RED
TECHNOLOGIES

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)
)
Wireless Telecommunications Bureau and)
Office of Engineering and Technology) GN Docket No. 15-319
Establish Procedure and Deadline for Filing)
Spectrum Access System (SAS))
Administrator(s) and Environmental Sensing)
Capability (ESC) Operator(s) Applications

Proposal by RED Technologies for Environmental Sensing Capability (ESC)

Version: 1.0

Date: September 5, 2019

Pierre-Jean Muller
Chief Executive Officer
RED Technologies
130, rue de Lourmel
75015 Paris – France

EXECUTIVE SUMMARY

RED Technologies, a leading developer of innovative spectrum management, is a French SME born from the innovation spectrum scarcity triggers. Today, our award-winning company, whose focus is dynamic spectrum management, is the premier enabler of Licensed Shared Access (LSA) with its cloud-based spectrum sharing solution, already piloted with global telecoms players across two major European terrains.

RED Technologies has been deeply involved in the regulation framework changes that enabled LSA and has patented inventions related to facilitating their success. Through our engagement with the ECC and CEPT, we follow and influence spectrum sharing policy and we have been leading LSA standardization activities at ETSI and 3GPP.

It is from this pivotal position that few years ago we did seek to invest in the US, we did apply to become SAS Administrator and we did actively contribute to the standards within the Wireless Innovation Forum (WInnF). Armed with this experience and after carefully reviewing what our market options are for getting ESC services from prospective ESC operators, we have decided we need to secure ESC services with our own where and when other alternatives are either not available or not satisfactory. Therefore, RED Technologies wish to apply to become an ESC operator, the focus of this proposal.

Please note RED Technologies did apply to become a SAS administrator and the application *[Ref. 13]* is currently under review by the FCC.

RED Technologies comprises a team of seasoned global telecoms professionals flanked by an influential Board, who together bring deep and unique expertise and experience. Our proficiency in the design and delivery of LSA including sensing capabilities has served as a test-bed and a springboard for our fully functional SAS + ESC solutions.

Investing in the US, a country so profoundly linked to telecoms innovation and entrepreneurship, is RED Technologies' paramount focus today. It is our intention to contribute to US job creation, to innovation and to the narrowing of digital divides by providing a locally delivered, state-of-the art, secure and rapid spectrum management service. To this effect, we will open a local service center on the East coast supported by a trained, locally recruited team. We expect to see fruitful idea exchange across our European and US team members, partners and customer base as we evolve our dynamic spectrum sharing solutions in parallel.

Our intention is to expand our offer in the US as part of a business strategy that reaches far beyond Europe and we bring robust, tested technology and the force of a dynamic, global-minded and skilled team to this task. We also offer a unique stance on spectrum management innovation through our knowledge of LSA in Europe and CBRS in the US which, we believe, will serve to stimulate entrepreneurship and trigger creative thinking within the sector.

Content

Figures

Tables

1. DOCUMENT PURPOSE

The Wireless Telecommunications Bureau and the Office of Engineering and Technology seek proposals for future Spectrum Access System Administrator(s) and Environmental Sensing Capability operator(s) in the 3550-3700 MHz band (3.5 GHz Band). See Public Notice ([Ref. 01], [Ref. 03]).

This document is the response from RED Technologies for managing of Environmental Sensing Capability (ESC).

Note:

The response of RED Technologies for the management of Spectrum Access System (SAS) has already been the subject of a separate response described in [Ref. 13].

This Application is organized as follows:

- Section 2 describes RED Technologies compliance with FCC and WInnF requirements,
- Section 3 reminds the 3.5 GHZ CBRS band concepts and objectives,
- Section 4 presents RED Technologies along with its technical and financial capabilities,
- Section 5 provides details about RED Technologies' SAS administration and product,
- Section 6 provides appendix.

2. FCC & WINNF COMPLIANCE

2.1. COMPLIANCE WITH FCC

2.1.1. FCC rules Part 96 Affirmation

RED Technologies affirms that its ESC will comply with all applicable rules as well as applicable enforcement mechanisms and procedures:

- **Subpart A – GENERAL RULES**
  - *96.11 – Frequencies*
- **Subpart G – ENVIRONMENTAL SENSING CAPABILITY**
  - ***96.67 – Environmental Sensing Capability***

Note:

Rules marked in bold are specific to ESC.

Rules marked in italic contain some ESC requirements but not only.

2.1.2. FCC Public Notice compliance matrix

The table below lists requirements coming from the FCC Public Notice document ([Ref. 01], section IV) and refers to the paragraphs of this document that meet these requirements.

