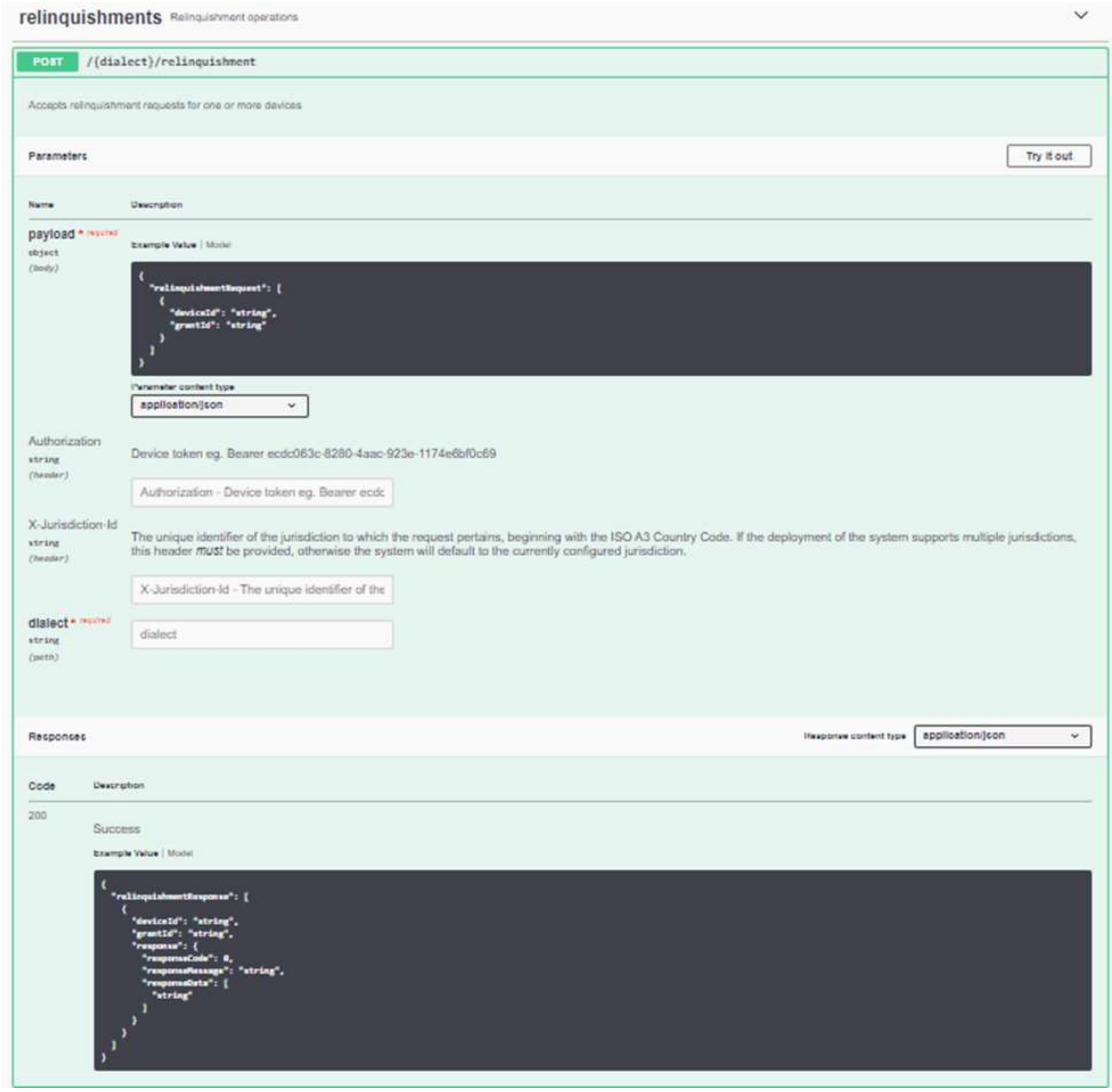


Figure 16: Registration Requests Swagger Dump for LAL dialect

3.5.2.6 Spectrum inquiry request and response

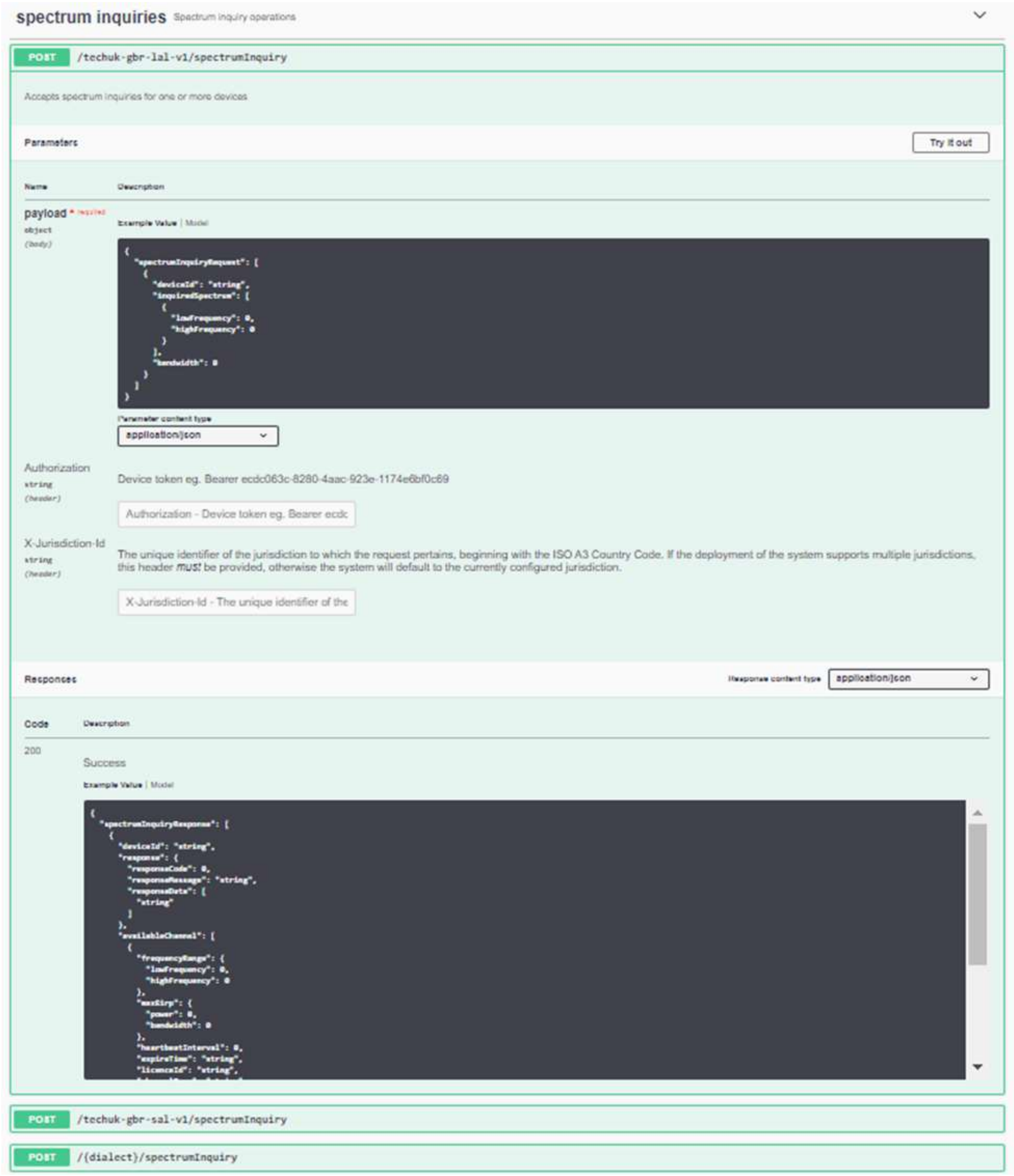


Figure 17: Registration Requests Swagger Dump for LAL dialect

3.5.2.7 Spectrum inquiry response

The following shows a Spectrum Inquiry (top) and Spectrum Inquiry Response (bottom) from the DSA Server when no measurement data has indicated the operating MNO. Such a capability was reported previously, but establishes a comparison baseline to the next step where 1810-1816.7 MHz is available.

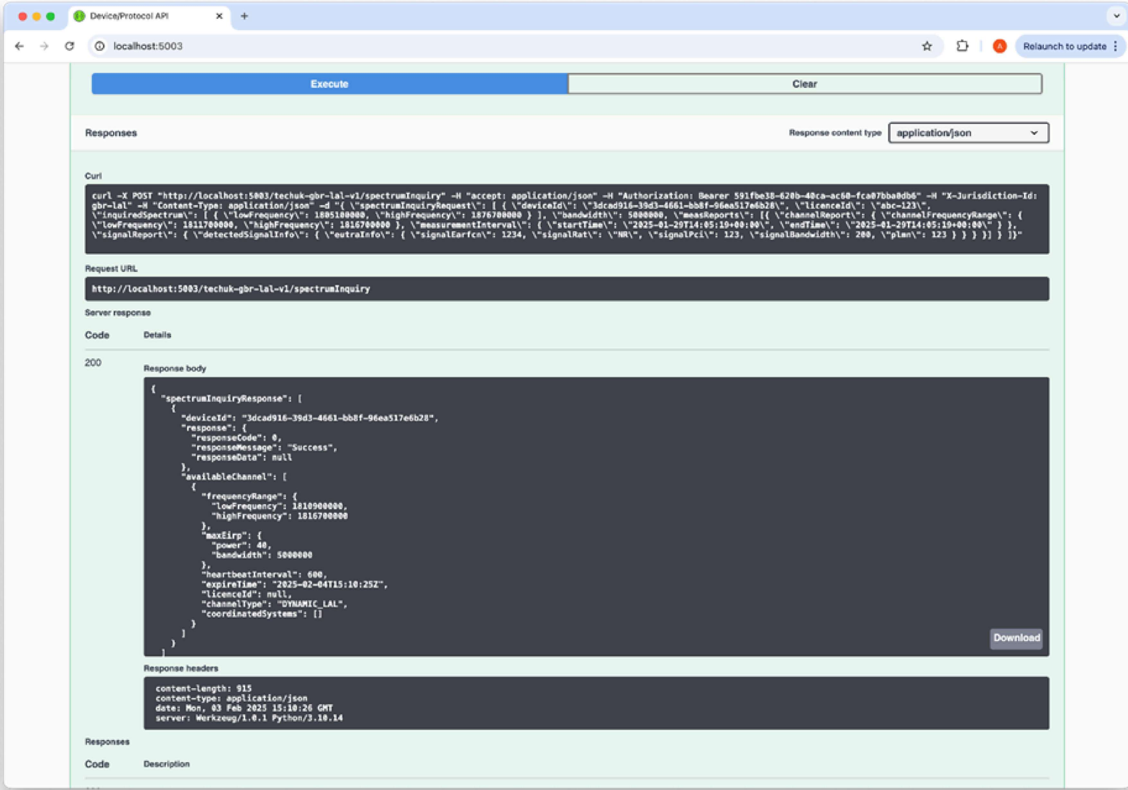


Figure 18: Spectrum Inquiry and Response Before Measurement Report indicates MNO operation in requested spectrum

3.5.2.8 Spectrum inquiry request with measurement report

The following shows a Spectrum Inquiry Request from a DSA Client that also includes a Measurement Report that indicates that the MNO has begun operation 1810-1816.7 MHz is available.

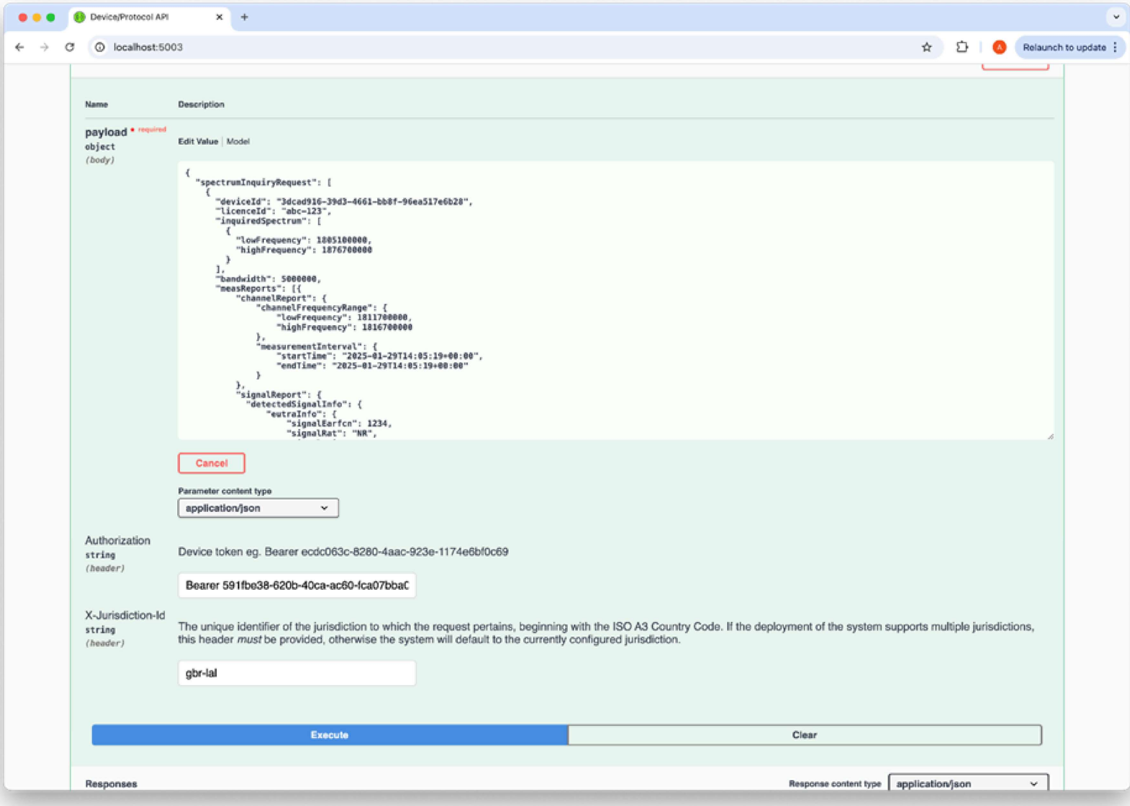


Figure 19: Spectrum Inquiry Request with Measurement Report

3.5.2.9 Spectrum inquiry response reflecting measurement change

The following shows a Spectrum Inquiry (top) and Spectrum Inquiry Response (bottom) from the DSA Server that reflects the change in availability to the preceding Measurement Report that indicates that inquired about spectrum is no longer available as the MNO has begun operation 1810-1816.7 MHz is available. Note that an inquiry in a different channel would yield a different response than the Null response shown.

