

Spectrum Sharing Committee Policy and Procedure

SSC Abbreviations and Definitions

This policy lists abbreviations and definitions accumulated from the FCC rules and approved WinnForum specifications. The policy is a living guidance document is subject to change and update as WinnForum specifications change. Versions of the policy are public and provided for reference and convenience only.

1 Abbreviations

3GPP	3rd Generation Partnership Project [10]
ACLR	Adjacent Channel Leakage Ratio
AI	Air Interface [11]
AMSL	Above Mean Sea Level (based on [10])
CA	Certificate Authority [1, 4, 6]
CBRS	Citizens Broadband Radio Service [5]
CBSD	Citizens Broadband radio Service Device [10]
CBSD-ID	CBSD Identifier [10]
CFR	Code of Federal Regulations
CGI	CBSD Group Identifier [10]
CPAS	Coordinated Periodic Activities among SASs [2]
CP	Certification Policy [4]
CPI	Certified Professional Installer [1, 2]
CPIDI	Certified Profession Installer Device Information
CPIR-ID	Certified Professional Installer Registration Identification [1]
CPS	Certification Practice Statement [4]
CRA	Certificate Requesting Account [4]
CRL	Certificate Revocation List [4, 5]
CSR	Certification Signing Request [4]
DoD	U.S. Department of Defense [10]
DP	Domain Proxy [5, 10]
DPA	Dynamic Protection Area [2, 10]
DR	Demand Response [4]
DRAS	Demand Response Automation Server [4]
ECC	Elliptic Curve Cryptography [4, 5]
EIRP	Effective Isotropic Radiated Power [2]
EMS	Element Management System [5]
ESC	Environmental Sensing Capability [1, 5, 6, 11,10]
E-UTRA	Evolved Universal Terrestrial Radio Access [11]
EUD	End User Device [10]
FCC	Federal Communications Commission [10]
FFS	For Further Study [10]

FIPS	Federal Information Processing Standards [4]
FRN	FCC Registration Number [6], 7]
FSS	Fixed-Satellite Service [10]
GAA	General Authorized Access [10]
GWBL	Grandfathered Wireless Broadband Licensee [1, 2]
GWPZ	Grandfathered Wireless Protection Zone [2]
HAAT	Height Above Average Terrain [2, 3, 10]
HTTP	Hypertext Transfer Protocol [6]
HTTPS	Secure HTTP (e.g., with TLS) [6, 7]
IAP	Iterative Allocation Process [10]
ID	Identifier, Identity [6]
id-at	X.500 attribute types. (OID value: 2.5.4) [4]
id-ce	Object Identifier for Version 3 certificate extensions. (OID value: 2.5.29) [4]
ICG	Interference Coordination Group [3]
IETF	Internet Engineering Task Force [4]
IMG	Interference Margin Group [10]
IOT	Inter-Operability Test [2, 5]
ISO	Independent System Operators [4]
JSIR	Joint Spectrum Interference Resolution [10]
JSON	JavaScript Object Notation [6, 7]
MFCN	Mobile / Fixed Communication Networks
MFG	Manufacturer [4]
NOAA	National Oceanic and Atmospheric Administration [2]
NTIA	National Telecommunications and Information Administration [10]
OA&M	Operations, Administration and Maintenance
OCSP	Online Certificate Status Protocol [5]
OID	Object Identifier [4]
OpenSSRF	Open source Standard Spectrum Resource Format [10]
OR-ID	Owner Registration ID
PA	Policy Authority [4]
PA	Priority Access [10]
PAL	Priority Access License [10]
PAL-ID	Priority Access License Identifier [10]
PKCS	Public-Key Cryptography Standard [4]
PKI	Public Key Infrastructure [1, 4]
PPA	PAL Protection Area [10]
PPA-ID	PAL Protection Area Identifier [10]
RAN	Radio Access Network [2, 5]
RFC	Request for Comment [4]
RFP	Request for Proposal [1]
RSA	Rivest, Shamir, Adleman (cryptography algorithm) [4, 5]
SAS	Spectrum Access System [10]
SMLA	Secondary Market Leasing Agreement [10]

TLS	Transport Layer Security [2, 3, 6]
UR-ID	User Registration ID [10]
UR-ID	User Registration Identity [2]
URL	Universal Resource Locator [6]
UTC	Coordinated Universal Time [6]
UUT	Unit Under Test [2, 5]
WBS	Wireless Broadband Service (FCC Rules Part 90, Subpart Z) [10]
WInnForum™	The Wireless Innovation Forum [1]
WISP	Wireless Internet Service Provider based on [12]