	Requirement Description	Reference	Comment
General requirements			
1	A detailed description of the scope of the functions that the SAS and/or ESC would perform	3.2.6	
2	A demonstration that the prospective SAS Administrator or ESC operator possesses sufficient technical expertise to operate an SAS and/or ESC, including the qualifications of key personnel who will be responsible for operating and maintaining the SAS and/or ESC.	4.1 4.2 4.3	
3	The prospective SAS Administrator or ESC operator must demonstrate that it is financially capable of operating an SAS and/or ESC for a five-year term. The proposal must include a description of the prospective SAS Administrator or ESC operator's business structure including ownership information. To the extent that the proponent will rely on fees to support its operations, the proposal should also describe the fee collection process and the entities from which the fees will be collected.	4.1 4.2 4.3	
4	A description of how data will be securely communicated between the SAS and its associated ESC and how quickly and reliably these communications will be accomplished.	5.1.3.2	
5	Technical diagrams showing the architecture of the SAS and/or ESC and a detailed description of how each function operates and how each function interacts with the other functions.	5.1.2	
6	A description of the propagation model and any other assumptions that the prospective SAS Administrator or ESC operator proposes to use to model operations and facilitate coordination in the band.	Not Applicable for ESC	

7	A description of the methods that will be used: - to update software and firmware and - to expeditiously identify and address security vulnerabilities.	5.4 5.1.3.1 5.1.3.2	For ESC only
8	An affirmation that the prospective SAS Administrator and/or ESC operator (and its respective SAS and/or ESC) will comply - with all of the applicable rules - as well as applicable enforcement mechanisms and procedures	2.1.1	For ESC only
Specific ESC requirements			
1	A description of the methods (e.g., interfaces, protocols) that will be used by the ESC to communicate with the SAS. It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or otherwise corrupt the operation of the ESC in performing its intended functions.	5.1.3.2	
2	A description of the sensing methodology it will use to detect federal transmissions and determine that the spectrum needs to be evacuated. This description must include a detailed description of the type of sensors to be used (i.e., infrastructure or device based), the sensing architecture to be employed, the sensing thresholds, any processing of sensor data, sensor sensitivity, and sensor resiliency to receiver front-end saturation and burn-out. The prospective ESC operator must also provide a description of the safeguards that will be used to "ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required to effectively operate the ESC by Part 96."	5.1.1 5.1.4	
3	A description of the methods (e.g., interfaces, protocols) that will be used by sensors to communicate with the ESC and the procedures, if any, that it plans to use to verify that all sensors can communicate with the ESC in a timely and secure manner. It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or individual sensors or otherwise corrupt the operation of the ESC in performing its intended functions.	5.1.3.3	

Table 1: FCC Public Notice compliance matrix

2.2. Compliance with WInnF

RED Technologies affirms that its ESC will comply with all WInnF requirements defined by the Release 1 documents and later releases when deemed available; and in particular, those referred in section §6.1.

Furthermore, RED Technologies, as an active member of the WInnF, plays a contributor role in continuous development of 3.5 GHz CBRS standards and tests. Given this, we expect our ESC product team to continuously update the product with latest standard releases.

2.3. Staff responsible for compliance

RED Technologies designates Luc DAVIT, senior manager at RED Technologies, to ensure compliance with the rules set forth by the Commission.

3. FCC' 3.5 GHZ CBRS BAND

3.1. A THREE-TIERED ACCESS MODEL

Historically, the 3550-3700 MHz (3.5 GHz) band was reserved for the Department of Defense (DoD) for radar systems but also for Fixed Satellite Service (FSS). The Federal Communications Commission decided to open this band to new actors and so created the **Citizens Broadband Radio Service (CBRS)**.

To do this, a three-tiered access model has been identified:

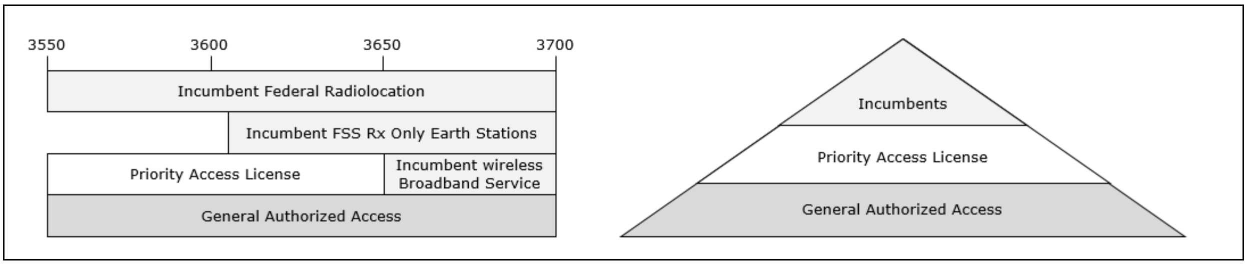

3550
3600
3650
3700
Incumbent Federal Radiolocation
Incumbent FSS Rx Only Earth Stations
Priority Access License
Incumbent wireless Broadband Service
General Authorized Access
Incumbents
Priority Access License
General Authorized Access

Figure 1 Three-Tier Model

This model defines the rules for spectrum sharing between the different actors who have been split into three main categories:

- Incumbent Users:
    - Authorized Federal entities, Fixed Satellite Service (FSS) operators, or Grandfathered Wireless Broadband Licensees. These users have absolute protection from interference from other users.
- Priority Access Licensee Users:
    - Users who hold one or more Priority Access License (PAL). These users shall be protected from interference from other PALS and General Authorized Access users.
- General Authorized Access (GAA) Users:
    - Users who are not be subject to individually-issued licenses and shall not cause interference to higher level users (Incumbent & PAL).

To manage the rules of this spectrum sharing model a 3.5 GHz CBRS band system has been defined by the FCC (see [Ref. 04])

3.2. 3.5 GHz CBRS band system Overview

The 3.5 GHz CBRS band system is composed of a set of functional entities linked together as shown in the diagram below:

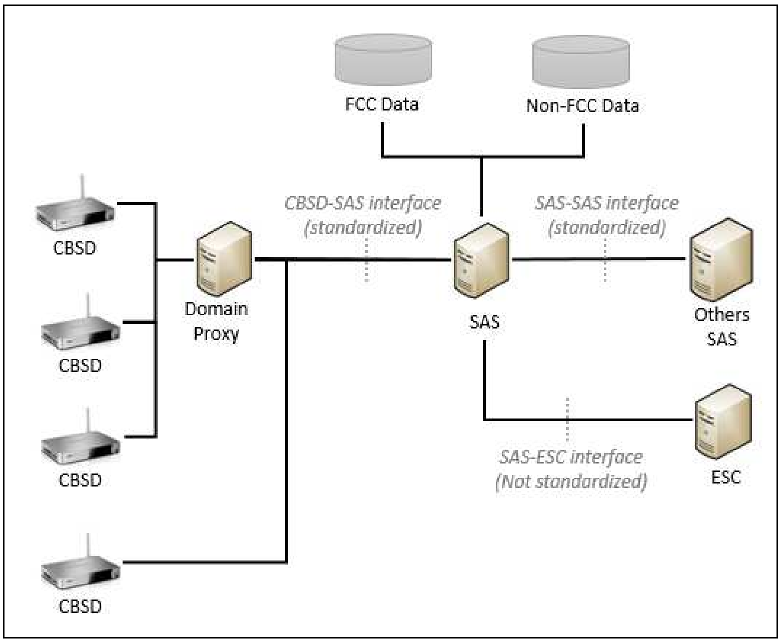


Figure 2 3.5 GHz CBRS band system overview

3.2.1. CBSD

Citizens Broadband Radio Service Device (CBSD) are fixed stations, or sets of fixed stations, that operate on a Priority Access or General Authorized Access.

For CBSDs' that comprise multiple nodes or networks of nodes, CBSD requirements apply to each node even if network management and communication with the SAS is accomplished via a single network interface.

3.2.2. Domain Proxy

The Domain Proxy is an intermediate device between the CBSDs and the SAS. On the one hand, it synchronizes, and aggregates messages sent from the CBSDs to the SAS, and on the other hand, it desegregates and roots messages sent from the SAS to the corresponding CBSDs.

3.2.3. FCC Data

The FCC provides a set of data for the 3.5 GHz CBRS band needs and for: FSS sites, Grandfathered Wireless Broadband Licensees protection zones, FCC IDs for CBSDs, PAL licenses.

This data can be retrieved from the FCC web portal.

3.2.4. Non-FCC Data

Additional non-FCC data that is also required: Census tracts, Maritime and terrestrial borders, Exclusion zones, Portal DPAs, E-DPAs.

This data is provided either by the United States Census Bureau or by the National Telecommunication and Information Administration (NTIA) using their web portal.

