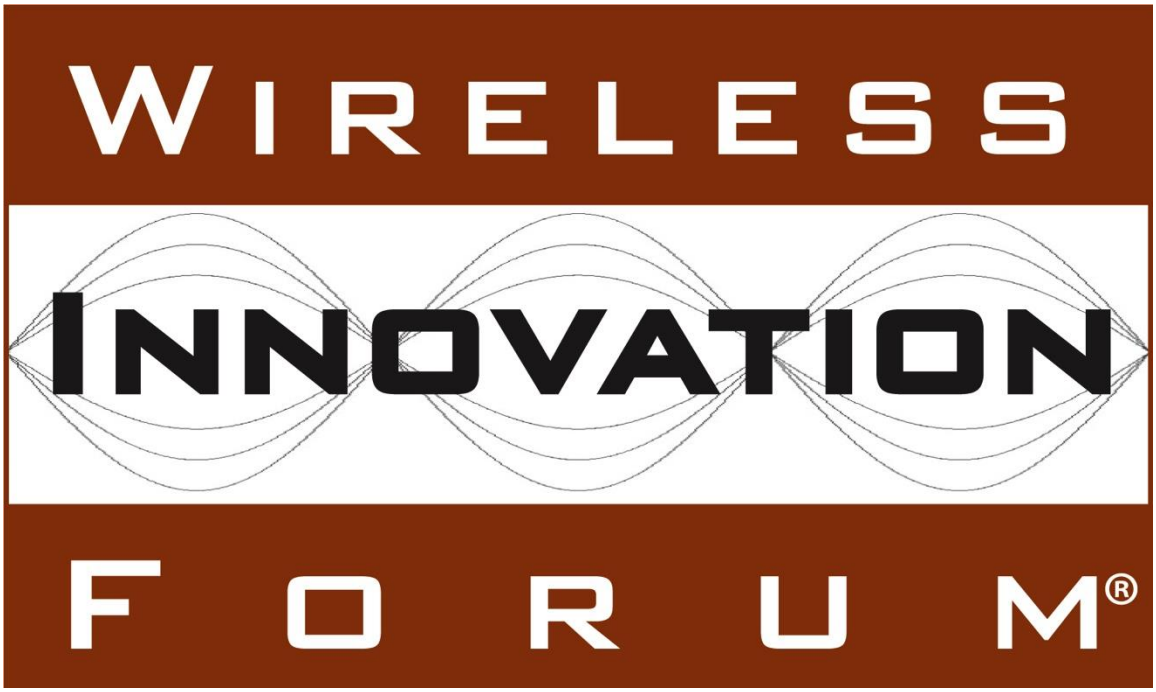

CBRS Communications Security Technical Specification

Document WINNF-15-S-0065

Version V1.0.0
2 August 2016

TERMS, CONDITIONS & NOTICES

This document has been prepared by the SSC Work Group 2 to assist The Software Defined Radio Forum Inc. (or its successors or assigns, hereafter "the Forum"). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the SSC Work Group 2.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter's copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum's participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

This document was developed following the Forum's policy on restricted or controlled information (Policy 009) to ensure that that the document can be shared openly with other member organizations around the world. Additional Information on this policy can be found here: http://www.wirelessinnovation.org/page/Policies_and_Procedures

Although this document contains no restricted or controlled information, the specific implementation of concepts contain herein may be controlled under the laws of the country of origin for that implementation. Readers are encouraged, therefore, to consult with a cognizant authority prior to any further development.

Wireless Innovation Forum ™ and SDR Forum ™ are trademarks of the Software Defined Radio Forum Inc.

Table of Contents

CBRS Communications Security Technical Report

1 Introduction

2 Scope

This document is a Technical Report on the communications security policies governing Spectrum Access System (SAS) and Citizens Broadband Radio Service Device (CBSD) communications interfaces. These policies describe a Public Key Infrastructure (PKI) which governs communications within the Citizens Broadband Radio Service (CBRS) ecosystem and provides authentication and authorization for messages exchanged within the SAS ecosystem as part of the protocols described in the SAS-CBSD Technical Report and the SAS-SAS Technical Report.