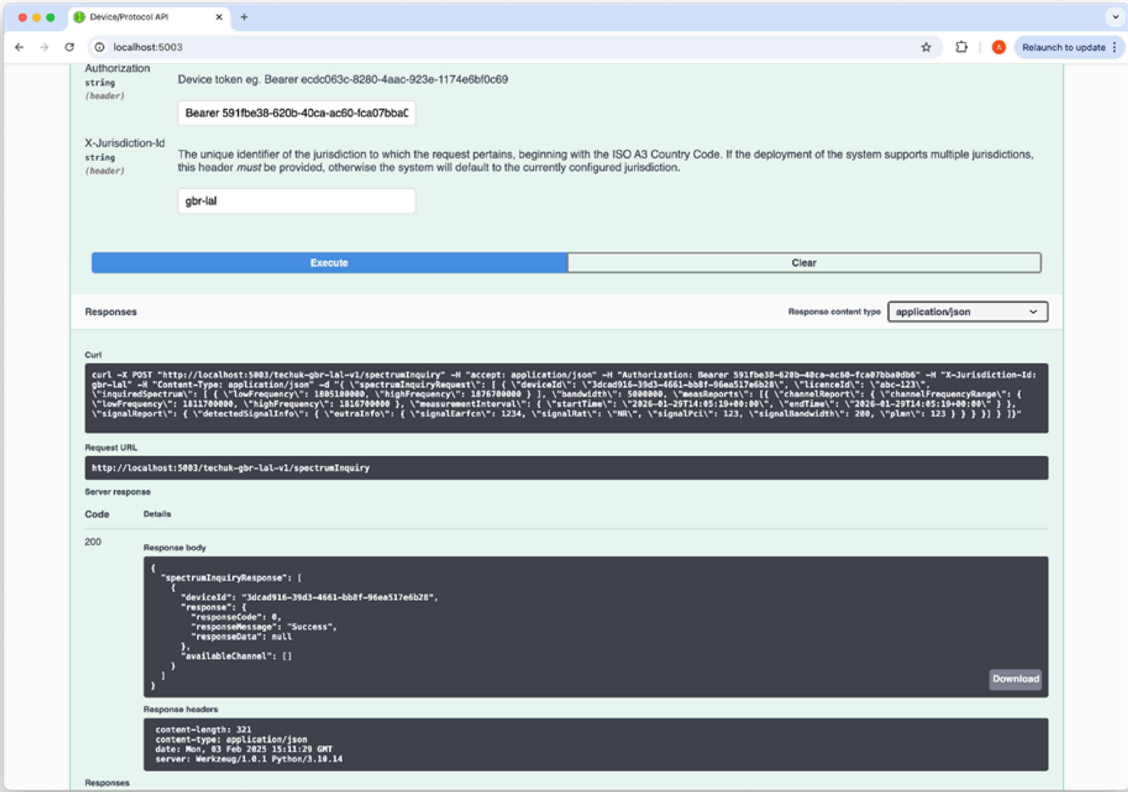


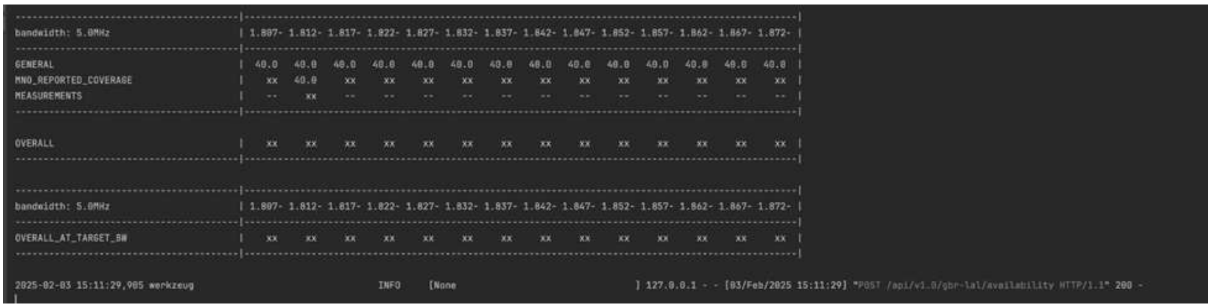
Figure 20: Spectrum Inquiry and Response after a Measurement Report that Indicates MNO Presence

3.5.2.10 Internal frequency assignment results

The following shows representations and visualisations of how the internal states of the SAS related to these messages:

bandwidth: 5.0MHz	1.807-	1.812-	1.817-	1.822-	1.827-	1.832-	1.837-	1.842-	1.847-	1.852-	1.857-	1.862-	1.867-	1.872-
GENERAL	40.0	40.0	40.0	40.0	40.0	40.0	40.0	40.0	40.0	40.0	40.0	40.0	40.0	40.0
MNO_REPORTED_COVERAGE	xx	40.0	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
MEASUREMENTS	--	--	--	--	--	--	--	--	--	--	--	--	--	--
OVERALL	xx	40.0	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx

bandwidth: 5.0MHz	1.807-	1.812-	1.817-	1.822-	1.827-	1.832-	1.837-	1.842-	1.847-	1.852-	1.857-	1.862-	1.867-	1.872-
OVERALL_AT_TARGET_BW	xx	40.0	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx



```
bandwidth: 5.0MHz            | 1.807- 1.812- 1.817- 1.822- 1.827- 1.832- 1.837- 1.842- 1.847- 1.852- 1.857- 1.862- 1.867- 1.872- |
GENERAL                      |  40.0   40.0   40.0   40.0   40.0   40.0   40.0   40.0   40.0   40.0   40.0   40.0   40.0   40.0  |
MNO_REPORTED_COVERAGE        |   xx   40.0     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx  |
MEASUREMENTS                 |   --     xx     --     --     --     --     --     --     --     --     --     --     --     --  |
OVERALL                      |   xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx  |

bandwidth: 5.0MHz            | 1.807- 1.812- 1.817- 1.822- 1.827- 1.832- 1.837- 1.842- 1.847- 1.852- 1.857- 1.862- 1.867- 1.872- |
OVERALL_AT_TARGET_BW         |   xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx     xx  |

2025-02-03 15:11:29,985 werkzeug      INFO     [None      ] 127.0.0.1 - - [03/Feb/2025 15:11:29] "POST /api/v1.0/gbr-lal/availability HTTP/1.1" 200 -
```

Figure 21: Channel Availability Table at Registered Location Before (top) and After (bottom) Measurement Report

3.6 Example measurement reports

3.6.1 Band 3 in Bath

The following is the measurement report as received by the DSA Server, having been sent by the DRAM (see Section 3), measured by the CellXica M3Q radio, during the practical demonstration to DSIT and Ofcom on 13th March, 2025:


```
"measReports": [
  {
    "channelReport": {
      "channelFrequencyRange": {
        "lowFrequency": 1822200000,
        "highFrequency": 1826200000
      },
      "channelRssi": -65,
      "measurementInterval": {
        "startTime": "2025-03-13T14:38:06.522",
        "endTime": "2025-03-13T14:38:06.522"
      }
    },
    "signalReport": {
      "detectedSignalInfo": {
        "eutraInfo": {
          "signalEarfcn": 1392,
          "signalRat": "LTE",
          "signalPci": 156,
          "signalBandwidth": 4,
          "plmn": 23420
        }
      },
      "signalRsrp": -96,
      "signalRsrq": -11
    }
  },
  {
    "channelReport": {
      "channelFrequencyRange": {
```

```
          "lowFrequency": 1844200000,
          "highFrequency": 1849200000
        },
        "channelRssi": -71,
        "measurementInterval": {
          "startTime": "2025-03-13T14:38:06.522",
          "endTime": "2025-03-13T14:38:06.522"
        }
      },
      "signalReport": {
        "detectedSignalInfo": {
          "eutraInfo": {
            "signalEarfcn": 1617,
            "signalRat": "LTE",
            "signalPci": 309,
            "signalBandwidth": 5,
            "plmn": 23430
          }
        },
        "signalRsrp": -93,
        "signalRsrq": -7
      }
    },
    {
      "channelReport": {
        "channelFrequencyRange": {
          "lowFrequency": 1864000000,
          "highFrequency": 1869000000
        },
        "channelRssi": -68,
        "measurementInterval": {
          "startTime": "2025-03-13T14:38:06.522",
          "endTime": "2025-03-13T14:38:06.522"
        }
      },
      "signalReport": {
        "detectedSignalInfo": {
          "eutraInfo": {
            "signalEarfcn": 1815,
            "signalRat": "LTE",
            "signalPci": 309,
            "signalBandwidth": 5,
            "plmn": 23430
          }
        },
        "signalRsrp": -96,
        "signalRsrq": -8
      }
    }
  ]
```


Figure 22: Band 3 Measurement report as received by the DSA Server from DRAM.

This shows the successful measurement of existing usage of Band 3 in Bath by Three (1822.2-1826.2 MHz) and by EE (1844.2-1849.2 MHz and 1864-1869 MHz) - both of which are only subsets of their licensed frequency ranges in this band. Note the decoding of the PLMN, PCI, EARFCN from the MIB and SIB1, and the measurements of RSRP, RSRQ, and RSSI.

3.6.2 Band n77 in Bath

The following is the measurement report as received by the DSA Server, having been sent by the DRAM (see Section 3), measured by the RANsemi PC802 radio, during the practical demonstration to DSIT and Ofcom on 13th March, 2025:


```
"measReports": [
 {
  "channelReport": {
   "channelFrequencyRange": {
    "lowFrequency": 4050000000,
    "highFrequency": 4100000000
   },
   "measurementInterval": {
    "startTime": "2025-03-13T15:02:36.382",
    "endTime": "2025-03-13T15:02:36.382"
   }
  },
  "signalReport": {
   "detectedSignalInfo": {
    "eutraInfo": {
     "signalEarfcn": 657500,
     "signalRat": "NR",
     "signalPci": 12345010,
     "signalBandwidth": 50000000,
     "plmn": 23488
    }
   },
   "detectedNrTddConfig": {
    "subcarrierSpacing": "kHz30",
    "nrTddUlDlPattern1": {
     "dlUlTransmissionPeriodicity": "ms5",
     "nrofDownlinkSlots": 7,
     "nrofDownlinkSymbols": 6,
     "nrofUplinkSlots": 2,
     "nrofUplinkSymbols": 4
    }
   }
  }
 }
]
```


Figure 23: Band n77 Measurement report as received by the DSA Server from DRAM.

This shows the successful measurement of existing usage of Band n77 in Bath by one of Telet's existing base-stations using a Shared Access Licence. Note the decoding of the uplink/downlink slot/symbol configuration, and subcarrier spacing, from the SIB1.

3.6.3 Sharing measurement data with Ofcom

The concept of a DSA Server, or similar, sharing real-time information on spectrum usage with Ofcom has previously been proven operationally. For TV White Space (TVWS), the White Space DataBase (WSDB) was required [30] to provide an API [31] called the "WSIP" to allow Ofcom staff to directly query the database for spectrum users in a given geographic radius and/or frequency range. This was used operationally by Ofcom's interference management team. While this interface had no need to provide measured data on PLMN, signal strength, TDD configuration etc., it is relatively straightforward for these fields to be incorporated into the WSIP protocol or similar.

Furthermore, the DSA Server developed for this Sandbox provides a 'Regulator Interface' (see Fig. 5), including a web interface. This provides search functionality, and displays results on a UK map, as shown in Fig. 21:

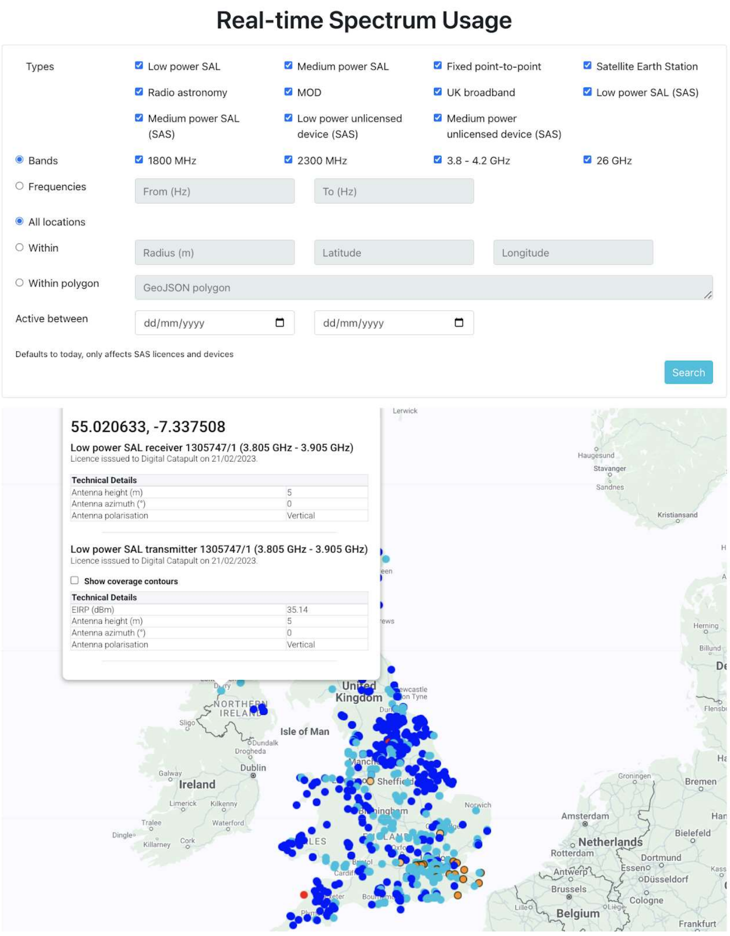


Figure 24: Screenshot of DSA Server Regulator Interface

3.7 Assumed MNO coverage

As discussed in detail in [Deliverable 1.2], Ofcom makes publicly available MNO-reported maps of incumbent Mobile Coverage [Coverage Checker]. This information is "consumer-grade" in intent: is grouped by technology (e.g., 3G, 4G, 5G) rather than by band / sub-band, it conforms to MNO claimed coverage with limited validation, and is only updated irregularly. This is insufficient for a DSA Server's needs, particularly because it does not describe which of their licensed frequency bands the MNO uses to provide that coverage, and therefore which of those bands are not being used in a given area. We anticipate that Ofcom will provide such data to a DSA Server in production, but for the purposes of this Sandbox we have simulated this for Band 3 through a series of assumptions.