Other data such as Shared PAL data, CPI credentials, Blacklisted CBSDs, Leasing agreement (secondary market), are either provided by the WInnF or by other organizations.

3.2.5. SAS

The SAS is the entity of the 3.5 GHz CBRS band system which authorizes and manages the use of spectrum in the 3550-3700 MHz (3.5 GHz) band. Its main goal is to protect the actors from interference according the rules defined by the Three-Tier Model.

3.2.6. ESC

The Environmental Sensing Capability (ESC) is the system that detects and communicates the presence of a signal from federal incumbent actors to the SAS to facilitate shared spectrum access consistent with sections 96.15 and 96.67 of the document [Ref. 04].

It must be managed and maintained by a non-governmental entity, and its main functions (as defined in the documents [Ref. 04] and [Ref. 05]) are to:

- Accurately detect the presence of a signal from a federal system in the 3550-3650 MHz band using approved methodologies that ensure that any CBSDs operating pursuant to ESC will not cause harmful interference to federal Incumbent Users;
- Communicate information about the presence of a signal from a federal Incumbent User system to one or more approved SASs;
- Maintain security of detected and communicated signal information;
- Comply with all Commission rules and guidelines governing the construction, operation, and approval of ESCs;
- Ensure that the ESC shall always be available to immediately respond to requests from authorized Commission personnel for any information collected or communicated by the ESC;
- Ensure that the ESC operates without any connectivity to any military or other sensitive federal database or system;
- Ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required to effectively operate the ESC by Part 96;

The ESC includes a system of RF sensors to detect federal frequency use in the 3.5 GHz Band.

ESC equipment may be deployed in the vicinity of the E-DPA (ESC monitored Dynamic Protection Area) to accurately detect federal Incumbent User transmissions.

The ESC must be developed, managed, and maintained by a non-governmental entity and should not require oversight or day-to-day input from NTIA or DoD.

4. ABOUT RED TECHNOLOGIES

The following section amends the strategy of RED defined in the referenced document [Ref. 13] (section 4. ABOUT RED TECHNOLOGIES).

4.1. BUSINESS STRATEGY

RED Technologies firmly believes that shared spectrum will create new commercial opportunities.

Cellular (LTE, 5G) services have made available a considerable number of frequency bands but these are assigned on an exclusive basis and are operated by "happy few" carriers.

The 3.5 GHz CBRS band opens up disruptive new models such as neutral host and private networks.

Neutral host allows deployments using common spectrum and common deployment and provides neutral host services (like Wi-Fi). However, while it is deployable as a standalone / private network, neutral host can interwork with legacy 3GPP carrier networks. This creates a fresh win-win situation because carriers that did not intend to deploy in-building or rural outdoors, can gain access to a much broader footprint

Neutral Host addresses the issues that many venue owners and enterprise IT leaders experience with in-building wireless. These include poor cellular coverage for voice services, overutilization of the 5 GHz Wi-Fi band, and a need for higher quality wireless data services.

Neutral Host native capabilities allow a local service provider network to support subscribers of multiple nationwide carriers within buildings thanks to the opportunity made possible by the 3.5 GHz CBRS band to deploy cellular (LTE) services without the "barrier-to-entry" expense of fully licensed spectrum.

RED Technologies will focus its business development on those local service providers offering a dedicated SAS services, PAL "Lessor/Lessee" optimized spectrum coordination and a REM-based interference management system specialized for private network deployment.

RED Technologies believes that once the 3.5 GHz CBRS band is deployed and commercially proven, the model will be exported and deployed globally and potentially extended to many other frequency bands in sub 1 GHz, sub 6 GHz and millimeter wave (mmWave) spectrum to feed much anticipated spectrum needs for 5G.

4.2. TECHNICAL CAPABILITY

RED Technologies is technically competent to develop, test and receive certification for its ESC system, in compliance with Commission rules and Wireless Innovation Forum standards.

RED Technologies leveraged its product development and testing from its field tested LSAlive© platform which was operated during multiple-month field trails in Rome, Italy in partnership with Nokia and Qualcomm, and in Paris, France in partnership with Ericsson and Qualcomm.

Since 2012 the company has developed **extended know-how** in the following domains:

- Spectrum Sharing,
- Cognitive Radio - Radio Environment Map (REM),
- Radio Propagation and Clutter Modelling,
- RF Sensing,
- LTE Radio Network Engineering and Self Organizing Networks,
- Standards (ETSI, 3GPP, Wireless Innovation Forum),
- Geographical Information System (GIS),
- High Performance Computing,
- Database development, security, networking, cloud, and web.