All requirements in this document are at the R2 level (requirements imposed by Wireless Innovation Forum as a means of addressing FCC requirements and other R2 requirements [n.4]).

3 References

3.1 Normative references

The following referenced documents are necessary for the application of the present document.

[n.1] “Public-key and attribute certificate frameworks”, ITU-T Recommendation X.509.

[n.2] “The Transport Layer Security (TLS) Protocol Version 1.2”, Internet Engineering Task Force Network Working Group, Aug 2008.

[n.3] “Security Requirements for Cryptographic Modules”, National Institute of Standards and Technology Information Technology Laboratory, May 25, 2001.

[n.4] “Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band”, WINNF-15-S-0112, Oct 2015.

[n.5] “Trust Service Principles and Criteria for Certification Authorities Version 2.0” March 2011, webtrust.org (http://www.webtrust.org/homepage-documents/item54279.pdf)

3.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] “Report and Order and Second Further Notice of Proposed Rulemaking”, GN Docket No. 12-354, FCC 15-47, Released: April 21, 2015

[i.2] “Interim SAS to CBSD Protocol Technical Report TR-A”, Wireless Innovation Forum Spectrum Sharing Committee Work Group 3.

4 Definitions and abbreviations

Citizens Broadband Radio Service Device (CBSD): Fixed 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 managed 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]

Spectrum Access System (SAS): 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 channels 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 System shall also refer to multiple Spectrum Access Systems operating in coordination and in accordance with Part 96. [i.1]

Public Key Infrastructure (PKI): A system which organizes 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.

Domain Proxy: 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. [i.1]

5 CBRS Public Key Infrastructure Organization

The goal of this section is to provide a high-level overview of the PKI governing SAS and CBSD communications. It discusses the PKI actors, including a relatively low number of SAS operators and domain proxy operators as well as the extension of the trust boundary to CBSD manufacturers and CBSDs.

5.1 Actors

The SAS ecosystem will be occupied by actors at different levels of bandwidth and interconnection. The densely-interconnected part of the network will be comprised of SAS operators (which are designed to be densely interconnected peer-to-peer), and domain proxy operators (both roles are expected to be large centrally managed services with addressable IP locations and with reliable high-bandwidth Internet connections).

In addition, the ecosystem will be occupied by specific devices which, when communicating directly with the SAS and not under the control of a centrally-managed domain proxy, shall be able to provide authentication credentials which verify their status as CBSDs certified to be extended emission authorizations by the SAS.

5.1.1 CBRS Root Of Trust CA ("Root CA")

The CBRS Root of Trust CAs ("CBRS Root CA") are the sets of public/private key pairs which serve as the trust anchors for all digital certificate chains in the CBRS ecosystem. The role of CBRS Root CAs is to formalize the qualifications of intermediate role CAs to issue end-entity certificates through a certificate signature. This allows entities within the PKI ecosystem to maintain a small and consistent trust list of trust roots. This is especially important for standalone CBSDs.

5.1.1.1 Designation process for root CAs

The WInnForum shall develop a process for the designation of CBRS Root CA administrators.

CBRS Root CA key material shall be generated and maintained in a controlled manner – that is, by organizations to be designated by a process developed by WInnForum and which are capable of securely generating keys under audited conditions, storing them on secure hardware, operating them to sign subCAs as needed, and importantly to ensure that the key custody can be transferred in a manner that is certified against WInnForum guidelines.

The process by which the WInnForum will designate CBRS Root CAs shall honor principles of technology diversity, key diversity, and supplier diversity, while taking measures intended to reduce the risk of key material loss and to enable orderly maintenance of Root of Trust key material through management transitions in the set of custodians of that key material.

The process will be an open process with objective selection criteria. The criteria may be selective insofar as they test for commitment to operate a long-term trust root, demonstrated experience in operating such a trust root, capability for secure offline key storage, viability of the enterprise in offering long-term trust root operation, and commitment to follow the detailed WInnForum guidelines governing the operation of the CA structure. The process will not be selective with a goal of eliminating qualified applicants in order simply to reduce the number of trust roots.