2 Definitions

Accreditation Standard. The standard defining how a Training Program Administrator can be accredited to run a CPI Training Program. [1]

Accrediting Body. An entity that accredits a Training Program Administrator to offer a CPI Training Program based on the Accreditation Standard. As of the publication of this version of this standard, “Accrediting Body” refers to the Wireless Innovation Forum (WInnForum). [1]

Adjacent Channel Leakage Ratio. The Adjacent Channel Leakage Ratio (ACLR) is the ratio of the filtered mean power over the assigned Aggregated Channel Bandwidth to the filtered mean power over the equivalent adjacent channel bandwidth. The power in the assigned Aggregated Channel Bandwidth and its equivalent adjacent channel bandwidth are measured with rectangular filters with measurement bandwidths equal to the Aggregated Channel Bandwidth. [FCC 18-149]

Admin Test Harness: A collection of routines that can be configured by the test operator to inject data that is required for the purpose of the test cases, into the SAS UUT. The Admin Test Harness also has the ability to recognize the completion of CPAS executed by the SAS UUT. [2]

Aggregated Channel Bandwidth. The Aggregated Channel Bandwidth is the bandwidth of a single channel, or in the case of multiple contiguous channels, the bandwidth between the upper and lower limits of the combined contiguous channels. [FCC 18-149]

Audit Requirements Guide. A document that sets forth the security and audit requirements and practices for CAs. [4]

Baseline State: Baseline State refers to the state of SAS UUT after it is triggered to reset by the test operator of Admin Test Harness. [2]

Blacklist: A list of CBSDs that are to be denied service. [3]

BTS-CBSD: A base transceiver station CBSD that serves one or more points, which may be EUDs or CPE-CBSDs. [3]

Category A CBSD. A lower power CBSD that meets the general requirements applicable to all CBSDs and the specific requirements for Category A CBSDs set forth in sections 96.41 and 96.43. [FCC rules]

Category B CBSD. A higher power CBSD that meets the general requirements applicable to all CBSDs and the specific requirements for Category B CBSDs set forth in sections 96.41 and 96.45. [FCC rules]

CBRS band: The 3550-3700 MHz Citizens Broadband Radio Service band. [3,11]

CBRS-wide: Across the entire CBRS system including all CBRS entities (note: this is equivalent to system-wide). [10]

CBSD Antenna: The radiating element(s) of the CBSD. From the perspective of the SAS-CBSD interface, each CBSD has one CBSD Antenna. Note that the CBSD's antenna may be instantiated with multiple physical antennas (e.g., an antenna array for MIMO operation), but those antennas must be transmitting one aggregate waveform collectively from a single geolocation, and with a total transmit power that conforms to all the CBSD's registration parameters and authorized transmit power levels provided by the SAS in its active grants (e.g., maximum allowable EIRP). [2, 3]

CBSD Group Identifier (CGI): An identifier used to allow one or more registering CBSDs to identify as a group that the CBSD User for those CBSDs has established. [10]

CBSD-ID: The system-wide unique identifier for registered CBSDs. [10]

CBSD Registration: The process required to register a valid Citizens Broadband Radio Service Device (CBSD) with a SAS. [3]

CBSD Registration. The procedure by which a CBSD indicates to a SAS its intention to operate. Successful registration implies a validation by the SAS that the CBD has been FCC certified and confers on the CBSD the right to be authorized by the SAS to operate in accordance with a Grant. During the registration process, each CBSD provides a fixed location, unique identifiers (e.g., owner information, device information), *Group* membership, and radio-related capabilities. A successful registration procedure concludes with the SAS providing a unique identifier for that CBSD. [10]

CBSD Test Harness. A collection of routines that can be configured by the test operator to interact with the SAS UUT via interfaces specified in [n.9] and automates critical test sequences and procedures in this document and [n.14]. Via these interfaces and following the specified test procedures, the CBSD Test Harness emulates the SAS-CBSD Request Messages specified in [n.9] that would be generated by one CBSD, using a TLS connection with CBSD certificate to the SAS UUT. If multiple CBSD Test Harnesses are directly connected to the SAS UUT, each has its own TLS connection to the SAS UUT. The software without the CBSD certificate is stored in a public location. [2]