RED Technologies received the prestigious Business France, Best Telecom Innovation Award at Mobile World Congress in 2015 (MWC) - https://www.linkedin.com/pulse/mwc15-red-technologies-receives-best-telecom-award-2015-abitbol?trk=pulse-det-nav_art.

4.3. FINANCIAL CAPABILITY

RED Technologies is a well-capitalized enterprise fully supported by its main shareholder CapDecisif Management.

RED Technologies adopts a clear business strategy for its US market (see §4.1).

In addition, RED Technologies will charge its SAS customers (PAL and GAA users) fees for its spectrum management and others value added services.

5. RED TECHNOLOGIES' ESC SOLUTION

5.1. SOLUTION OVERVIEW

5.1.1. Introduction

Our Environmental Sensing Capability (ESC) system is a system that continuously acquire, digitize and analyze the presence of a signal from federal incumbents in the 3550-3650 MHz band. It can detect radar waveforms as described in [Ref. 15], and notify the SAS of in-band incumbent radar activity within 60 seconds with 99% probability.

Our ESC is being deployed near ESC-monitored Dynamic Protection Area (E-DPA) defined along the Alaska; USA West, East and Gulf coasts; Puerto Rico and Hawaii.

Our ESC has no connectivity to any military or any other sensitive federal database. Moreover, it does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required to effectively operate the ESC as per Part 96.

5.1.2. Architecture

Our Environmental Sensing Capability (ESC) system, is composed of 2 mains entities:

- RF ESC Sensors which are in charge to listen to the radar activity of 1 or multiple E-DPAs.
- The ESC Controller which is in charge, upon notification from the RF ESC Sensors to notify the SAS of the activation / deactivation of an E-DPA.

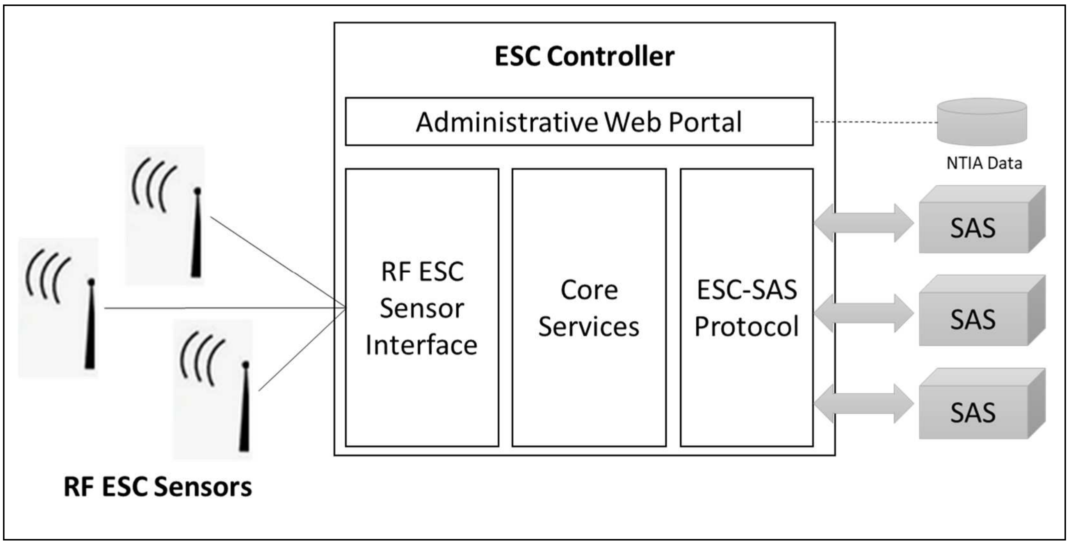


Figure 3 : ESC architecture overview

In the context of our architecture, the action of seeing a radar pulse burst is called "**detection**" and the action of knowing that a radar is present in an E-DPA is called "**declaration**".

An ESC RF Sensor and its associated ESC controller are responsible for the process to "detect" then "declare" that a radar is present within an E-DPA.

The ESC controller and its associated SASs are responsible to undertake subsequent mitigation actions to protect radars from being interfered from CBRS activity.

5.1.3. ESC Controller

5.1.3.1. Administrative Web Portal

This Administrative Web Portal provides access to RED Technologies authorized staff for administration, maintenance and monitoring of the ESC.

Any authorized staff must authenticate with his/her login and password to access the Administrative Web Portal.