For our purposes, quantitatively accurate band-by-band coverage maps are not needed to prove the concept of the sharing mechanism. As such, a crowd-sourced coverage tracker, which presents band-by-band maps, was used as a broad qualitative indication of coverage in Band 3. Where possible, the accuracy of these maps was verified experimentally (see Section 5). To approximate this qualitative reference, a 'filter' was applied to each MNO's Ofcom-published coverage data, according to the level of rural/urban classification in each UK Census Output Area (OA), with a different 'rurality' threshold chosen for each MNO; where the rurality was above that MNO's threshold, the Ofcom coverage was assumed, and where the rurality was below the threshold, no coverage was assumed (see figure 25 & 26):

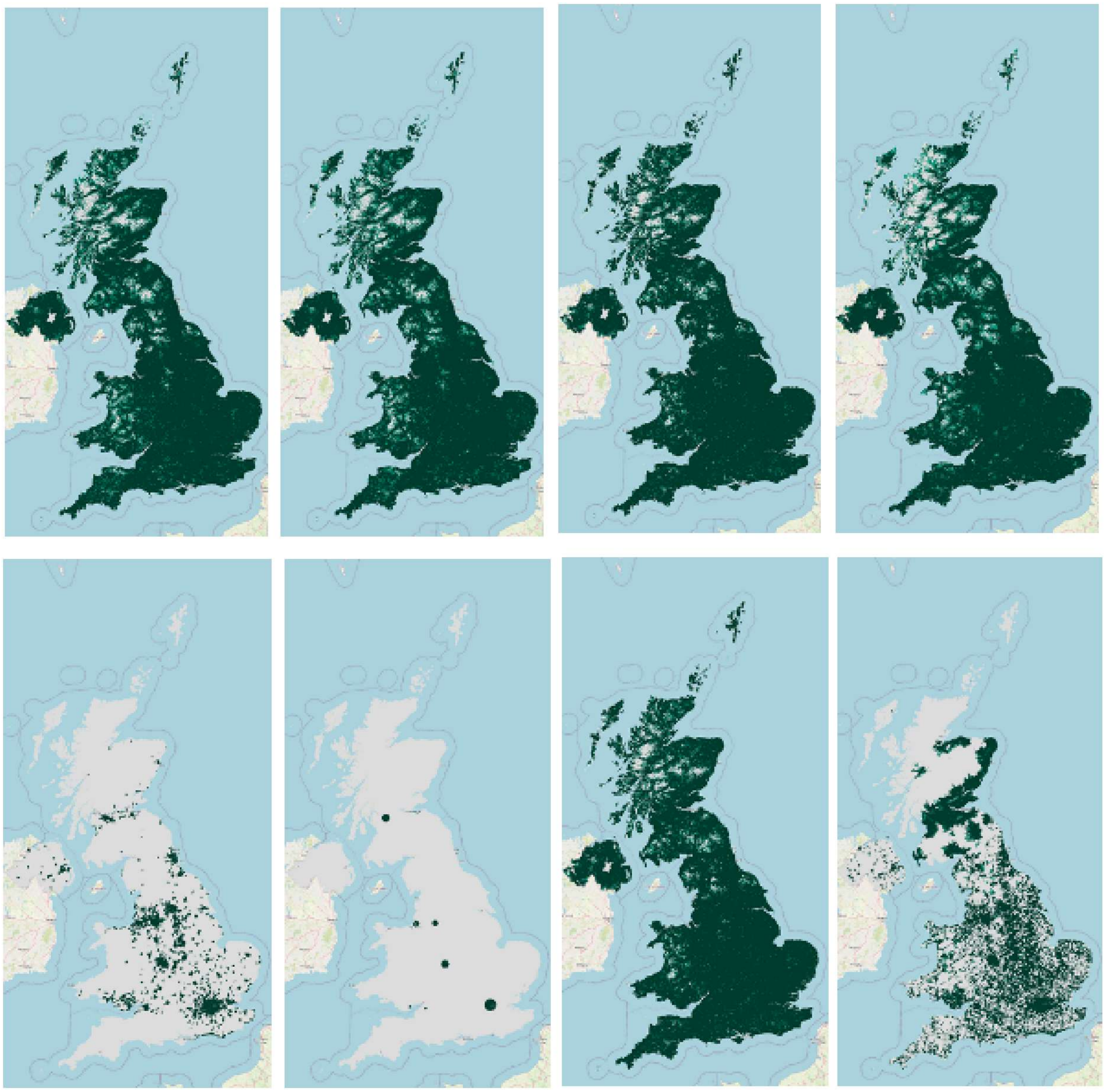


Figure 25: Imported Ofcom 4G coverage maps (top row) and assumed Band 3 coverage maps (bottom row) for each MNO (left-to-right: O2, Vodafone, EE, Three).

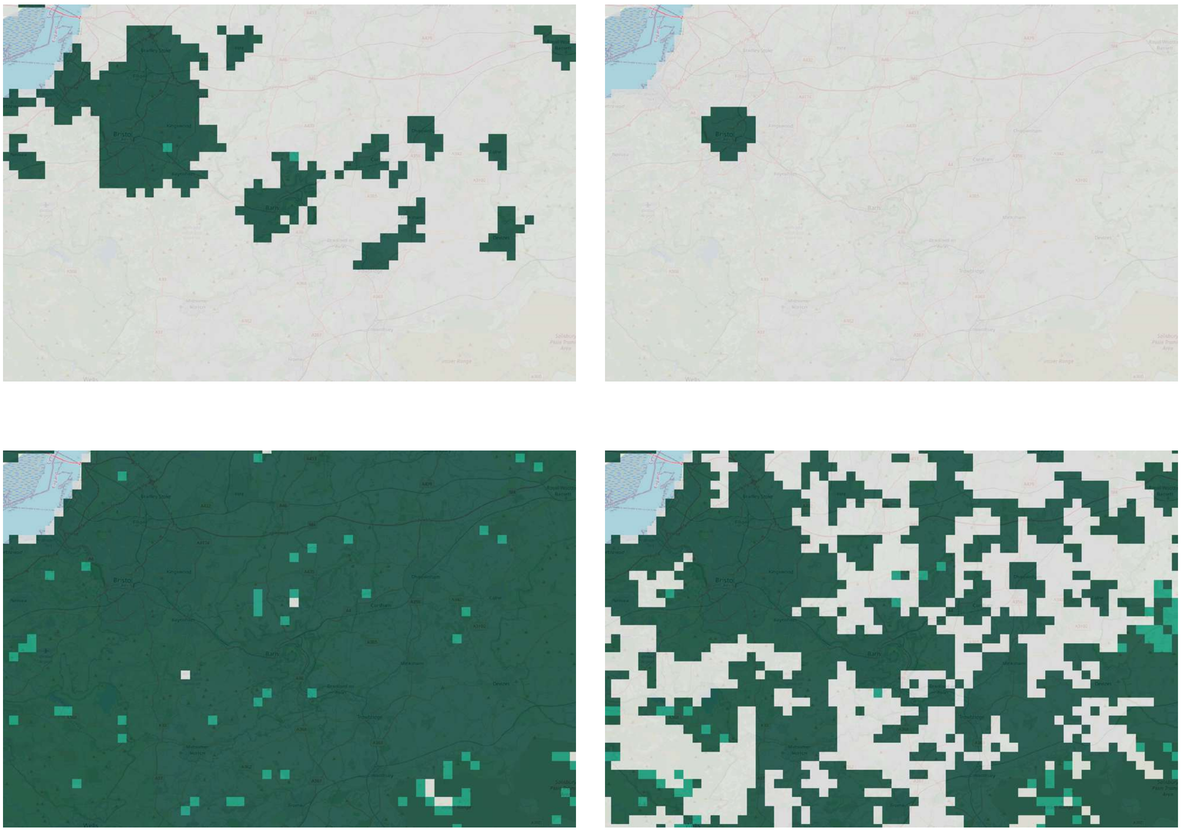


Figure 26: Assumed Band 3 coverage maps in the Bath area for each MNO (left-to-right, top-to-bottom: O2, Vodafone, EE, Three).

We emphasise that this method is purely for the purposes of the Sandbox, and a better solution is for Ofcom to provide more detailed and accurate maps to the DSA Server, potentially within a Non-Disclosure Agreement (NDA).

3.8 Security analysis

[FW-MS19] conducted a security analysis of the design of the DSA Server and DSA Server-Client Protocol [FW-MS17] by comparing to the practices adopted of the more mature CBRS security standards [28] and [29]. This resulted in the following recommended actions for commercialisation.

1. A process for designating and managing root and intermediate CAs needs to be defined.
2. Acceptable certificate lifetimes need to be defined
3. The process by which secret keys are employed needs to be defined and assessed.
4. While the DSIT specification mandates at least use of TLS 1.2, the CBRS standards recommend the use of 1.3 when the standard is finalised. As TLS 1.3 is now specified, the DSIT protocol design should reassess if TLS 1.3 is appropriate.
5. The DSIT ciphersuites are a subset of the CBRS ciphersuites. Any expansion on the DSIT ciphersuites can be considered in implementation.

6. Section7 of [29] addresses a topic (securing key material with the CBSD) that is beyond the scope of this document, but should be assessed by the RAN partner.
7. Section 9 of [29] documents critical processes to maintain the CBRS trust boundary. These are implementation specific processes and thus beyond the scope of this document.
8. However, assessments of the spectrum sharing ecosystem enabled by the DSIT project should examine the implementation approach for each of the listed items when applicable (e.g., possibly not for blacklist management).

Additionally, as opposed to CBRS which reports measurements from ESC to SAS, in the proposed sharing regime, measurements are reported over the DSA Server-Client protocol, thus making the communications of those messages in scope.

Additionally, the extent to which data from measurements of incumbent (MNO) operations should be obfuscated at various stages should be determined by Ofcom. For example: what can be reported by DSA clients in Measurement Reports, what is reported to Ofcom by the DSA Server, and what (if anything) is made available to the public by the DSA Server. [29] leaves this process to SAS and ESC specification (and ultimately DoD review).

4 gNB Integration

4.1 Available signalling and measurements

The data that we require for this DSA model is potentially contained in all radios although it is not easily interrogated as different radios use different methods to deal with the data; the DRAM middleware function has been specifically developed for this purpose. We are able to look at the gNB and or UE data at three different levels as below:

4.2 Level 1 – Signal Level (RSRP)

The first stage in the process uses RSRP (Reference Signal Received Power) to determine the presence and the strength of signals.

- Currently used in US CBRS in conjunction with data held by SASs
- Demonstrated with simple TinySA Spectrum Analyser (and in the lab with the Blinq Demo operating in the Upper 5 GHz Band)
- RSRP is waveform agnostic
- Able to determine presence and level of signals, but requires access to additional data (such as the B3 Channelisation Overlay) to identify source of signal

4.3 Level 2 – Collection and analysis of MIB and SIBs

The Master Information Block (MIB) and System Information Blocks (SIBs) in 5G NR (New Radio) facilitate initial synchronization and contribute to building a spectrum usage model. The sandbox exercise has used the data extracted at this level which has proven to be satisfactory and fit for our purposes.

- Used for Mobile<>Mobile spectrum pairing scenarios
- Demonstrated with Cellica M3Q and RANsemi PC802 demos (B3/n77)
- Both LAL and SAL applications (+ Permissive in n77)
- Detectable at low signal levels - below interference threshold
- **PBCH (Physical Broadcast Channel)**: Carries the Master Information Block (MIB), which provides essential information needed to decode other system information.
    - Can be decoded at very low signal levels - >20dB below interference threshold
- **SIB (System Information Block)**: These are broadcast by the gNB to all UEs within its cell.

- They contain essential information for cell access, including:
  - Cell ID – uniquely identifies site (and location)
  - PLMN (Public Land Mobile Network) ID – Identifies owner
  - Frequency band information
  - Bandwidth information
  - Random access parameters
  - Timing information – including frame structure

MIB and SIB Information Summary

Information Element (IE)	Location	Content
Master Information Block (MIB)	PBCH	- System frame number (SFN)
		- Subcarrier spacing (SCS) configuration
		- Cell barring information
System Information Block 1 (SIB1)	PDSCH	- Cell identity, PLMN identity
		- Tracking area code, cell selection/reselection information
		- QMC (Quasi co-location) information
System Information Block 2 (SIB2)	PDSCH	- Radio resource configuration: common and dedicated (CORESET, Search spaces for RACH, PUSCH, PUCCH, PRACH)
		- Scheduling information
System Information Block 3 (SIB3)	PDSCH	- Intra-frequency and inter-frequency neighboring cell information
Other SIBs (4-24)	PDSCH	- UE specific configurations (e.g., power control, mobility, etc.), paging information, multicast/broadcast settings, etc.