CBSD User: The registered entity that has operational responsibility for the CBSD. [10]

Certificate. A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Validity Period, contains a Certificate serial number, and is digitally signed by the CA that issued the certificate. [4]

Certificate Applicant. An individual or organization that requests the issuance of a Certificate by a CA. [4]

Certificate Application. A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate. [4]

Certificate Chain. An ordered list of Certificates containing a Subscriber Certificate and one or more CA Certificates, which terminates in a root Certificate. [4]

Certificate Policy (CP). The principal statement of policy governing the PKI. [4]

Certificate Signing Request (CSR). A message conveying a request to have a Certificate issued. [4]

Certificate Authority (CA). An entity authorized to issue, manage, revoke, and renew Certificates in the PKI. [4]

Certification Practice Statement (CPS). A statement of the practices that a CA employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates. [4]

Certificate Requesting Account (CRA). The online portal to assist Certificate Applicants in requesting Certifications. [4]

Certified Professional Installer (CPI): Any individual trained and currently validly certified from an accredited CPI Training Program based on the relevant Part 96 rules and associated technical best practices for the Citizens Broadband Radio Spectrum (CBRS). [10]

CPI Accreditation Standard: Standard defining how a CPI Training Program Administrator can be accredited to run a Certified Professional Installer (CPI) Training Program. The CPI Accreditation Standard includes a curriculum standard defining the requirements necessary for trainees to be certified as a Certified Professional Installer. The CPI Accreditation Standard includes a requirement for an objective certification test to be administered by a program administrator as part of the CPI Training Program. Passing this test is a prerequisite for an individual to be considered a Certified Professional Installer. [10]

CPI Accrediting Body: Entity that accredits a CPI Training Program Administrator to offer a CPI Training Program based on the CPI Accreditation Standard. This entity must be independent from CPI Training Program Administrators. [10]

CPI Device Information (CPIDI): The body of information required to be entered by a CPI to register a valid CBSD with a SAS for installation and to allow for spectrum grant requests and transmission pursuant to Part 96 rules, industry standards, or SAS-specific requests. [10]

CPI Training Program: A required training curriculum contained in a valid program, as defined by the CPI Accrediting body, for certification of a CPI. Such curriculum may have mandatory (such as Part 96 and rules-based requirements) and optional components (such as industry best practices or manufacturer or SAS specific training). [10]

CPI Training Program. Mandatory training/curriculum required by the CPI Training Program Administrator as a prerequisite for taking the objective certification test. [1]

CPI Training Program Administrator: Entity such as a network equipment operator that develops a Certified Professional Installer (CPI) Training Program, gains accreditation, administers the objective certification test and maintains certification records. [10]

CPI Training Program Administrator: Entity such as a Network Equipment Operator, an equipment vendor, a SAS operator, or a third-party training organization that develops a Certified Professional Installer (CPI) Training Program, gains accreditation, administers the objective certification test and maintains CPI records [1]

CPI Registration Identification (or ID) (CPIR-ID): The unique identifier provided by the CPI Accrediting Body through the CPI Training Program to CPIs who are validly and currently certified and registered as CPIs. [10]

Channel. The contiguous frequency range between lower and upper frequency limits. [3]

Citizens Broadband radio Service Device (CBSD). Fixed Stations, or networks of such stations, that operate on a Priority Access or General Authorized Access basis in the Citizens Broadband Radio Service consistent with Title 47 CFR Part 96. For CBSDs which 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. End User Devices are not considered CBSDs. [FCC rules]

Citizens Broadband radio Service Device (CBSD): Fixed Stations, or networks of such stations, that operate on a Priority Access or General Authorized Access basis in the Citizens Broadband Radio Service consistent with Title 47 CFR Part 96 [n.8]. For CBSDs which 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, 11]

Citizens Broadband radio Service Device (CBSD): Fixed Stations or Portable Base stations or access points, or networks of such base stations or access points, that operate on a Priority Access or General Authorized Access basis in the Citizens Broadband Radio Service consistent with this rule part. Does not include End User Devices. For manage networks, it is likely that information exchanges between CBSDs and the SAS would be aggregated through a domain proxy such as a network access manager. For the purpose of this Technical Report, the CBSD may also include such a domain proxy [i.1]. [9]