Authorized staff can use the Administrative Web Portal to:

- To know the status of an E-DPA if needed (see figure on right)
- To update E-DPA.kml file when new file is provided by NTIA (see [Ref. 17])
- To know the status of the communication with RF ESC sensors (alive / dead)
- To know the status of the communication with the SAS (alive / dead)

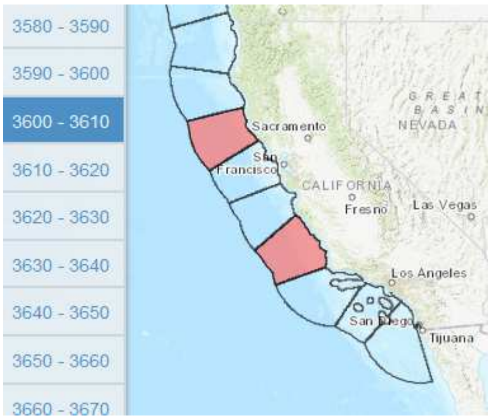


Figure 4 : Example of activated E-DPA

5.1.3.2. ESC -SAS Protocol

To date, no ESC-SAS protocol has been standardized, therefore RED Technologies has defined a proprietary protocol for communicating between its SASs and the ESC.

This ESC-SAS protocol takes over some principles defined by the SAS-SAS ([Ref. 06]) and SAS-CBSD ([Ref. 07]) interfaces, and security rules defined in document [Ref. 09] and [Ref. 10]:

- Protocol based on the HTTPS
- TLS mutual authentication (TLS-v1.2) using certificate
- TLS Encryption
- Protocol message encoded using JSON (RFC-7159)
- SAS-ESC Registration / Deregistration
  - Used by the SAS to register / deregister to the ESC
- SAS-ESC Heartbeat (including E-DPA status)
  - Used periodically by the SAS to check that the ESC is still alive, including E-DPA status
- SAS-ESC DPA Status Notification (including E-DPA status)
  - Used by the ESC to notify a change of E-DPA status to the SAS

In the future, if the WINNF or any others standard organizations decide to standardize this ESC-SAS interface, RED Technologies will study the possibility to adopt this standard.

5.1.3.3. RF ESC Sensor interface

The interface between RF ESC Sensors and ESC Controller is proprietary.

As for ESC – SAS Protocol, HTTPS with TLS mutual authentication and TLS Encryption is used for RF ESC Sensor interface.

An ESC RF Sensor and its associated ESC controller are responsible for the process to "detect" then "declare" that a radar is present within an E-DPA.

An ESC RF sensor notifies the ESC controller of the detection or disappearance of a radar signal on one or multiple 10 MHz channels in 3550 – 3650 MHz band in quasi real-time i.e. with less than a few seconds of latency.

The ESC-ESC protocol will take over some principles defined by the SAS-SAS ([Ref. 06]) and SAS-CBSD ([Ref. 07]) interfaces, and security rules defined in document [Ref. 09] and [Ref. 10]:

- Protocol based on the HTTPS
- TLS mutual authentication (TLS-v1.2) using certificate
- TLS Encryption
- Protocol message encoded using JSON (RFC-7159)
- ESC-ESC Heartbeat
    - Used periodically by the ESC controller to check that the ESC sensor is still alive
- ESC-ESC Detection Flag Notification
    - Used by the ESC sensor to notify a detection or disappearance of a radar signal on one or multiple 10 MHz channels in 3550 – 3650 MHz band

5.1.3.4. Core Services

Based on the Detection Flag Notification from the ESC RF Sensors, the Core Service identify the corresponding E-DPAs/channels . Nevertheless, no information will allow the ESC controller to geolocate the position of the incumbent in the zone managed by the sensor.

The Core Service notifies the SAS of the change of state of the corresponding E-DPAs/Channels via the ESC-SAS protocol.

If the communication between an ESC RF Sensor and the ESC Controller is down, the ESC Controller informs the SAS that the associated E-DPAs/Channels are activated.

If there is no ESC RF sensor on one or multiple E-DPAs, those DPAs/Channels are always activated.

5.1.4. RF ESC Sensors

The ESC RF sensor includes a RF front-end, a baseband processor and co-processor. The baseband processor runs Radar pulse burst detection algorithms to detect the presence of Radar signal as well as the carrier frequency of the Radar signal. This all takes place in real time.