The designation process may allow for modifications to the trust list. The criteria for such modifications (including additions and deletions) shall be defined by the WInnForum guidelines governing the operation of the CA structure. The designation process may incorporate requirements for key escrowing capabilities and corresponding contract terms on the part of root CA operators in order to minimize the probability of such an event occurring, and shall provide documentation for update procedures and notifications to ecosystem participants to provide the proper notice of any change of this magnitude.

The Root CA designation process shall be either handled by WInnForum staff or delegated to an independent entity which will apply the selection criteria. The process shall provide for ongoing procedures for overseeing and publishing the trust list in a secure manner and for transfer of such oversight responsibility to any successor entity.

All CBRS Root CA operators shall generate and maintain their keys under auditable conditions and follow all operating procedures required by the "WebTrust Principles and Criteria for Certification Authorities 2.0". [n.5] A CBRS Root CA operator shall sign a CA for any subCA as specified in the operational specification to be produced by WInnForum and agreed to by designated Root CA operators.

Any CA provider may serve multiple CA administrator roles (Root CA, subCA, etc) concurrently provided that for each role the CA adheres to the WInnForum defined verification/validation requirements associated with that role.

The WInnForum shall establish minimal standards as to the key algorithm and key sizes for the CBRS Root CA keys and criteria for signing intermediate CA certificates consistent with this document. These choices for other CAs within the hierarchy can be changed and adjusted with more ease at a later time and as prevailing recommendations require. CBRS Root CA certificates, however, will need to be generated before any other certificates are created, and will go on to be used as trust anchors by all actors within the CBRS system.

5.1.2 SAS Providers

A SAS provider is an entity which performs centralized aggregate interference protections for the entities in the ecosystem which merit such protection (principally incumbent and priority access receivers). The trust responsibilities of a SAS provider are to accurately perform this interference protection and to provide correct emission authorizations and notifications of such authorizations to its peers.

5.1.3 SAS-CA

The SAS Provider CA (SAS-CA) is an intermediate CA which serves as the issuing subCA for end-entity certificates used by SAS providers. All standardized SAS provider TLS interfaces including CBSD to SAS, Domain Proxy to SAS, and SAS to SAS shall require authentication via certificates issued by a SAS CA. SAS CAs shall generate and maintain their keys under auditable conditions and follow all operating procedures required by the WebTrust Principles and Criteria for Certification Authorities 2.0 [n.5]

5.1.4 Domain Proxy Operators

A domain proxy operator is an entity managing a system which controls various CBSDs. Those CBSDs do not communicate directly with the SAS, but are controlled by a system which communicates with the SAS on their behalf.

The trust responsibility of a domain proxy operator is to provide positive control of the CBSDs it manages to provide assurance that they are compliant with the emission authorizations issued by the SAS to which the domain proxy communicates.

CBSDs used by domain proxy operators do not need to have any specific trust relationship with the CBRS PKI. The operator has a responsibility to provide assurance that the equipment they operate has the operational characteristics (location, antenna direction, peak operating power, etc) claimed for it. Thus the operator of a domain proxy is within the trust boundary for the operation of equipment under its control.

5.1.5 Domain Proxy CA

A Domain Proxy CA is an intermediate CA which serves as the issuing subCA for end-entity certificates used by Domain Proxy Operators. All Domain Proxy to SAS communication shall require authentication via certificates issued by a Domain Proxy CA. Domain Proxy CAs shall generate and maintain their keys under auditable conditions and follow all operating procedures required by the WebTrust Principles and Criteria for Certification Authorities 2.0 [n.5]

5.1.6 Professional Installers

Category B CBSDs and some Category A CBSDs require professional installation and configuration. After passing an accredited professional training program, a professional installer would be authorized by the training program to receive a CBRS PKI signed digital certificate. The certificates would be individualized to each professional installer to ensure both authentication and non-repudiation. Professional installers would use their certificates when interacting with either SAS and/or a Domain proxies to attest to various CBSD installation and configuration parameters.