Cluster List: The set of CBSDs, identified by their CBSD-IDs, included in a PPA claim. The PAL Holder provides this Cluster List to the Managing SAS. These are the CBSDs that provide service and coverage within the claimed PPA. [10]

Coastline. The mean low water line along the coast of the United States drawn according to the principles, as recognized by the United States, of the Convention on the Territorial Sea and the Contiguous Zone, 15 U.S.T. 1606, and the 1982 United Nations Convention on the Law of the Sea, 21 I.L.M. 1261. [FCC rules]

Coexistence Group: A group of CBSDs that coordinate their own interference within the group according to a common interference management policy. [10]

Compliance Audit. A period audit that a CA system undergoes to determine its conformance with PKI requirements that apply to it. [4]

Compromise. A violation of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information has occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key. [4]

Control Objectives. Criteria that an entity SHALL meet in order to satisfy a Compliance Audit. [4]

Coordinated Periodic Activities among SAS's (CPAS). Periodic coordination among SASs, which in Release 1 operation is comprised of scheduled external database synchronization, Full Activity Dump Exchange, IAP, and DPA move list calculation. In Release I, these coordination activities happen daily among SASs. Note: "trigger CPAS" as used in this document differs from normal operation in the following three ways; in particular: (1) all activities will be completed as fast as possible; (2) FAD generation by the SAS UUT is omitted; (3) the SAS UUT will only pull from the external databases specified by the Admin Test Harness. [2]

County. Counties shall be defined using the United States Census Bureau's data reflecting county legal boundaries and names valid through January 1, 2017. [FCC 18-149]

CPE-CBSD: A fixed, stationary CBSD used as customer premise equipment, the served CBSD which is a client of the BTS-CBSD, which may operate at a higher power level than an EUD, and which transmits during the same time slots as an EUD. [3, 10, (WINNF-TS-0112-V1.6.0 Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band (pending approval by the FCC))]

CRL: Certificate Revocation List. A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the revoked Certificates' serial numbers, and the specific times and reasons for revocation. [4]

CRL: Certificate Revocation List Usage Agreement. An agreement setting forth the terms and conditions under which a CRL or the information in it can be used. [4]

Device Certificate. An end-entity non-CA certificate of the PKI chain installed in CBRS devices such as SAS Provider, Domain Proxy, Installer, PAL and CBSD devices. [4]

Digital Certificate Subscriber Agreement. An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Subscriber. [4]

Domain Proxy (DP): An entity engaging in communications with the SAS on behalf of multiple individual CBSDs or networks of CBSDs. The Domain Proxy can also provide a translational capability to interface legacy radio equipment in the 3650-3700 MHz band with a SAS to ensure compliance with Part 96 rules. [10]

Domain Proxy (DP): An entity engaging in network management and aggregate communications with the SAS on behalf of a multiple individual CBSD nodes or networks of such nodes. [9]

Domain Proxy (DP) Test Harness. A collection of routines that can be configured by the test operator to interact with the SAS UUT via interfaces specified in [n.9] and automates critical test sequences and procedures in this document and [n.14]. Via these interfaces and following the specified test procedures, the DP Test Harness emulates the SAS-CBSD Request Messages specified in [n.9] that would be generated by one or more CBSDs, using a TLS connection with DP certificate to the SAS UUT. If multiple DP Test Harnesses are connected to the SAS UUT, each has its own TLS connection to the SAS UUT. The DP function within the DP Test Harness merely aggregates the Request Messages of multiple single CBSDs and disaggregates the respective Response Messages of the SAS UUT and does nothing else (i.e., does not have any other unique functionality of a real Domain Proxy). The software without DP certificate is stored in a public location specified in [i.1]. [2]

Dynamic Protection Area (DPA): A predefined protection area which is activated or deactivated to protect a federal incumbent radar. An activated DPA must be protected from aggregate CBSD interference. A deactivated DPA is not protected from CBSD interference. [10]

Elliptic Curve Cryptography (ECC). A public-key cryptography system based on the algebraic structure of elliptic curves over finite fields. [4]

End User Device. A device authorized and controlled by an authorized CBSD. These devices may not be used as intermediate service links or to provide service over the frequencies listed in section 96.11 to other End User Devices or CBSDs. [FCC rules]

Environmental Sensing Capability (ESC). A system that detects and communicates the presence of a signal from an Incumbent User to an SAS to facilitate shared spectrum access consistent with sections 96.15 and 96.67. [FCC rules]