SIB 1

Field Name	Description	Example
Cell Identity	Unique identifier for the cell	1234567
PLMN Identity	Public Land Mobile Network identifier (MCC+MNC)	MCC: 234, MNC: 88 (Telet)
TAC	Tracking Area Code	0x0042
Cell Barred	Indicates if the cell is barred for access	TRUE/FALSE
Connection Establishment Failure Control	Parameters for handling connection failures	Max RLC Retransmissions: 4
SI Scheduling Information	Information about the scheduling of other SIBs	SIB2 periodicity: 320ms
Serving Cell Information	Information about the serving cell	Frequency band: n77
Common Parameters	Common parameters for all	Default Preamble Format: 0

Field Name	Description	Example
	UEs in the cell	
Additional Assistance Data	Optional assistance data for UEs	-

Note: This table provides a general overview of the data contained in a 5G SIB 1.

SIB 2

Spectrum Modeling with MIB/SIB Information

We have used the information extracted from the MIB and SIBs to construct a model of the local spectrum environment:

1. **Cell Identification and Synchronization:** The MIB on the PBCH provides crucial information for initial cell acquisition, including the SFN and the cell's subcarrier spacing. This allows the receiver to synchronize with the 5G NR cell.
2. **Cell Selection/Reselection:** SIB1 contains parameters for cell selection and reselection.expand_more This helps the receiver determine the best cell to connect to based on signal strength, quality, and load conditions.
3. **Resource Allocation Understanding:** SIB2 provides details on how the cell's resources are organized, including control and data channels (CORESET, search spaces, etc.). This knowledge enables the receiver to efficiently decode transmitted data and control signals.
4. **Neighbor Cell Discovery:** SIB3 contains information about neighboring cells on the same and different frequencies.expand_more The receiver can use this to anticipate potential handovers, optimize mobility, and potentially aggregate signals from multiple cells (carrier aggregation).
5. **UE Configuration Optimization:** Other SIBs (4 and above) contain information that the UE uses to configure itself optimally for the specific network deployment. This includes parameters like power control settings, mobility parameters, and other UE-specific configurations.

Building the Spectrum Model

By continuously monitoring and decoding the MIB and SIBs, the receiver can build a dynamic model of the local spectrum:

- **Frequency Occupancy:** The receiver identifies which frequency resources are occupied by 5G NR cells, neighboring cells, and potentially other technologies.
- **Cell Parameters:** The receiver maintains a database of parameters for each detected cell (e.g., cell ID, signal strength, channel configurations).
- **Resource Availability:** The receiver tracks the availability of radio resources within each cell to estimate potential data rates and connection quality.exclamation

Benefits of Spectrum Modeling

This spectrum model enables the receiver to:

- **Optimize Performance:** Choose the best cell and radio resources for optimal connection quality and data rates.
- **Efficient Resource Utilization:** Avoid interfering with other users and technologies by intelligently selecting channels.
- **Seamless Mobility:** Anticipate handovers and make informed decisions about when and how to switch cells.

4.4 Level 3 – Collection and analysis of RRC (Radio Resource Control) Signalling between gNB and UEs

The further extraction of radio parameters from the signaling channel between the gNB (5G base station) and UE (user equipment) can provide essential data for spectrum management. Going forward the proposed next phase of dynamic spectrum management utilises the parameters below as we move from TRL6 to TRL8/9.

Parameter	Description	Spectrum Management Use
RSRP (Reference Signal Received Power)	Power of the reference signals received by the UE from the gNB.	Coverage Analysis: Identify areas of weak signal strength. Interference Detection: High RSRP from multiple cells indicates potential interference. Dynamic Spectrum Sharing (DSS): Used to make real-time decisions about spectrum allocation between 4G and 5G.
RSRQ (Reference Signal Received Quality)	Ratio of RSRP to the total received power.	Interference Assessment: Low RSRQ signifies high interference. Cell Selection/Handover: Guide UE to select the cell with the best signal quality, maximizing spectrum use. Network Optimization: Find areas where pilot pollution could be an issue.
SINR (Signal-to-Interference-plus-Noise Ratio)	Ratio of the desired signal power to the power of interference and noise.	Spectrum Efficiency: High SINR implies efficient spectrum use; low SINR suggests inefficient use due to interference. Capacity Planning: Monitor SINR to estimate network capacity and identify potential bottlenecks. Interference mitigation: locate and mitigate sources of interference.
CQI (Channel Quality Indicator)	UE's estimate of the channel quality, used for scheduling.	Adaptive Modulation and Coding (AMC): Ensures the optimal modulation and coding scheme is used, maximizing data rate within the allocated spectrum. Resource Allocation: Helps gNB allocate resources efficiently based on UE channel conditions.
PMI (Precoding Matrix Indicator)	UE's preferred precoding matrix for MIMO.	MIMO Optimization: Utilizes MIMO effectively, increasing spectrum efficiency and capacity. Spatial Multiplexing: Improve the capability of multiple data streams to transmit simultaneously.

RI (Rank Indicator)	UE's estimate of the number of useful transmission layers.	MIMO Layer Management: Optimizes the number of layers used in MIMO transmissions, maximizing spectrum usage. Adaptive Beamforming: Helps maximize the power transmitted towards a specific user.
TA (Timing Advance)	Adjustment applied by the UE to synchronize its uplink transmission with the gNB.	Uplink Synchronization: Essential for efficient uplink spectrum use. Distance Estimation: Can provide rough estimates of UE distance from the gNB.
UE Power Headroom	Difference between maximum UE transmission power and actual transmission power.	Uplink Power Control: Prevents UE from using excessive power, reducing interference to neighboring cells. Coverage Prediction: Used to create coverage maps.
BLER (Block Error Rate)	Ratio of incorrectly received data blocks to the total number of blocks.	Link Quality Assessment: Indicates the reliability of the communication link. Retransmission Management: Triggers retransmissions when BLER is high, optimizing resource utilization.
Handover Parameters (e.g., A3 Offset)	Parameters that affect when a UE hands over to a new cell.	Mobility Management: Optimizes handovers to minimize service interruptions and maximize spectrum efficiency. Load Balancing: Directs UEs to less congested cells.
Cell Load Indicators (gNB)	Measurement of the utilization of cell resources by the gNB.	Dynamic spectrum allocation: In a heavily loaded cell, less spectrum may be allocated to users. Traffic Management: Facilitates dynamic spectrum sharing and traffic management.

5 Practical Implementation

5.1 Scope of proof of concept demonstrations

In the context of the overall DSA server architecture, Telet undertook the development of a practical implementation of an operational mobile telephony network working with the DSA server to dynamically gain access to the spectrum to offer mobile telephone services. The two main sub-systems developed were:

1. Customisations of existing eNB and gNB radios (the mobile base stations)
2. Development of a middleware application to interface between the radios and the DSA server.

The relationship between these sub-systems and the DSA server is shown below:

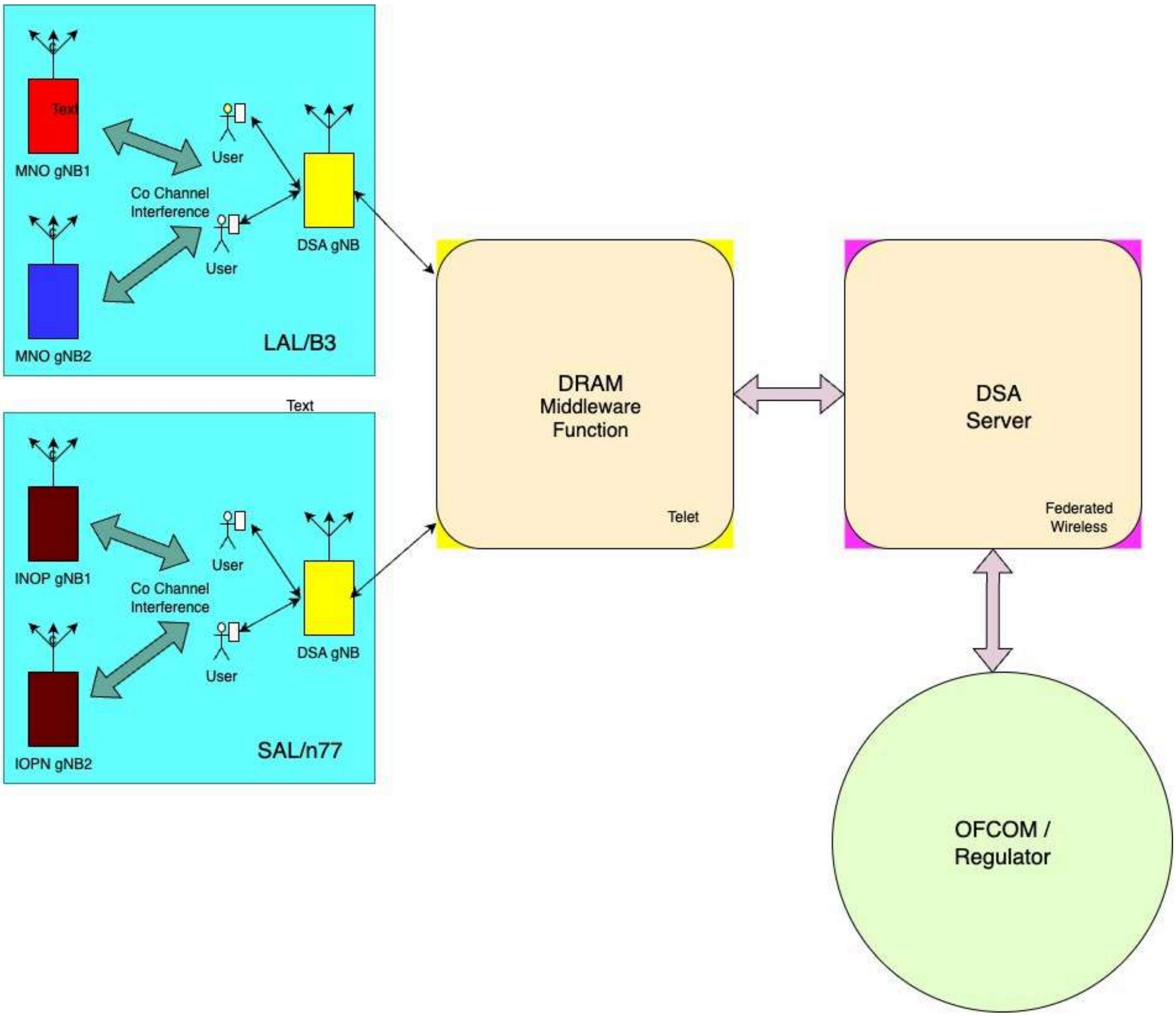


Figure 27: Relationship between the radios, DRAM and DSA server

5.2 Radio Customisations

Telet determined that the two main currently deployed radio architectures should be evaluated as part of the proof of concept. These architectures are based on respectively:

1. Radios using customised silicon, based on Field Programmable Gate Arrays (FPGAs) such the Ransemi PC802.
2. The more modern Software Defined Radio (SDR) architecture radios such as the CellXica M3Q

The primary reason for using examples of each of these architectures was to demonstrate the advantages and disadvantages of each architecture in terms of delivery of the required scanning and sensing functions required.

Telet engaged with these two UK based radio manufacturing companies to undertake the required customisations to allow the radios to conduct both full band spectrum scanning and also undertake signal sensing on the device operating frequency. This sensing operation is required to detect the presence of co-channel interference (CCI) when another network operator comes on-line on the same frequency as the sensing radio is operating on. The required customisations included:

1. Hardware modification to the RF filters to allow the full band to be scanned..
2. Updates to the internal radio software to provide the required scanning and sensing operations
3. Development of an external software interface to the radios to allow them to be remotely controlled via an application programming interface (API). In practice the two architectures used two different APIs. This highlights the role of the connecting middleware is being able to translate multiple API dialects into the common format required to interface to the DSA server.

During the implementation of these changes it became apparent that the size of the customisation task was somewhat larger than had been anticipated when the project was proposed, with the result that the hardware and software changes were not delivered until much later than was originally planned. This had a knock on effect on the project schedule with the result that it was not possible to operate the end to end system for as long as had been originally planned.

5.3 Detailed description of the radio equipment used

5.3.1 CellXica Band 3 M3Q

The M3Q in its commercial form is a 3GPP release 9 compliant, 2×2 MIMO LTE base station designed to support 32 concurrent connected-state users and user-plane data rates up to 60Mbps for applications such as in-building or rural coverage. The M3Q also supports spectrum monitoring in support of Self Organising Networks (SON).

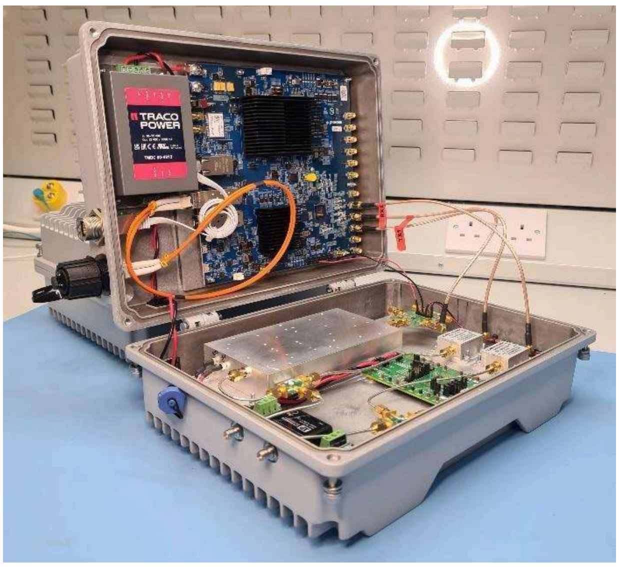
The firmware for the units that we will be using will be modified in order to allow the easy extraction of radio data parameters in near real time. The key data that can be extracted is a combination of the data contained in the MIB and SIB that are broadcast by 4G cells. The

SDR architecture also allows other functionality, including the ability to monitor (or ‘look through’) on the transmit channel when in use. This will allow any potential interference to be immediately detected and identified, so that a spectrum ‘release’ procedure can be initiated

EXSITE-M3Q GiLTE Basestation

5.3.2 RANSemi PC802 Band 3

This is a modified version of the RANsemi Reference Design utilising the Picocom PC-802 chipset. The firmware modifications will allow rapid scanning and identification of any signals within the band, with all radio data being exported through a custom API. When in traffic, the radio will be capable of allocating ‘look through’ time slots which will be used to identify any co-channel use of the allocated spectrum.