For example, a network operator may rely on a "professional installer" which uses such a credential to provide CBSD metadata to a SAS operator including the fact that the directional high-gain antenna is pointing at an azimuth of 90 degrees (east). The installer credential is within the trust boundary of the PKI, and so that installer is responsible and accountable for the accuracy of that information. SAS Operators shall authenticate various CBSD operating parameters via digital signatures from professional installers.

5.1.7 Professional Installer CA

A Professional Installer CA is an intermediate CA which serves as the issuing subCA for end-entity certificates used by Professional Installers. Professional Installer certificates will be used to cryptographically sign various CBSD operating parameters to be verified by SAS providers. Professional Installer CAs shall generate and maintain their keys under auditable conditions and follow all operating procedures required by the WebTrust Principles and Criteria for Certification Authorities 2.0 [n.5]

5.1.8 CBSD Manufacturers

In addition to the high-bandwidth connections between SAS and domain proxy operators, the ecosystem will extend to encompass a class of devices which are not large, centrally-managed systems. These individual CBSDs will use a trust boundary implanted by the manufacturer. There may potentially be orders of magnitude more such devices than there are SAS and domain proxy operators.

The trust delegation of these CBSDs is to their manufacturers. A manufacturer must provide such a device with firmware which acts like a ”mini-Domain Proxy" and controls the electrical and physical characteristics of the CBSD to remain within the emission authorizations given it by the SAS and the corresponding FCC rules.

The CBSD's access to its credential shall be designed to provide assurance that the CBSD is operating with the certified software system with which it was designed. For example, storage of private key material, and any needed boot assurance required for certification, may be done in many different ways, so long as industry best practices are followed. Possible implementations may use a Trusted Platform Module, a Secure Element, an ARM TrustZone, or other similar technology.

A CBSD manufacturer is an entity which creates and distributes the hardware which must be provided authorization by a SAS to transmit. As such, the manufacturer has the trust responsibility to provide each CBSD with the proper hardware and software so that it will only respond to proper emission authorizations issued by the SAS. The responsibilities of the manufacturer also includes the correct provisioning of key material into each CBSD such that it can be uniquely identified.

The piece of software within a CBSD which communicates with the SAS can be viewed as a "mini-Domain-Proxy". Thus the responsibility of the manufacturer is similar to that of the Domain Proxy operator: it shall provide assurance that the data reported by the CBSD to the SAS is accurate, and that controls issued to that "mini-Domain-Proxy" are faithfully executed by the hardware it is controlling (albeit in this case, that hardware is the same unit running the software).

A good example of this is key provisioning for Digital Rights Management (DRM) systems such as in the cable industry in set-top boxes.

5.1.9 CBSD Manufacturer CA

A CBSD Manufacturer CA is an intermediate CA which serves as the issuing subCA for end-entity certificates used by CBSD Manufacturers. CBSD Manufacturer certificates will be used to cryptographically sign various CBSD manufacturing time parameters to be verified by SAS providers. CBSD Manufacturer CAs shall generate and maintain their keys under auditable conditions and follow all operating procedures required by the WebTrust Principles and Criteria for Certification Authorities 2.0 [n.5]

5.2 PKI Structure

Visualized as a signature tree, the long-lived certificates in the PKI are organized similarly to this:

CBRS Root CA (Root of trust)

- SAS Provider CA
  - SAS provider A
  - SAS provider B
- Domain Proxy CA
  - Domain Proxy A
  - Domain Proxy B
- Professional Installer CA
  - Professional Installer A
  - Professional Installer B
- PAL CA
  - PAL Cert A
  - PAL Cert B
- CBSD Manufacturer CA
  - CBSD manufacturer A
  - CBSD manufacturer B