Environmental Sensing Capability (ESC) Test Harness: A collection of routines that can be configured by the test operator to interact with the SAS UUT in order to execute the ESC functionalities of the test cases described in this document. Via these interfaces and following the specified test procedures, the ESC Test Harness emulates the messages that would be sent from an ESC system to a SAS. The ESC Test Harness software is stored in a public location specified in [i.1]. [2]

Exclusion Zone. A geographic area wherein no CBSD shall operate. Exclusion Zones shall be enforced and maintained by the SAS. Exclusion Zones will be converted to Protection Zones following the approval and commercial deployment of an ESC and SAS consistent with this part. [FCC rules]

Exigent Audit/Investigation. An audit or investigation by where there is a reason to believe that an entity's failure to meet PKI Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the PKI posed by the entity has occurred. [4]

Fixed Station. A CBSD or End User Device that transmits and/or receives radio communication signals at a fixed location. Fixed Stations may be moved from time to time but Fixed CBSDs must turn off and re-register with the SAS prior to transmitting from a new location. [FCC rules]

General Authorized Access (GAA) User. An authorized user of one or more CBSDs operating on a General Authorized Access basis, consistent with section 96.33, et seq. [FCC rules]

Geo-Location Capability. The capability of a CBSD to register its geographic coordinates within the level of accuracy specified in section 96.39. The CBSD location is used by the SAS to determine frequency availability and maximum transmit power limits for CBSDs. [FCC rules]

Grandfathered Wireless Broadband Licensee. A licensee authorized to operate in the 3650-3700 MHz band consistent with section 90.1338. [FCC rules]

Grandfathered Wireless Protection Zone. A geographic area and frequency range in which Grandfathered Wireless Broadband Licensees will receive protection from Citizens Broadband Radio Service transmissions and defined using methodology determined by the Wireless Telecommunications Bureau and Office of Engineering and Technology. [FCC rules]

Grant. The authorization provided by a SAS to a CBSD, subject to a Heartbeat exchange, to transmit using specified operating parameters. *Grants* are identified by a unique *Grant* identifier. Once issued, a *Grant's* operating parameters are never changed; if new or modified operating parameters are required, then a new *Grant* must be obtained. The *Grant's* operating parameters are maximum EIRP and *Channel*. A *Grant* can be in different states as defined in section 7. [3]

Granted State: The "GRANTED" state refers to a spectrum Grant that has been allocated to a CBSD by the SAS. This Grant state does not allow radio transmission by the CBSD relative to the Grant. [3]

Group: A collection of *CBSDs* which are provided a special, common form of management by the SAS. The nature of the special management is dependent on *Group* type. [3]

Incumbent User. A federal entity authorized to operate on a primary basis in accordance with the table of frequency allocations, fixed satellite service operator, or Grandfathered Wireless Broadband Licensee authorized to operate on a primary basis on frequencies designated in section 96.11. [FCC rules]

Initial Certification. Initial Certification in this specification applies to Release 1; however, after Initial Certifications, each SAS administrator could have an alternate method that, when approved by the FCC, would be allowed. [10]

Intellectual Property Rights. Rights under one or more of the following: copyright, patent, trade secret, trademark, or any other intellectual property rights. [4]

Interference Coordination Group: A group of CBSDs that does not require intra-group, inter-CBSD interference coordination from the SAS. [3]

Key Generation Ceremony. A procedure whereby a CA's key pair is generated, its private key is backed up, and/or its public key is certified. [4]

Largest Allowable PPA Contour Method: The FCC-mandated contour calculation method that defines the largest allowable size of a PPA. This is based upon the Managing SAS calculated protection area of the CBSDs on the PPA's Cluster List, the CBSDs' largest allowable EIRPs, the CBSDs' antenna heights and antenna parameters, the RF propagation model, and a -96 dBm/10 MHz threshold. [10]

License Area: The geographic component of a PAL. A License Area consists of one county. [FCC 18-149]

Main Test Harness: A collection of routines that can be configured by the test operator to interact with the SAS UUT in order to execute the test cases. It includes the reference models, Admin Test Harness, SAS Test Harnesses, DP Test Harnesses, CBSD Test Harnesses, and all other test harnesses defined in this document. The Main Test Harness software is stored in a public location specified in [i.1]. [2]