The ESC RF Sensor main characteristics are:

- 20 MHz to 6 GHz real-time remote spectrum monitoring system.
- Automated wide area, close-proximity signal monitoring, interference detection, identification, location & reporting.
- Analog and digital signal analysis with I/Q recording for signal classification, demodulation and decoding.
- The RF Sensor is equipped with a tailored RF Front End filtering composed of a passband filter, a Low Noise Amplifier and an Automatic Gain Control function with a filter frequency-response curve with at least 60 dB of dynamic range.
- The ESC RF sensor solution is IP67 proof with power over Ethernet (PoE) and Ethernet/IP based backhaul.
- The RF ESC sensor solution has been designed to meet certification requirements as per TM-18-526 ([Ref. 14]), TM-18-527 ([Ref. 15]) and TM-18-534 ([Ref. 16]).

5.2. ESC CERTIFICATION

RED Technologies will follow the test and certification process as defined by "Procedures for Laboratory Testing of Environmental Sensing Capability Sensor Devices" [Ref. 15] and [Ref. 16].

5.3. ESC DEPLOYMENT

RED Technologies will deploy its ESC Controller, in a cloud environment, whereas the ESC RF Sensor is a standalone equipment deployed outdoor on a tower.

5.3.1. ESC Controller Deployment

After the study of several service providers, **RED Technologies selected Amazon Web Services (AWS),** to host its ESC Controller, for the following main reasons:

- AWS provides lots of services and tools for computing, storage, database, networking, security.
- **Data is hosted on US territory (Oregon, California, Virginia, and Ohio).**
- AWS IT infrastructure is designed and managed in alignment with the best security practices and a variety of IT security standards:

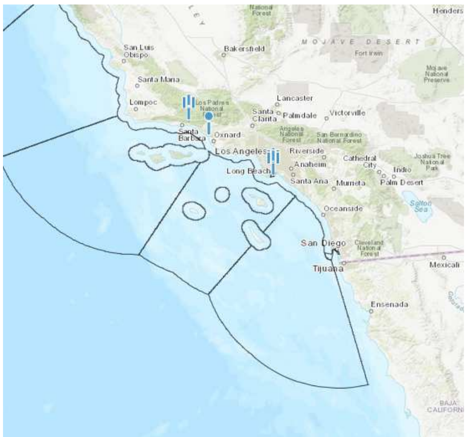
5.3.2. ESC Sensor Deployment

the ESC RF Sensor is a standalone equipment deployed outdoor on a tower.

Radio site acquisition and ESC sensor equipment installation will be performed with the utmost attention to detail, which in turn will ensure that it is done in accordance with state-of-the-art engineering and WInnF specifications.

Deployments will be market driven.

We will also propose that our ESC to be used as back-up for other ESC operators and vice-versa.



5.4. ESC SOFTWARE/FIRMWARE UPDATE

5.4.1. Update the ESC Controller Software

The ESC Operator will use the *AWS Elastic Beanstalk* (see §**Error! Reference source not found.**) to deploy, manage and scale the Administration Web portal on servers and will follow the following AWS related procedures:

- Launch an application with AWS Elastic Beanstalk (https://aws.amazon.com/getting-started/tutorials/launch-an-app/)
- Update your Elastic Beanstalk App (see https://aws.amazon.com/getting-started/tutorials/update-an-app)

5.4.2. Update the ESC RF Sensor Firmware and Hardware

ESC RF sensor can be replaced in part or fully – special attention will be made to minimize the downtime for the replacement of the RF sensor or firmware upgrade. While the RF sensor is out of service, the corresponding monitored E-DPAs and Channels are activated.