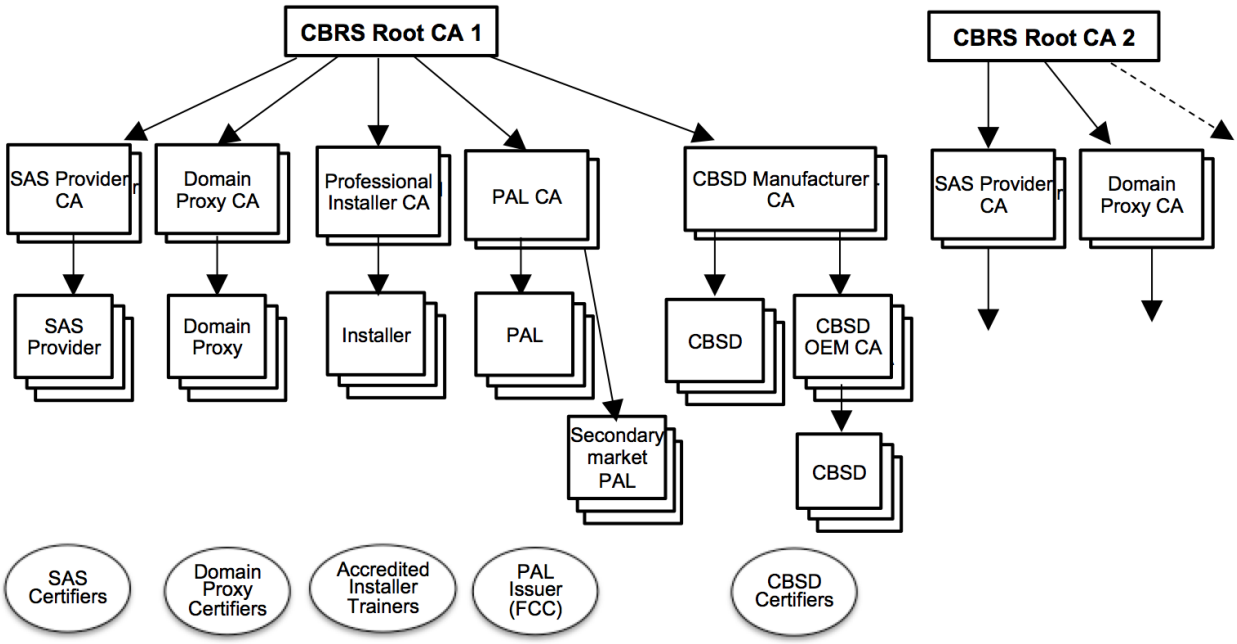

Figure 1: PKI Structure

Each branch in the CBRS PKI chain is signed by the certificate above it in the tree. A particular leaf certificate (e.g. "SAS provider B") has an X.509 certificate with chain entries for each of its parent nodes in the tree.

For example, this certificate would have a chain consisting of "SAS provider B" *signed by* "SAS provider CA" *signed by* "CBRS Root CA".

Once the X.509 certificate has been exchanged, the fingerprint of the certificate can be used to identify its authentication state. As such, a higher-level certificate shall not be used to sign a lower-level certificate which has already been signed by another higher-level certificate.

To put it another way, each certificate should belong to exactly one branch in the signature tree. Certificates used for different roles (e.g. a SAS and domain proxy being implemented by the same piece of software) should be kept separate. Certificates identify an actor and a role, not just an actor.

5.3 CBRS Certificate Attributes

Certificates used in the CBRS PKI shall follow the web PKI structure in these details:

Issuer: This data element should be formatted identically to the way web PKI structures the "Issuer" element: as a record reflecting the identity of the CA. These fields are present:

C	Country	X520countryName
ST	State	X520StateOrProvinceName
L	City	X520LocalityName
O	Organizational name	X520OrganizationName
OU	Organizational Unit name	X520OrganizationalUnitName
CN	Domain name	X520CommonName

Subject: This data element carries the same format as the "Issuer" element, and the same fields. It represents the identity of the subject to whom the certificate is issued.

Issuing subCAs signing certificates shall ensure that the C, ST, L, and O fields (if present) reflect the identity and legitimate location of signed certificates.

5.3.1 X.509 extensions which have the same meanings as in the web PKI:

Web PKI certificates contain several other X.509 data elements which correspond to capabilities or attributes of the certificate.