Managing SAS: The SAS that administers a PAL and serves the CBSDs that form the Cluster List of a PPA registered to a PAL Holder that is authorized to use that PAL. The Managing SAS is the SAS which accepts, checks, and validates a PPA claim and which issues a PPA-ID for a valid PPA, and which shares the PPA-ID and the PPA vertex points with all SASs. Subsequently, the Managing SAS serves the CBSDs on the PPA Cluster List. The Managing SAS also serves CBSDs using GAA grants and their CBSD Users. [10]

Mobile Station: A device intended to be used while in motion or during halts at unspecified points. [FCC rules]

Non-Public Registration Data. CBSD registration data that would allow one to identify a licensee and must [shall] therefore be obfuscated pursuant to FCC Requirement 96.55(a)(3). [10]

OR-ID: Owner Registration ID. The system-wide unique identifier for Registered Owners. [Source: WINNF-15-S-0112-V1.0.3 CBRS Operational and Functional Requirements]

Owner / Registered Owner: The owner of one or more CBSD devices and/or the owner of one or more PAL licenses. All owners of CBSDs must be registered as owners, whether they use GAA or PAL spectrum. All owners of PAL licenses must be registered as owners, even if they have not deployed any CBSDs. All pre-registered eligible lessees must be registered as owners. All brokers or transferring agents who handle PAL rights or PPA claims must be registered as owners. [Source: WINNF-15-S-0112-V1.0.3 CBRS Operational and Functional Requirements]

PAL-ID: The system-wide unique identifier for a PAL. [10]

PAL database: The system-wide accessible database that allows the look-up of a PAL boundary and PAL ownership based upon the PAL-ID. [10]

PAL Holder: The entity who has legal rights to make PPA claims under the registered PAL. [10]

PAL Reserved Channel: A 10 MHz channel in the range of 3550-3650 that a SAS may establish for exclusive use of a set of one or more CBSDs that are registered as belonging to a PPA based upon acquired PAL rights. [3]

PAL Protection Area (PPA): The area of protected use of a channel or set of channels within an owned or leased PAL. The PPA is defined by a set of CBSDs (the Cluster List) and a boundary (a set of vertex points) that define the PPA within the PAL. All SAS are obligated to protect PPAs from interference. [Source: WINNF-15-S-0112-V1.0.3 CBRS Operational and Functional Requirements]

PAL Protection Area (PPA): An area within a PAL established by a PAL owner for protecting exclusive use of channels based upon the acquisition of PAL rights. The area is based upon the coverage area of the set of CBSDs that are members of the PPA. The SAS maintains a list of CBSDs that are members of the PPA. [2]

PAL Protection Area Identifier (PPA-ID): The system-wide unique identifier for a PPA. [10]

PAL Protection Area Information (PPA Information). PPA information includes PAL Database Record and PPA (as defined in [n.11]), which includes the cluster list, list of PAL-IDs, and the polygon describing the zone. When Admin Test Harness injects PPA information into SAS UUT, Admin Test Harness shall inject PAL Database Record first and then PPA Zone Definition Message. [2]

PAL Protection Area (PPA) database. The system-wide accessible database that allows the look-up of a PPA boundary and associated PAL information based upon the PPA-ID. [10]

PKCS #8: Public- Key Cryptography Standard #8. Public-Key Cryptography Standards #8 developed by RSA Security Inc., which defines a secure means for the transfer of private keys. [4]

PKCS #10: Public-Key Cryptography Standard #10. Public-Key Cryptography Standards #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request. [4]

PKI: Public Key Infrastructure. A system which organizations credentials vouched for by a hierarchical structure containing a Root of Trust (RoT). The Root of Trust signs credentials for trusted parties which authenticate their identities. Those parties may then sign credentials for another level of trusted parties. [9]

PKI: Public Key Infrastructure. The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. [4]

PKI: Public Key Infrastructure Participant. An individual or organization that is one or more of the following within the PKI: WinnForum, a CA, a Subscriber, or a Relying Party. [4]

Portable Station. A device designed to be used within 20 centimeters of the body of the user. [FCC rules]

Priority Access License (PAL). A license to operate on a Priority Access basis, consistent with section 96.23, et seq. [FCC rules]

Priority Access Licensee. A holder of one or more PALs. Priority Access Licensees shall be entitled to protection from General Authorized Access Users and other Priority Access Licensees within the defined temporal, geographic, and frequency limits of their PAL, consistent with the rules set forth in this part. [FCC rules]