The High-Level Specification of the PC802 based units is as below:

Table 8: PC802 high level equipment specification

Item	Supplied by
RF port 1	Transmit / receive
RF port 2	Receive-only, network monitor port
Tx output power	≤ 20dBm
Tx operating frequency	1805 - 1880 MHz
Tx IBW	≤ 20MHz
Rx operating frequency	1710 – 1785 MHz
Rx noise figure	≤ 4dB
Antenna	2 x Omni, 8dBi, vertically polarised
DC power	48V DC, ≤ 60W
Data interface	10GBASE-SR, OM3 multi-mode 850nm
Dimensions	321 x 213 x 135 mm
Weight	≤ 10kg
Ingress protection	IP67
Mounting method	Pole-mount kit

5.3.3 RANSemi PC802 n77

For the purpose of testing and measurement collection in band n77, the project sourced additional n77 band versions of the PC-802 reference platform. Whilst both B3 and n77 versions use the RANsemi designed PC802 SoC for all of the radio stack and signal processing, the B3 version operated both 4G and 5G FDD waveforms within the 1800 MHz band, whilst the n77 version operated solely a TDD waveform in the 3.8-4.2 GHz range.

5.3.3.1 Identification of Timing and Framing configuration

The n77 unit is capable of both detecting and operating with different framing structure; this allows the testing of interference scenarios between gNBs operating with different UL/DL split configurations.

5.3.3.2 Power Limitations

A further limitation of the n77 devices developed was that as the unit was not fitted with a production power amplifier the output power was limited to around 10 dBm. This was not an issue for the proof of concept as the purpose of the device was to be able to scan, sense and then change operating parameters based on directions from the DSA server. This requirement was demonstrable with the limited output RF power levels that the experiment n77 PC802 was able to produce.

5.3.4 4G/5G Core Network

To demonstrate full operational capability the test radios were connected to local 4G/5G cores, implemented with Open5GS. This was used in conjunction with Telete SIMs, both in physical and eSIM formats in order to allow full operational interaction with User Equipments.

5.3.5 Visualising Live Spectrum Use - TinySA Spectrum Analyser

To demonstrate live spectrum occupancy in real time a TinySA Spectrum Analyser was configured to scan the complete downlink frequency range 1805 - 1880 MHz.

The TinySA was further connected to a remote management platform that enabled outputs to be remotely managed and data collected.

5.4 Level 3 Data Collection

Whilst the Level 2 data collection provides a full range of data against which assessment of interference between co-channel gNBs can be carried out, the algorithm does not take into account any effects of interference experienced at the User Equipment end of communications links.

In order to get an accurate picture of exactly what radio conditions exist at the user end of each communications link, it is possible to collect radio measurement data from the user equipment. Within normal operation of the 4G/5G system, UEs and gNBs constantly measure the conditions on both uplink and downlink radio paths. This data is then used by the gNB to dynamically adjust the configuration of the radio link in order to operate at optimal efficiency.

Whilst in this stage of development, we were not able to extract this data directly from within the UE<>gNB signalling links, it was possible to extract captures of this data from UEs for analysis later. The tool used to do this was a specialised engineering application, **Network Signal Guru.**

Network Signal Guru

Network Signal Guru (NSG) is a comprehensive mobile app designed for in-depth analysis and troubleshooting of cellular networks. It caters to network engineers, field technicians, and radio frequency (RF) optimization professionals, providing a wealth of information and features to assess and enhance network performance.

Key Capabilities and Functionality:

- **Multi-Technology Support:**
    - NSG supports a wide range of cellular technologies, including GSM, GPRS, EDGE, UMTS, HSDPA, HSUPA, CDMA2000, EVDO, LTE (FDD & TDD), 5G NR (SA & NSA), and mmWave.
    - This allows users to analyze various network types and generations, making it a versatile tool for different scenarios.
- **Real-Time Monitoring:**
    - NSG provides real-time monitoring of various network parameters, including signal strength, quality, data rates, latency, and more.
    - This enables users to quickly identify and diagnose issues in the field, leading to faster troubleshooting and optimization.
- **Protocol Decoding and Analysis:**
    - NSG decodes various protocol layers, including 3GPP, Layer 2, Layer 3, and SIP.
    - This allows for deep analysis of signaling and data traffic, providing insights into call setup, handover procedures, data transfer, and potential issues.
- **Data Collection and Logging:**
    - NSG records all the measured data, allowing users to analyze logs offline and track changes in network performance over time.
    - The logged data can be exported in various formats, including PCAP, CSV, and KML, for further analysis and visualization.
- **Voice and Data Testing:**
    - NSG supports voice and data tests to assess the quality of service (QoS) from the end user's perspective.
    - This includes call quality analysis, data throughput tests, and latency measurements.
- **Map Integration:**
    - NSG integrates with maps to display cell tower locations, signal coverage, and measurement routes.
    - This visual representation helps in identifying coverage gaps, overlapping cells, and potential interference issues.
- **Device and Chipset Support:**
    - NSG supports a wide range of Android devices with various chipsets, including Qualcomm, MediaTek, Samsung Exynos, and Huawei Kirin.
    - It typically requires root access for Qualcomm and MediaTek devices and custom ROM for Huawei Kirin.

Additional Features:

- **Customization:** Users can customize the app's interface and settings to suit their preferences.
- **Scripting:** NSG supports scripting for automating tasks and creating custom tests.
- **Remote Access:** Users can remotely control and monitor NSG from a computer using a web interface.
- **Cloud Synchronization:** NSG can synchronize data with cloud storage for easy access

and sharing.

Applications:

NSG is used in various scenarios, including:

- **Network Optimization:** Identifying and resolving coverage gaps, interference issues, and capacity bottlenecks.
- **Troubleshooting:** Diagnosing and resolving problems related to call drops, poor data speeds, and network congestion.
- **Benchmarking:** Comparing the performance of different networks or devices.
- **Research and Development:** Collecting data for research and development of new wireless technologies.

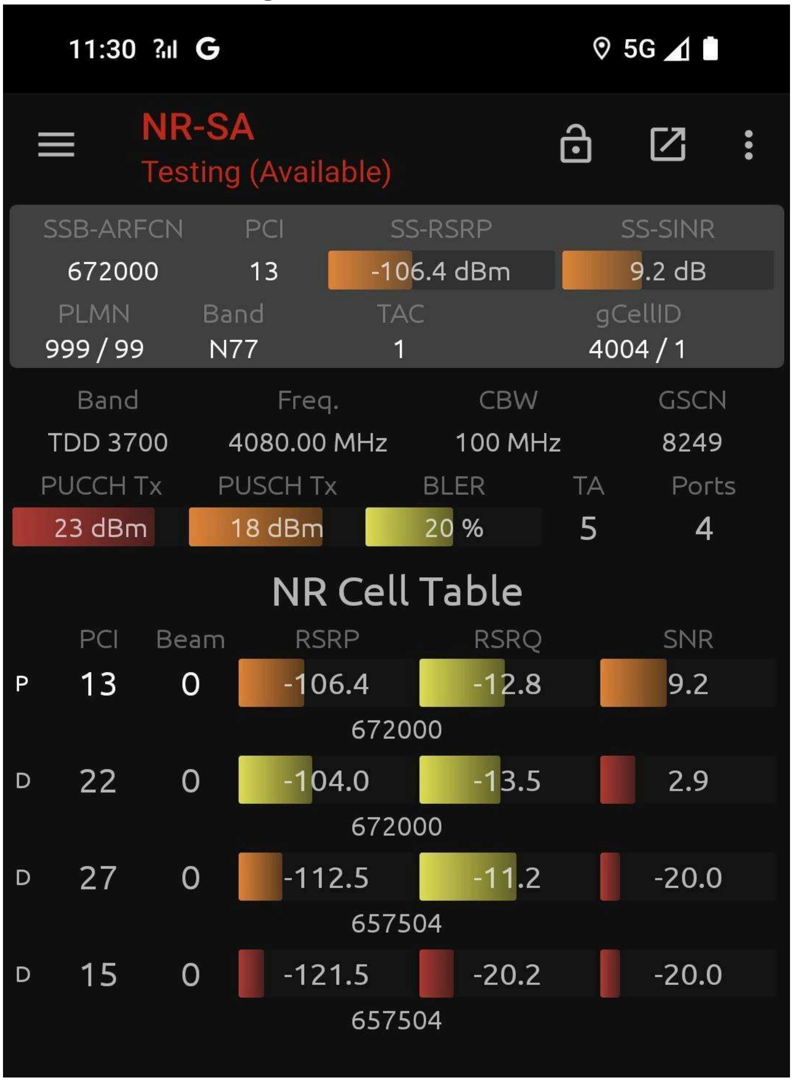


Figure 28: NSG screen showing detected cells.

This screenshot shows one of the many views of live data being collected on a test UE running Network Signal Guru in central Bath. This device was connected to the Bath 5G SA network operating a 100 MHz channel in the n77 band on 4080.00 MHz (NRARFCN 672000). At the time the device was recording co-channel signals from four different gNBs (on PCIs 13, 22, 27 and 15). For each of these the RSRP (Reference Signal Received

Power), RSRQ (Reference Signal Received Quality), and SINR (Signal-to-Interference-plus-Noise Ratio) are shown.

Figure 29: NSG data collection in Bath city centre

These photos show members of the QMUL WP2 Team using NSG in Central Bath to collect Real World RF measurements against which to validate their propagation and interference models.

5.5 The Middleware - Dynamic Radio Access Manager

As indicated above there is a requirement for a dedicated interface between the customised radios and the DSA server. This middleware has been named the **Dynamic Radio Access Management (DRAM)**. The DRAM sits between the 4G / 5G radios (eNBs / gNBs) and theDSA server.

The DRAM provides a number of functions:

1. Control of the radio (scanning, sensing and change of parameters)
2. Translation of the radio data into a format that the can be used to interact with the DSA server
3. Undertake the logging of all key actions in the middleware database. This is required to support the demonstration of functionality in the POC. In an operational environment it is almost a key requirement in support of any interference investigation as it provides an audit trail of the device's operational parameters such as operating frequency, operating bandwidth, and output power. Additional audit trail data on operating modes is also available through the 4G/5G core server.
4. Coordinating requests to the DSA server to obtain spectrum leases, The full internal middleware logic that handles the DSA server protocol has been documented using Miro to define the control flow. A full version of the internal design is available online at: https://miro.com/app/board/uXjVLFq-0dQ=/ . The following image is included only to illustrate this activity. As with many of these software tools, it is necessary to access them directly to fully interact with them.

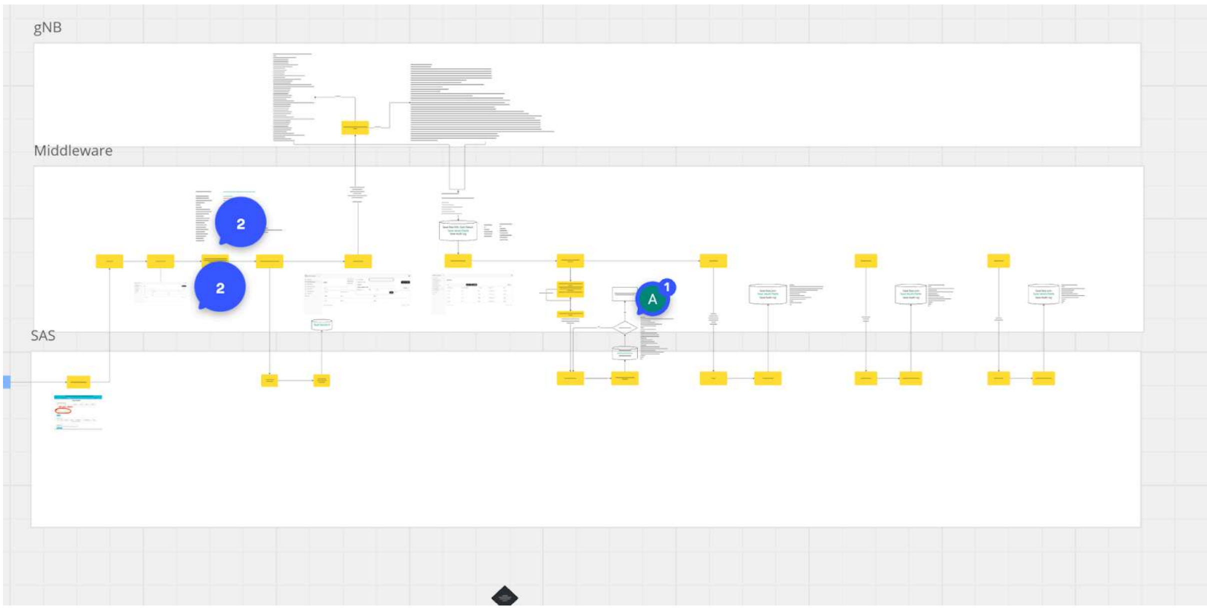


Figure 30: MIRO diagram showing DRAM internal control flow

We also show the logic flow for heartbeat processing below:

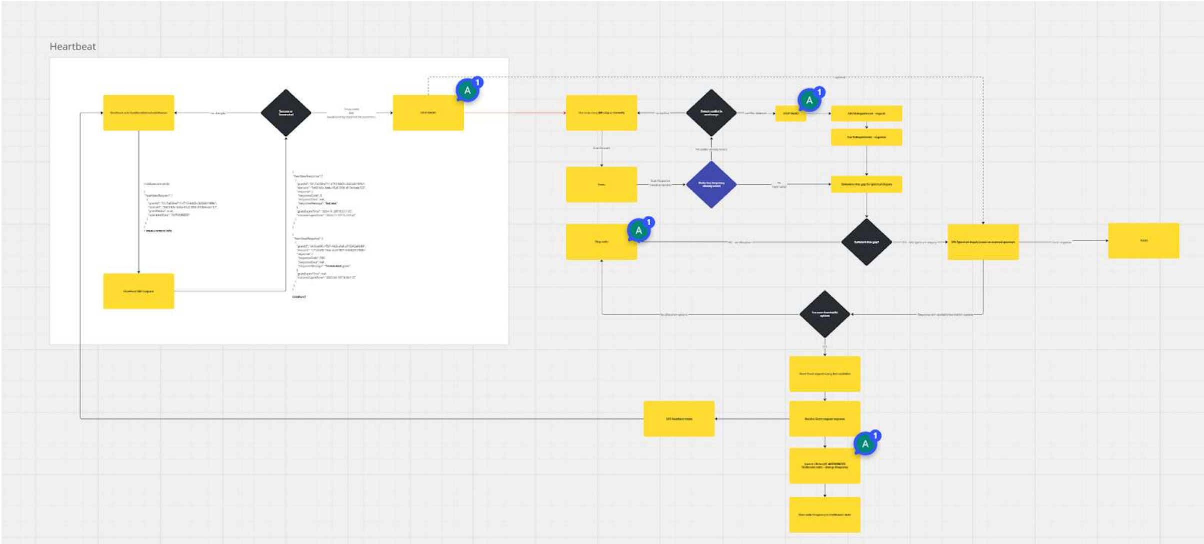


Figure 31: Miro diagram showing heartbeat control logic

For illustration purposes we have abstracted this detailed internal control flow into the following high level view (Note that in earlier version of the requirement that the DSA server was designated the Spectrum Access Server and hence the use of the SAS nomenclature in the figure :

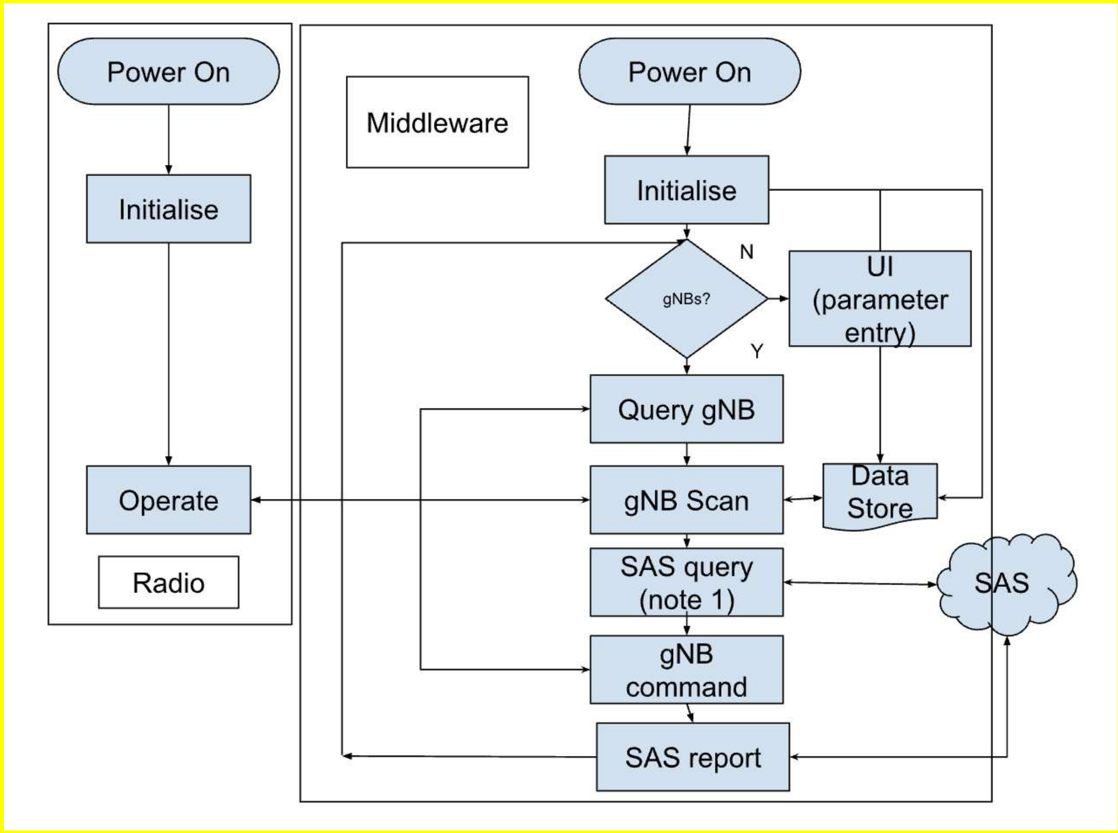


Figure 32: High level flow chat of the DRAM control flow

A full specification for DRAM has been documented elsewhere and this has been submitted as a separate project report (DSA server middleware requirements) .

5.5.1 The DRAM operating mode

For the project, a single instance of the middleware runs and provides a single point of control for the attached radio. In considering the wider implications of how the DRAM might be deployed we have observed that the DRAM can exist in a number of forms. For example it could be:

a. hosted on the radio itself. In this case the manufacturer would integrate the functionality directly into the radio to allow it to operate in a stand along mode.
b. Hosted on dedicated servers or in the cloud controlling a number of deployed radios on behalf of a single operator.
c. Hosted on dedicated servers or in the cloud but offering a DRAM service to multiple operators who wish to connect to the DSA server without the overhead of operating a dedicated DRAM server.

5.5.2 The DRAM database

In addition to the logging functionality outlined above, the DRAM database serves the following additional purposes:

1. Repository for static data e.g. Band data setting out characteristics of each band
2. Repository of radio specific data. It is assumed that the DRAM will need to control a number of connected radios (as in this case where three radios were all controlled from the same DRAM). Each radio requires specific data relating to key data such as the location, type of equipment, etc.
3. Repository of data extracted from and sent to the radios.
4. Repository of DSA server requests and responses
5. Repository of DSA authentication data. This is highlighted earlier as authentication and access control is a key security requirement for DRAM operation to avoid rogue operators subverting the integrity of the overall dynamic spectrum allocation process.

5.5.3 The DRAM radio control

The DRAM, as the main interface to the radios, needs to manage a number of activities:

1. Initiate a full spectrum scan operation. We note that conducting a full scan can take some time and is also radio dependent. At present we control this in the DRAM via a parameter. The scan is initiated as an asynchronous operation, with the results being available at some later point. In real operation there is a requirement for the scan rate to be set to meet any regulatory requirements.
2. Extraction of the results of the spectrum scan results. As noted above the scan initiation is asynchronous and hence there is a need to respond to either a call back, or hold off for a defined period of time before querying the results of the scan operation.
3. Translation of the radio scan results into a common DSA server format. As already noted, it must be anticipated that each radio manufacturer will define their own radio API, and also the format of any supplied data. In dealing with the two radio architectures chosen for the POC this practical issue was encountered and a separate “translation” was required for the CellXica and PC802 data formats (this is illustrated later when the POC results are documented, and can also be seen in the data archive.
4. Initiate a co-channel interference (CCI) measurement from the radio. Again, as with the spectrum scan operation, sensing of CCI takes finite time (and is dependent on the radio architecture). Whilst it at first glance appears to be necessary to conduct CCI measurements frequently we have observed the local mobile RF environment does not change at a granularity of seconds or minutes. In practical terms it takes significant time to plan, deploy and test 4G and 5G radio infrastructure. Again for the purposes of the POC we have run the CCI operation at a relatively high rate in order to “demonstrate” behaviour, a less frequent rate is likely to be required in practice. The exact rate of CCI measurements if something that we believe needs to considered and specified from a policy perspective

5. Initiate of command to change the operating parameters for the radios themselves. There are two cases that we need to deal with here that reflect the differences between the FDD and TDD mobile bands.
    a. Common to both FDD and TDD and the DSA server,when it issues a spectrum lease, can require that any of the three parameters of frequency, bandwidth and operating power need to be changed.
    b. For the TDD bands there is an additional requirement to alter the parameters that control:
        i. The device timing source. If interference is to be avoided then all TDD devices in close proximity need to operate using the same time synchronisation source.
        ii. The up link and down link (UL/DL) operating split. At present most, if not all, devices operate on a common UL./DL split that favours download over upload. In our interactions with content providers such as the BBC it is clear that content provision requires a UL heavy split. The DSA server algorithms are capable of determining the actual UL/DL splits that allow proximate base stations to operate without leading to interference. The DRAM therefore needs to be able to control the UL/DL settings and we have demonstrated this as can be seen later when we document the POC.
6. Initiate a command to stop the radio from passing traffic. There are a number of circumstances where the regulator may want to stop an installation from operating (national or local emergencies). This command needs to be initiated by the DRAM at the direction of the DSA server. In the POC we demonstrate that that the equipment is capable of receiving and responding to such a request within sub two minute response times

5.5.4 The DRAM DSA interface

We note that the DRAM DSA interface is simply an implementation of the DSA server protocol. An issue that the project encountered was in providing responses to DSA server heartbeats. This requires asynchronous operation as the instructions from the DSA server can arrive at any time, and have to be responded to in a timely manner. The operational systems (at TRL8) will need to comply with the defined requirements for the DRAM by responding to DSA server heartbeats as within the timeframe specified.

5.5.5 Determination of operational parameters

Within the PoC, we have used initial values for parameters such as heartbeat frequency, scan repetition, and co-channel interference sensing rate. The DSA system can vary these parameters as directed by the regulator. These are likely to be driven by criteria such as the speed with which the regulator wishes spectrum configuration, and radio transmission shutdown to be achieved.

6 POC demonstration

Once the three radios had been sourced and the DRAM middleware development completed with integration to the radios and the DSA server the project switched to focus on developing the end to end POC. The ability to run the POC as an end-to-end system represents a key project outcome that achieves the stated aim of building a TRL level 5 / 6 demonstrator. It will also confirm claims that the proposed dynamic spectrum allocation method can request and issue a spectrum lease in “minutes” rather than months. An additional outcome of the POC is the demonstration of the ability of the dynamic control of the radios to scam, sense CCI and change operating parameters under the control of the DRAM.

6.1 POC demonstrator components.

To demonstrate DSA server based spectrum allocation the POC required the assembly of the following system components:

- Access to a fully operational DSA server. This was hosted by Federated Wireless on an internet connected cloud based server. As noted earlier the DSA server was pre-populated with data that allowed spectrum leases to be issued at the locations where the POC demonstrator was operated.
- Access to a full operational DRAM instance. The POC DRAM instance was also hosted on an internet connected cloud server. The DRAM insurance had been prepopulated with key data that allowed:
    a. Authenticated communication with the DSA server
    b. Connection profiles for the 3 POC test radios:
        i. Band 3
            1. CellXica M3Q

Figure 33: CellXica M3Q radio example

            2. band 3 PC802 prototype radio

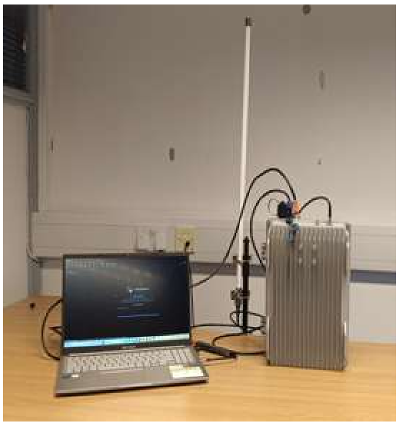


Figure 34: band 3 PC802 in field deployable unit

ii. Band n77
   1. Experimental n77 PC802 board

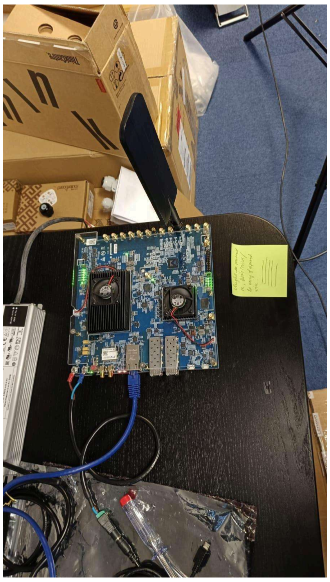


Figure 35: n77 PC802 experimental board

- Access to a pre-configured 4G/5G Open6GS core server that would allow UEs to connect via the radios to allow the passage of mobile traffic. This is a key outcome as the ability to secure access to spectrum is only of value if mobile communication is demonstrated
- Access to an active mobile network. This is required in order to demonstrate the operation of the spectrum scan functionality. In the case of testing conducted at the Telet Bath laboratory, access to the following mobile networks was available:
  a. Existing MNO band 3 networks operating in the Bath area
  b. Existing MNO band n78 networks operating in the Bath area
  c. Access to the ONEWord n77 mobile network operating in the Bath city centre area

d. Access to base stations in the Telet Bath laboratory that were able to be controlled to demonstrate CCI and the ability of the POC setup to support mobile operation

- Access to a number of items of test equipment that would allow the independent verification of the POC operation. This included:
    a. A spectrum analyzer that could operate in both band 3 and band n77 so that independent verification of the presence of RF signals can be demonstrated.
    b. Network Signal Guru (NSG) equipped mobile handsets that are capable of detecting detailed mobile signaling data such as MIB and SIB. These devices are also capable of collecting longitudinal data during the POC that can be analysed in more detail after the demonstration is completed.
    c. Access to the NSG Airscreen analysis application. This application allows for the replay of collected NSG data, as well as offering a number of more sophisticated signal analysis functions.
    d. Access to various UE devices equipped with the correctly configured SIM cards that can be used to “attach” to the via the POC demonstrator radios to the attached 4G/5G mobile network core server.