6. APPENDIX

6.1. DOCUMENTATION REFERENCE

Ref	Title	Source	Reference
[Ref. 01]	PUBLIC NOTICE Wireless Telecommunications Bureau and Office of Engineering and Technology Establish Procedure and Deadline for Filing Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s) Applications GN Docket No. 15-319	FCC	DA 15-1426 Released: December 16, 2015
[Ref. 02]	PUBLIC NOTICE WIRELESS TELECOMMUNICATIONS BUREAU AND OFFICE OF ENGINEERING AND TECHNOLOGY CONDITIONALLY APPROVE SEVEN SPECTRUM ACCESS SYSTEM ADMINISTRATORS FOR THE 3.5 GHZ BAND	FCC	DA 16-1426 Released: December 21, 2016
[Ref. 03]	PUBLIC NOTICE WIRELESS TELECOMMUNICATIONS BUREAU AND OFFICE OF ENGINEERING AND TECHNOLOGY ESTABLISH “SECOND WAVE” DEADLINE FOR PROPOSALS FROM PROSPECTIVE SPECTRUM ACCESS SYSTEM (SAS) ADMINISTRATOR(S) ANDENVIRONMENTAL SENSING CAPABILITY (ESC) OPERATOR(S) GN Docket No. 15-319	FCC	DA 17-339 Released: April 7, 2017
[Ref. 04]	Federal Communications Commission - FCC 15-47 REPORT AND ORDER AND SECOND FURTHER NOTICE OF PROPOSED RULEMAKING GN Docket No. 12-354	FCC	Released: April 21, 2015
[Ref. 05]	Federal Communications Commission - FCC 16-55 ORDER ON RECONSIDERATION AND SECOND REPORT AND ORDER GN Docket No. 12-354	FCC	Released: May 2, 2016
[Ref. 06]	Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS) - SAS Interface Technical Specification Document WINNF-16-S-0096	WInnF (WG3)	Release 1
[Ref. 07]	Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS) - Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification Document WINNF-16-S-0016	WInnF (WG3)	Release 1
[Ref. 08]	Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band Document WINNF-15-S-0112	WInnF (WG1)	Release 1
[Ref. 09]	CBRS Communications Security Technical Specification	WInnF	Release 1

	Document WINNF-15-S-0065	(WG2)	
[Ref. 10]	CBRS Operational Security Technical Specification Document WINNF-15-S-0071	WInnF (WG2)	Release 1
[Ref. 11]	WInnForum CBRS Certificate Policy Specification Document WINNF-17-S-0022	WInnF (WG5)	Release 1
[Ref. 12]	SPECTRUM SHARING COMMITTEE PROJECT ROADMAP	WInnF	April 4, 2017
[Ref. 13]	Proposal by RED Technologies for Spectrum Access System Administrator	RED	05/05/2017 (v1.0)
[Ref. 14]	NTIA Technical Memorandum 18-526 Distinction Between Radar Declaration and Pulse Burst Detection in 3.5 GHz Spectrum Sharing Systems	U.S. Department of Commerce	October 2017
[Ref. 15]	NTIA Technical Memorandum 18-527 Procedures for Laboratory Testing of Environmental Sensing Capability Sensor Devices	U.S. Department of Commerce	November 2017
[Ref. 16]	NTIA Technical Memorandum TM-18-534 Further Procedures for Laboratory Testing of Environmental Sensing Capability Sensor Devices	U.S. Department of Commerce	June 2018
[Ref. 17]	NTIA Letter to FCC on Commercial Operations in the 3550-3650 MHz Band Docket Number: GN Docket No. 12-354 Web site: https://www.ntia.doc.gov/fcc-filing/2015/ntia-letter-fcc-commercial-operations-3550-3650-mhz-band defining e-dpa.kml file	NTIA	April 14, 2015

Table 2: Documentation Reference

6.2. GLOSSARY

Terms	Description
3GPP	3rd Generation Partnership Project
AWS	Amazon Web Services
CA	Certificate Authority
CBSD	Citizens Broadband Radio Service Devices
CBRS	Citizens Broadband Radio Service
CFT	Call For Tender
CMMI	Capability Maturity Model Integration
CR	Cognitive Radio
CRAN	Cloud-RAN
DoD	Department of Defense
DP	Domain Proxy
EMS	Element Management System
ESC	Environmental Sensing Capability
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FSS	Commercial Fixed Satellite Service
GAA	General Authorized Access
GIS	Geographical Information System
GWBL	Grandfathered Wireless Broadband Licensee
IOT	Interoperability Testing
ITM	Irregular Terrain Model
ITS	Institute for Telecommunication Sciences
LAA	Licensed-Assisted Access
LSA	License-Shared Access
LSAlive©	RED Technologies License-Shared Access Product
LTE	Long Term Evolution
LTE-U	LTE Unlicensed
mmWave	millimeter Wave
MWC	Mobile World Congress
NTIA	National Telecommunications and Information Administration (regulator of U.S. federal government spectrum use)
OET	Office of Engineering and Technology
OOBE	Out Of Band Emission
PALs	Priority Access Licensees
RAN	Radio Access Network
REM	Radio Environment Map
RSS	Received Signal Strength
SAS	Spectrum Access System
SASlive©	RED Technologies Spectrum Access System Product
SDR	Software Defined Radio
SLA	Service Level Agreement
TT&C	Telemetry, Tracking, and Control
ULS	Universal Licensing System
WTB	Wireless Telecommunications Bureau
WInnF	Wireless Innovation Forum

Table 3: GlossaryPress Release

END OF DOCUMENT