Processing Center. A secure facility created by an appropriate organization (e.g., Symantec) that houses, among other things, the cryptographic modules used for the issuance of Certificates. [4]

Protection Zone. A geographic area wherein CBSDs may operate only with the permission of an approved SAS and ESC. [FCC rules]

Public Registration Data. Data that SAS Administrators must share with the public according to FCC requirement 96.55(a)(3). [10]

Reference Model. Reference Model refers to a calculation implement in the Main Test Harness. The Reference Model includes the calculation of the Propagation Models, Iterative Allocation Process (IAP), PPA creation, Antenna Gain Model (including antenna pattern), aggregate interference, and DPA Move List as specified in [12, 2]

Registered Owner Identifier (ROI): An identifier used to allow one or more registering CBSDs to identify its (their) Registered Owner and to allow the association to a specific grouping that the Registered Owner has established. This grouping may correspond to area, to a domain proxy or proxies, to a lessee, or some other useful group. [12]

Registration Conditional (REG-Conditional): A parameter in the *RegistrationRequest* object that may be provided by the CBSD or may be provided through other means. [3]

Relying Party. An individual or organization that acts in reliance on a certificate and/or a digital signature. [4]

RSA (Algorithm). A public key cryptographic system invented by Rivest, Shamir, and Adlman. [4]

Secret Share. A portion of the activation data needed to operate the private key, held by individuals called “Shareholders.” Some threshold number of Secret Shares (n) out of the total number of Secret Shares (m) shall be required to operate the private key. [4]

Secret Sharing. The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations. [4]

Security Repository. Database of relevant security information accessible on-line. [4]

Security Policy. The highest-level document describing security policies. [4]

Service Area. One or more contiguous License Areas held by the same Priority Access Licensee. [FCC rules]

SAS: Spectrum Access System. A system that authorizes and manages use of spectrum for the Citizens Broadband Radio Service in accordance with subpart F. [FCC rules, [11]

SAS: Spectrum Access System. A system that maintains records of all authorized services and CBSDs in the Citizens Broadband Radio Service frequency bands, is capable of determining the available channel at a specific geographic location, provides information on available channels to CBSDs that have been certified under the Commission's equipment authorization procedures, determines and enforces maximum power levels for CBSDs, and enforces protection criteria for Incumbent Users and Priority Access Licensees, and performs other functions as set forth in the Federal Communications Commission (FCC) rules. Spectrum Access Systems shall also refer to multiple Spectrum Access Systems operating in coordination and in accordance with Part 96 [i.1]. [9]

SAS: Spectrum Access System Administrator. An entity authorized by the Commission to operate an SAS in accordance with the rules and procedures set forth in section 96.63. [FCC rules]

SAS Essential Data: SAS-Essential Data are defined as data shared between any two SASs which are required to fulfill all SAS functions required by 47 C.F.R Part 96. [10]

SAS Under Test. A Spectrum Access Systems (SAS) to which the sequence of steps listed in the test specifications in this document is applied via the SAS, CBSD, and ESC Test Harnesses, the SAS Under Test exchanges sequences of simulated messages with simulated Spectrum Access Systems, simulated CBSDs, and simulated ESCs according to the test specifications in this document. In this document, it is referred to as SAS UUT (Unit Under Test). [2]

SAS Test Harness. A collection of routines that can be configured by the test operator to interact with the SAS UUT via interfaces specified in [n.11] and automates critical test sequences and procedures in this document and [n.14]. Via these interfaces and following the specified test procedures, the SAS Test Harness emulates the SAS-SAS Messages specified in [n.11] that would be generated by one SAS. The software without SAS certificate is stored in a public location specified in [i.1]. [2]

SAS Test Harness. A collection of routines that can be executed by the test operator, to interact with the CBSD or DP/CBSD UUT via interfaces specified in [n.5]. Test Harness emulates the message sequences that would be generated by a SAS and it is used to automate critical test sequences and procedures in this document. The SAS Test Harness software is stored in a public location specified in [i.1]. [5]

SMLA: Secondary Market Leasing Agreement. The leasing terms by which PAL rights are conveyed from a PAL licensee to an eligible lessee. [10]

Sub domain. The portion of the PKI under control of an entity and all entities subordinate to it within the hierarchy. [4]

Sub domain Participants. An individual or organization that is one or more of the following within the Subdomain: WInnForum, a Subscriber, or Relying Party. [4]