6.2 Key outcomes of the POC

The POC has a number of key outcomes that need to be demonstrated. These include:

- Successful ability to register the DRAM with the DSA server. This is a key outcome as for the dynamic spectrum sharing mechanism to work we need to establish a secure machine to machine (M2M) interface between the DRAM and the DSA server
- Successful ability to register multiple radios, and multiple types of radio (manufacturers) with the DRAM (and by inference independently control those radios
- Successful ability for the DRAM to interact with the registered radios. Specifically the ability to translate the different protocols and data formats used by differing radios to the common protocol and data format required by the DSA server.
- Demonstrate the capability of the three radios to detect and characterize the presence of other mobile radio base stations operating in the vicinity of these devices.
- Demonstrate the capability to detect CCI through a sense mechanism
- Demonstrate the capability of the radio to respond to remote re-configuration commands, and for the DRAM to frame, and execute these remorse commands.
- Demonstrate the ability of the DRAM to detect the asynchronous heartbeats issued by the DSA server in a timely manner and then execute local actions on the radios in line with the heartbeat instructions including the ability to direct a remote radio to stop passing traffic when directed so to do.

6.3 The dynamic frequency allocation demonstrations

As already noted, the project demonstrated POC operation in both band 3 and band n77 using two different radio architectures. This results in the overall POC being split into three main sub-phases as shown in the following table. The table also shows details of specific use-cases that the project has considered in terms of both system operation as well as economic modelling in WP3.

Table 9: POC demonstrator use cases

	1. DSAL (semi-manual)	**2. DLAL**	**3. DSAL (automated)**
Frequency Band	Band n77	Band 3	Band n77
Use-case	Short term/Rapid Access TV Content Production or Event	4G networks in unused MNO spectrum	Private 5G with automated densification
Relevance	Now	Now	Future
Duration	Up to 1 week	24 hours	As for SAL (indefinite)
Security of Tenure	Yes: first-come-first-served	No: MNO can 'bump' DLAL user without notice	Yes: but assignment may change
Requesting Assignment	Human uses DSA Server webpage	Radio (or client) contacts DSA Server automatically	Radio (or client) contacts DSA Server automatically
Heartbeat interval	-	10 minutes	10 minutes
Heartbeat purpose	-	1. Report measurements 2. Check assignment is still valid (i.e. no new MNO usage)	1.Report measurements 2. Check for changes to assignment (frequency, TDD, etc.)

6.4 Use Case 1: DSAL (semi-manual)

Use Case 1 is illustrated by means of the following pseudo machine to machine dialog which shows a typical sequencing of communication between the DRAM (client) and the DSA server (server). The DRAM communicates an action with the associated radio based on the responses received back from the DSA server.

Table 10: DSA to DRAM pseudo dialog

Protocol activity	System component	Pseudo Dialog
Registration	Client	"My device has this location and these technical parameters" (antenna, height AGL, etc.)
	Server	"That's good to know, thanks."
Spectrum Inquiry	Client	"What spectrum is available to my device?"
	Server	"You can use Channels A and B at 40dBm, or D at 20dBm, but don't use C."
Grant Request	Client	Please can my device use channel B at 40dBm?"
	Server	"Yes, you are now authorized to transmit for the next 24 hours, as long as you check with me every 10 minutes"
Heartbeat Request	Client (every 10 minutes)	"My device is using channel B, is this still OK?"
	Server	"Yes, keep going" OR "No! Stop transmitting immediately and start again."
Relinquish Grant	Client	"My device won't use channel B any more."
	Server	"That's good to know, thanks."
Some requests can also include Measurement Reports	Client	"My device just detected a device with PLMN 123 in channel B, with RSSI of -123dBm, etc."
	Server	"Good to know. Stop using channel B immediately and start again".

Each of the communications between the DSA server and the DRAM is in the form of a Javascript Object Notation (JSON) formatted message passed over a REST API on the DSA server. The following example JSON object shows an indicative DRAM spectrum inquiry and the associated DSA server response to the spectrum inquiry request:


```
{
 "spectrumInquiryRequest": [
  {
   "deviceId": "eacdd431-1f7f-48b8-8ba4-d838513e8d39",
   "inquiredSpectrum": [
```

```
          {
            "lowFrequency": 1805100000,
            "highFrequency": 1876700000
          }
        ],
        "bandwidth": 5000000
      }
    ]
  }
```

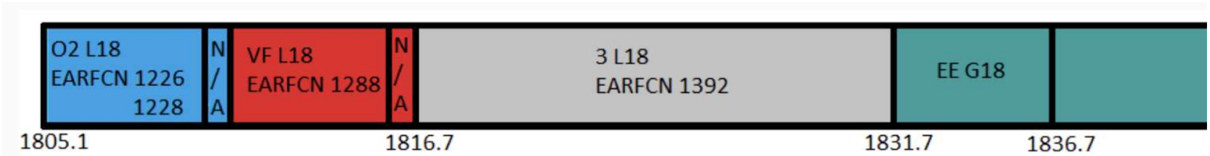


```
{
  "spectrumInquiryResponse": [
    {
      "deviceId": "eacdd431-1f7f-48b8-8ba4-d838513e8d39",
      "response": {
        "responseCode": 0,
        "responseMessage": "Success",
        "responseData": null
      },
      "availableChannel": [
        {
          "frequencyRange": {
            "lowFrequency": 1805100000,
            "highFrequency": 1810900000
          },
          "maxEirp": {
            "power": 40,
            "bandwidth": 5000000
          },
          "heartbeatInterval": 600,
          "expireTime": "2025-03-04T15:41:17Z",
          "licenceId": null,
          "channelType": "DYNAMIC_LAL",
          "coordinatedSystems": []
        },
        {
          "frequencyRange": {
            "lowFrequency": 1810900000,
            "highFrequency": 1816700000
          },
          "maxEirp": {
            "power": 40,
            "bandwidth": 5000000
        },
          "heartbeatInterval": 600,
          "expireTime": "2025-03-04T15:41:17Z",
          "licenceId": null,
          "channelType": "DYNAMIC_LAL",
          "coordinatedSystems": []
        }
      ]
    }
  ]
}
```

6.5 Use Case 2: Band 3 DLAL in Bath

In the second POC use case we demonstrate the dynamic operation of the sense and avoid capability of the radios and the attendant interactions with the DSA server. .

We note that the current band 3 band plan shows the following spectrum allocations:



6.6 Why we used Band 3 for the Local Access Licence PoC Use Case.

The choice of Band 3 for the LAL POC use case was a deliberate choice and reflects our experience in operating a number of mobile networks across the UK. Specifically we note that not all spectrum bands are of equal utility:

- Whilst n77 is currently the main band used for deployment of Private 5G Networks, it is not well suited for services offering Public Services
- The declared aim within the April 2023 DSIT Wireless Infrastructure Paper is to achieve *'nationwide coverage of public 5G SA service to all populated areas of the UK by 2030"*. In order to offer public service, it is necessary to use bands that are licensed to all UK MNOs. This limits operation to only 4 bands:
    - Band 20 - 800 MHz
    - Band 3 - 1800 MHz
    - Band 1 - 2100 MHz
    - Band n78 - 3.4-3.8 GHz
- **Carrier Profiles** MNO SIMs include Carrier Profile settings; these effectively turn off all bands that are not used by the MNO within the current country. This is done to reduce time and resources spent scanning bands which would not be used. As UK MNOs currently do not use n77, the result is that devices with MNO SIMs fitted will not see n77 Private Networks and will never attach.
- **Wider Use** Only 5G NR waveforms only permitted in n77. A much wider range of waveform (5G/4G/3G/2G and IoT) are available in Band 3. Band 3 is also one of the main anchor channels for multi-band Carrier Aggregation (CA).

6.7 Use case 2 sequencing

The sequencing of the PoC operations between the Independent Operator of Private Networks (IOPN) and MNOs is shown in the following table.

Black represents IOPN active, Red denotes MNO (Vodafone).

Table 11: Use case 2 sequencing

Sequence	VM02 Spectrum	VF Spectrum
Step 1 – status quo - Telet radio performs initial scan and finds no VM02 or VF usage in Band 3	-	-
Step 2 – Telet radio starts on initial assignment - (Vodafone)	-	
Step 3 – Incumbent MNO (Vodafone) starts using channel	-	 
Step 4 – CCI detected above interference threshold - Telet radio ceases and rescans band	-	
Step 5 – Telet radio starts using VMO2 spectrum		

6.8 Independent verification of spectrum usage

To independently demonstrate the change of operating frequency following the execution of the use case sequence we show both before and after spectrum analyser results:

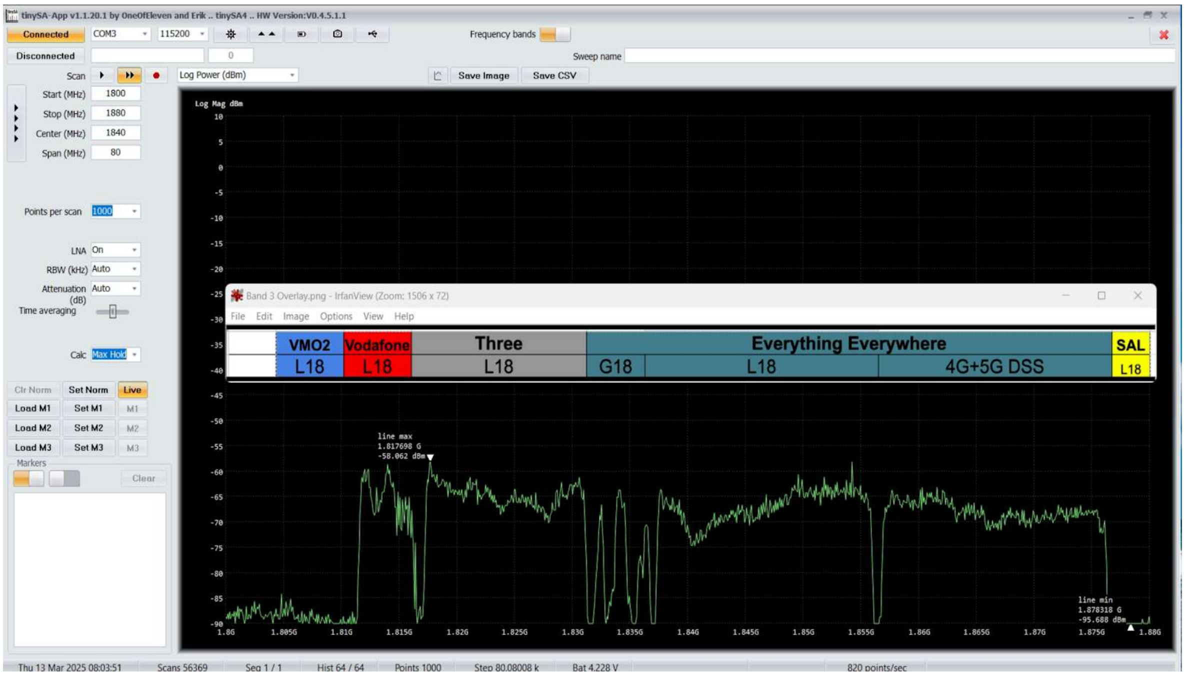


Figure 36: Example spectrum analyser plot showing the RF environment including the test radio operation. Occupied channels in the Three and EE spectrum allocations are clearly visible. Our DSA gNB is using a 5 MHz channel in the Vodafone allocation.

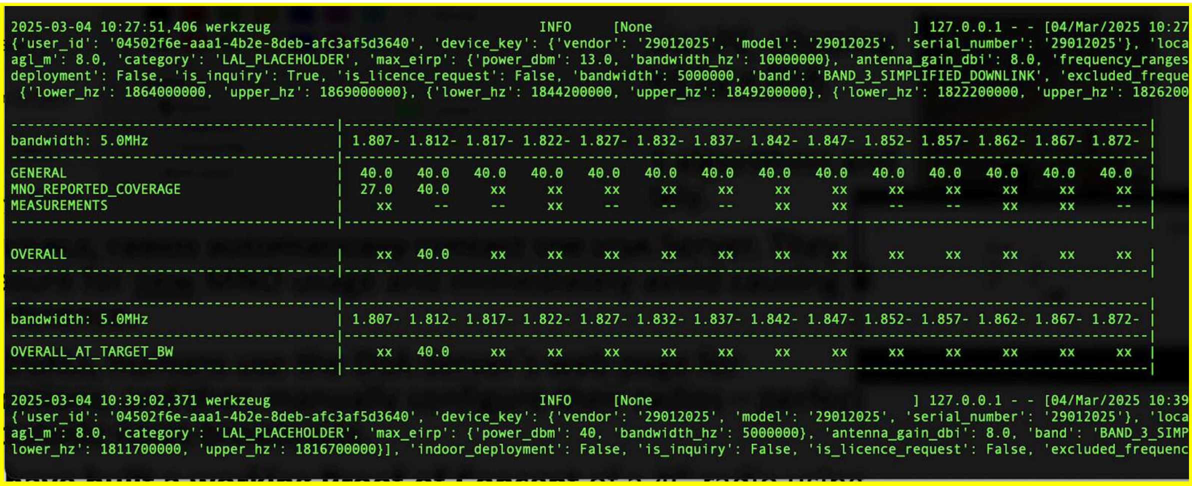


Figure 37: Co-channel interference is identified within 2 seconds of a MNO illuminating within their primary allocated spectrum. This causes the secondary user to release the channel and undertake a full band scan to collect full band spectrum occupancy, prior to submitting a new spectrum application to the DSA Server.

Figure 38: The secondary user receives a new spectrum allocation from the DSA server, and changes frequency to operate on the vacant VMO2 channel.

In addition to the use of the spectrum analyser, NSG was also used to verify the local band 3 RF environment, along with more detailed signalling information. The following Airscreen snapshot shows the environment. A more detailed trace of the equipment's operation can be found in the NSG trace data files on the project data archive.

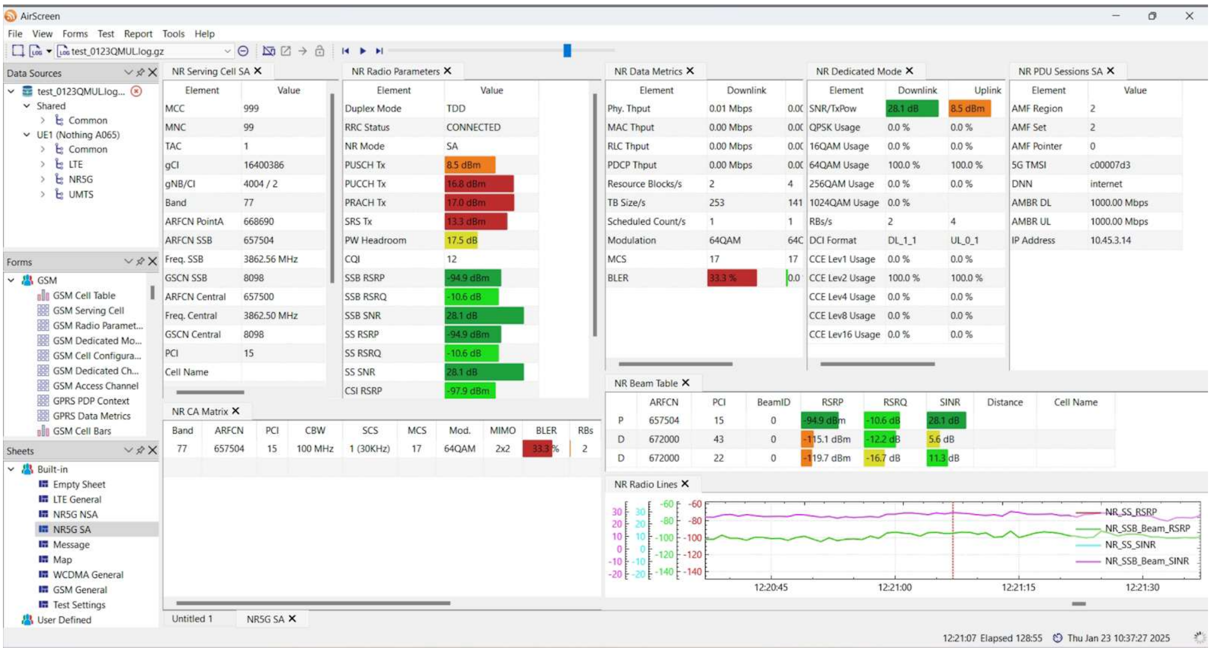


Figure 39: Example NSG AirScreen display showing captured local RF signalling environment

6.9 Spectrum Sharing Mechanism - Proof of Concept

6.9.1 Test Plan

The tests involved integrating the DRAM with multiple base stations, ensuring spectrum scans could be remotely executed. Data extracted from scans is formatted into a combined Spectrum Update and Channel Request which is pushed to the DSA server to inform spectrum availability and requests for usage of the spectrum in the given area.

The functionality of this process and carried out the proof of concept by setting up our own interfering transmitters that simulated incumbent users.

The spectrum sharing proof of concept test plan involved an end-to-end run through of the system, from gNB to DRAM to DSA server and vice versa. The focus of this was ensuring the following steps were functional:

1. Radio scan initiated and the data is processed by the DRAM and sent to the DSA server.

2. Secondary user submits a spectrumInquiryRequest, receives response…grantRequest&response…which will allow them to transmit on a given frequency, when a successful grantResponse is received.
3. radio transmitting

and then the second phase of this is when an incumbent/primary user is detected.

4. incumbent user transmitting
5. A stopped from transmitting
6. Goes through the whole spectrum inquiry and grant request process again.
7. Both radios transmitting and not interfering.

7 Conclusions and Next Steps

7.1 Conclusions

WP1 has successfully provided an end-to-end demonstration of technical solutions that increase the level of spectrum sharing relative to current spectrum authorisation and access methods, utilise network equipment to make and characterise measurements of the radio environment, and share measurements (via the DSA Server) with Ofcom and DSIT.

In particular, the following high-level outcomes were shown:

- Licensed DSA is technically viable and enables near-real time spectrum assignment from a DSA Server, instead of the existing multi-week or multi-month process;
- Coordinated Sense and Avoid is an efficient and cost-effective mechanism for detecting and protecting evolving MNO operations;
- Extending existing CBRS protocols for new jurisdictions, bands and sharing rules is feasible and well-positioned for the UK to leverage the existing CBRS device and software ecosystem;
- Proof of concept support for DSA Server performing inter-network interference management with a limited TDD alignment capability.

7.2 Next steps

To capitalize on the findings in this Sandbox, we recommend the following steps.

<u>Engage the community to build ecosystem support for approach and protocols</u>

- As regulatory actions are needed (see [WP3 Final Report]), the project participants should brief Ofcom on the findings, demonstrate the operation of the system, and discuss how LIcensed DSA can be realised in practice.
- Engage standards bodies and other industry and academic groups to formalize the protocols developed herein to broaden ecosystem support.
    - A DySPAN 2025 (London) poster presentation on the project is planned
    - Dr. James (Jody) Neel is scheduled to speak at a WINNF event in May in the US regarding the Sandbox, and the Client-Server Protocol[1]

<u>Develop the technology to TRL 8</u>

- Increase deployment scale beyond single site networks so that more realistic coordinated sense and avoid testing can be performed and so that inter-network interference alignment techniques can be prototyped. Suggested scale for this is to run a full Pilot Deployment within a defined area (25 x 25 km), operating DSA within the area under an OFCOM T&D Licence.

[1] https://www.wirelessinnovation.org/2025-international-spectrum-sharing-workshop

- Increase reliability via more rigorous testing of challenging field scenarios and by bringing the DSA Server closer to commercial-grade offering (e.g., increasing reliability / uptime and addressing identified security objectives)
- Improve application realism via field trials for event-based / short term use cases with partner DSA Operators (e.g. BBC) and possibly MNOs
- Expand the supported range of device support for both DRAM integration and gNB measurements (Level 2) to identify potential ecosystem issues that may limit support
- Create more realistic prototypes modeling interactions with Ofcom, such as the licensing step of licensed DSA and an interface to enable Ofcom to conduct enforcement actions
- Consider funded real-world deployments similar to the Open Networks Ecosystem projects where smaller network operators are funded to work with local authorities to deploy DSA enabled radios to provide mobile and FWA services to community events.

Improve and extend the functionality to further increase the benefit of the technology

- Increase capabilities via direct extensions of the technology, such as supporting multi-band licensing and re-assignments, which would reduce the risks for DSA operators building private networks in shared spectrum without a protected anchor band
- Create new capabilities that build on the technology to enable new functions, e.g., collecting and making available spectrum survey (utilization, measurements) data from managed RANs and using that data for automated enforcement activities and identification of interferers from measurements
- Develop deferred technologies, such as:
    - Providing an interface for MNOs to self-report planned coverage updates
    - TDD alignment with non-cooperative networks
    - Level 3 Data Collection - UE reporting measurements and PLMN detections, which will likely necessitate alternate UE provisioning, e.g., for a wider PLMN scan list on initialization

8 Glossary of Terms and Abbreviations

5GNR – 5G New Radio. Standard 5G Waveform

5GNT – 5G New Thinking. An earlier project whose results are leveraged in aspects of this project

AFC – Automated Frequency Controller

AGL – Above Ground Level

AP – Access Point

CBRS – Citizens Broadband Radio Service. Shared spectrum in the US in the range 3.55-3.7 GHz characterised by the use of a spectrum database (Spectrum Access System) to enforce spectrum sharing rules for spectrum access

CCI - Co-Channel Interference

Client – (DSA) Client of the DSA Server REST Protocol - The client may be a single device or middleware that represents one or more devices where the device or the middleware implements the DSA Server-Client Protocol.

CxG – Coexistence Group – A group of DSA devices abiding by a common interference management policy.

CxM – Coexistence Manager – An entity responsible for managing one or more CxG (selection of interference management policy and group membership)

DRAM - Dynamic Radio Access Manager (Middleware interfacing Radios to DSA Server)

DSA – Dynamic Spectrum Access

DSIT – Department for Science Innovation and Technology

EIRP – Equivalent Isotropically Radiated Power (dBm)

gNB – The gNB (gNodeB) is the base station within a 5G New Radio (NR) system.

Grant – A time-limited assignment of spectrum to a client operator according to the configuration information provided by the Client

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol + TLS

ICG – Interference Coordination Group – A collection of DSA devices capable of managing interference among themselves.

IOPN – Independent Operator of Private Networks, e.g. Telet

Inquiry – A request on the availability of spectrum for a client operator according to the configuration information provided by the Client

JSON – JavaScript Object Notation

Server - The singular or collection of (DSA) Servers implementing the Server side of the DSA Server Client REST Protocol. It may be implemented by a single entity or a collection of entities.

TLS – Transport Layer Security

URL – Uniform Resource Locator

9 References

[1] Ofcom, “Enabling wireless innovation through local licensing,” 25 July 2019.

[2] Ofcom, “Shared Access Licence: Guidance Document,” 20 September, 2022.

[3] Ofcom, “Local Access Licence: Guidance Document,” July 2019.

[4] Ofcom, “Local Access Licence Chart,“:10 June, 2024.

[5] Ofcom, “Enhancing the Shared Access framework: Statement on further measures to support licensees and enable new use cases,” 2 December 2024.

[6] Ofcom, “Update on Spectrum Policy Implementation Timelines for Shared Access Licensing and Radio Amateur Licensing Framework,” 6 December, 2025.

[7] Ofcom, “Implementing TV White Spaces,” 12 February 2015.

[8] Wireless Innovation Forum (WINNF), “Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS)-Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification,” Document WINNG-TS-0016, v 1.2.6, 29 November 2020.

[9] WINNF, Extensions to SAS-CBSD Interface Technical Specification (Release 2), WINNF-TS-3002, 6 June, 2023.

[10] OnGo Alliance, “CBRS Coexistence Technical Specifications,” CBRSA-TS-2001, v3.1.0, 17 July 2020

[11] ISED, "Non-competitive local licensing (NCLL)” 11 December 2024.

[12] IEEE, “IEEE Std 802.11h-2003 Part 11,” 14 October 2003.

[13] Wi-Fi Alliance, “AFC System to AFC Device Interface Specification v1.5,” May 5, 2023.

[14] Federated Wireless, “Adaptive Network Planning Tool,” Available online: https://www.federatedwireless.com/planning-tool/

[15] Federated Wireless, “5GNT Spectrum Availability Server,” Available online: https://www.5gntsharedaccesslicencing.uk/

[16] Ofcom, “Mobile and broadband checker,”.Available online: https://checker.ofcom.org.uk/en-gb/mobile-coverage

[17] Ofcom, “2020 coverage obligations: Notice of compliance verification methodology,”February 20, 2024.

[18] 3GPP “User Equipment (UE) conformance specification; Radio transmission and reception; Part 4: Performance,” TS 138.521-4-NR, 8 October, 2024.

[19] 5GNT, “A Standard for Client-Server DSA,” Deliverable D3C-4, 28 February, 2022

[20] Wi-Fi Alliance, “AFC System to AFC Device Interface Specification v1.5”

[21] 5G New Thinking, “Client-to-Server Communications for Dynamic Spectrum Access: ANNEX: Analysis & Discussion,” February 2022.

[22] OnGo Alliance, “CBRS Coexistence Technical Specifications,” CBRSA-TS-2001, v3.1.0, 17 July 2020. Available online: https://ongoalliance.org/wp-content/uploads/2021/04/CBRSA-TS-2001-V3.1.0_Approved-for-publication.pdf

[23] IETF RFC-2616, “Hypertext Transfer Protocol -- HTTP/1.1”, June 1999

[24] Ofcom, OfW 590 Technical Frequency Assignment Criteria for Shared Access Radio Services, Ofcom, Available online: https://www.ofcom.org.uk/__data/assets/pdf_file/0027/183744/Shared-Access-technical-frequency-assignment-criteria.pdf

[25] Ofcom, Consultation: Expanding access to the 6 GHz band for mobile and Wi-Fi services, 13 February 2025, https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-3-4-weeks/consultation-expanding-access-to-the-6-ghz-band-for-commercial-mobile-and-wi-fi-services/main-document/expanding-access-to-the-6-ghz-band-for-mobile-and-wi-fi-services.pdf?v=391052

[26] IETF RFC-8259, "The JavaScript Object Notation (JSON) Data Interchange Format", December 2017

[27] Wireless Innovation Forum, “Signaling Protocols and Procedures for Citizens

Broadband Radio Service (CBRS): Spectrum Access System (SAS)-Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification," Document WINNG-TS-0016, v 1.2.6, 29 November 2020. Available online: https://winnf.memberclicks.net/assets/CBRS/WINNF-TS-0016.pdf

[28] Wireless Innovation Forum, "CBRS Threat Model Technical Report," Document WINNF-15-P-0089, v1.0.0, 11 May, 2016.

[29] Wireless Innovation Forum, "CBRS Communications Security Technical Specification," Document WINNF-TS-0065, v2.0.0, 24 April, 2017.

[30] Template WSDB contract, Ofcom, 2015, previously available at https://www.ofcom.org.uk/_resources/documents/spectrum/spectrum-information/white_space_database_contract_for_operational_use_of_wsds.pdf.

[31] WSIP API specification, Ofcom - no longer available online.