Subject. The holder of a private key corresponding to a public key. The term “Subject” can, in the case of a Device Certificate, refer to the Subscriber requesting the device certificate. [4]

Subscriber. The entity who requests one or more Certificates (e.g., a manufacturer) to be installed in one or more devices under its control. The Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate (s). [4]

Superior Entity. An entity above a certain entity within the PKI. [4]

Trusted Person. An employee, contractor, or consultant or an entity within the PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and /or its practices. [4]

Trusted Position. The positions within the MFGH entity that SHALL be held by a Trusted Person. [4]

Trustworthy System. Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. [4]

Unit Under Test. A CBSD or DP/CBSD(s) that is tested for compliance with WInnForum test specification. The SAS Test Harness is used to receive and send messages with the Unit Under Test (UUT) according to the test procedures contained in this document. The term “Unit Under Test” is applied generically within this document to include, where appropriate, either a CBSD or the combination of a domain Proxy and CBSD. [5]

User Registration ID (UR-ID). The system-wide unique identifier for Registered Users of the CBRS; these may be CBSD Users or PAL Holders. [10]

Validity Period. The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked. [4]

3 References

1. [Wireless Innovation Forum, Spectrum Sharing Committee, “Test and Certification for Citizens Broadband Radio Service \(CBRS\); Wireless Innovation Forum, Spectrum Sharing Committee, “CBRS Certified Professional Installer Accreditation Technical Specification.” WINNF-TS-0247 V1.1.0, January 2019.](#)
2. [Wireless Innovation Forum, Spectrum Sharing Committee, “Conformance and Performance Test Technical Specification; SAS as Unit Under Test \(UUT\).” WINNF-TS-0061 V1.4.0, December 2018.](#)

3. [Wireless Innovation Forum, Spectrum Sharing Committee, "Signaling Protocols and Procedures for Citizens Broadband Radio Service \(CBRS\): Spectrum Access Systems \(SAS\) – Citizens Broadband Radio Service Device \(CBSD\) Interface Technical Specification."](#) WINNF-TS-0016 V1.2.3, October 2018.
4. [Wireless Innovation Forum, Spectrum Sharing Committee, "WInnForum CBRS Certificate Policy Specification."](#) WINNF-TS-0022 V1.1.2, February 2018.
5. [Wireless Innovation Forum, Spectrum Sharing Committee, "Test and Certification for Citizens Broadband Radio Service \(CBR\); Conformance and Performance Test Technical Specification; CBSD/DP as Unit Under Test \(UUT\)."](#) WINNF-TS-0122 V1.0.1, September 2018.
6. [Wireless Innovation Forum, Spectrum Sharing Committee, "Signaling Protocols and Procedures for Citizens Broadband Radio Service \(CBRS\): Spectrum Access Systems \(SAS\) – SAS Interface Technical Specification."](#) WINNF-TS-0096 V1.3.0, April 2018.
7. [Wireless Innovation Forum, Spectrum Sharing Committee, "Operations for Citizens Broadband Radio Service \(CBRS\): Priority Access License \(PAL\) Database Technical Specification."](#) WINNF-TS-0245 V1.0.0 (Formerly WINNF-16-S-0245-V1.0.0), July 2017.
8. [Wireless Innovation Forum, Spectrum Sharing Committee, "CBRS Operational Security."](#) WINNF-TS-0071 V1.0.0 (Formerly WINNF-15-S-0071-V1.0.0), July 2017.
9. [Wireless Innovation Forum, Spectrum Sharing Committee, "CBRS Communications Security Technical Specification."](#) WINNF-TS-0065 V1.1.0 (Formerly WINNF-15-S-0065-V2.0.0), July 2017.
10. [Wireless Innovation Forum, Spectrum Sharing Committee, "Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band."](#) (WINNF-TS-0112-V1.6.0), October 2018.
11. [Wireless Innovation Forum, Spectrum Sharing Committee, "Signaling Protocols and Procedure for Citizens Broadband Radio Service \(CBRS\): WInnForum Recognized CBRS Air Interfaces and Measurements."](#) WINNF-SSC-0002 V4.0.0, November 2018.
12. [Wireless Innovation Forum, Spectrum Sharing Committee, "Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band."](#) (WINNF-TS-0112 V1.0.0 (Formerly WINNF-15-S-0112-V1.0.0), July 2017.