- Version
- Serial Number
- Algorithm ID
- Validity
  - Not Before
  - Not After

- Subject Public Key Info
  - Public Key Algorithm
  - Subject Public Key
- Issuer Unique Identifier (optional)
- Subject Unique Identifier (optional)
- Any extensions with defined meanings in the web PKI (optional)

When these X.509 data elements (and any other common certificate metadata which may added in subsequent versions of Transport Layer Security (TLS)) are present, they have the same meaning as they do in the web PKI.

Basic Constraints:

CA:TRUE should be set for the root certificates and any intermediates
CA:FALSE should be set for all leaf certificates
Path Length Constraint=0 should be set for issuing subCAs (manufacturer subCA excepted)
Path Length Constraint=None should be set for all leaf certificates

This need not be a critical (required) extension.

X509v3 Certificate Policies:

If present, this policy should refer to a number managed under the Wireless Innovation Forum IANA Private Enterprise Number (to be applied for if it does not already exist), and which refers to particular specifications of certificate policies.

X509v3 Key Usage:

If present, this data element contains information on the use of the certificate.

X509v3 Subject Key Identifier:

If present, this data element contains the hash of the key for the subject of the certificate.

X509v3 Authority Key Identifier:

If present, this data element contains the hash of the key for the CBRS-CA issuing key.

X509v3 Subject Alternative Name:

If present, this data element contains the domain name (DNS name) corresponding to the Subject Common Name of the certificate. This extension may also contain permanent identifier descriptors as in RFC 4043.

X509v3 Extended Key Usage:

If present, this data element contains information on the use of the certificate.

Key Sizes and Digest Algorithms:

Certificates must meet the following requirements for algorithm type and key size:

Root CA Certificates

Digest algorithm	SHA-384 or SHA-512
Minimum RSA modulus bits	4096
ECC curve	NIST P-384 or P-521

Intermediate CA Certificates

Digest algorithm	SHA-384 or SHA-512
Minimum RSA modulus bits	4096
ECC curve	NIST P-384 or P-521

End-Entity Certificates

Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus bits	2048
ECC curve	NIST P-256, P-384 or P-521

5.3.2 SAS 1.3.6.1.4.1.46609.1.x extensions:

In addition to the above web PKI standard extensions, SAS entities can make use of an additional extension. This extension is rooted in a Private Enterprise Number from IANA granted to the Wireless Innovation Forum, which will look like this:

1.3.6.1.4.1.46609.1.x

These sections are custom SAS extensions within the X509 extension system. They will be defined as strings comprised of string field names and values.

(46609 is the Wireless Innovation Forum Private Enterprise Number. See http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers)

Fields:

ROLE 1.3.6.1.4.1.46609.1.1	The role of the subject in the SAS ecosystem. Can take values of: SAS INSTALLER

	CBSD OPERATOR (Domain Proxy Operator) PAL CA (note: enumeration may be extended to include PAL licenses) (note: enumeration may be extended to include ESC) Each role will carry particular capabilities to engage in various kinds of communication. For instance, the INSTALLER role will be able to supply CBSD installation metadata to SAS. The SAS role will be authorized to engage in SAS-SAS and SAS-CBSD communications.
ZONE 1.3.6.1.4.1.46609.1.2	For a PAL role certificate, this field ordinarily contains the name of the PAL zone. (It may also contain a more structured definition of the outline of a PAL zone.)
FREQUENCY 1.3.6.1.4.1.46609.1.3	For a PAL role certificate, this field contains some metadata to describe the PAL license, in MHz, separated by a dash character. (Multiple ranges may be specified in comma-separated format.)
TEST 1.3.6.1.4.1.46609.1.999	For any role certificate, this field contains “TRUE” if the certificate is a test-mode certificate which may not authorize emission outside a testing context. The field will not be present in live production certificates.

This attribute should be a string formatted in a familiar X.509 style using colon separated KEY:VALUE pairs. Examples:

“ROLE:CBSD”

“FREQUENCY:3660-3670,3710-3720”

Note: a CBSD role certificate needs enough information to uniquely identify the CBSD without the opportunity for masquerade. There may be CA:TRUE CBSD certificates issued to

manufacturers or trusted operators and which they then use to sign (and possibly field-provision) individual CBSD certificates.

Fields are only applicable for particular role types. Certificate role type and applicable fields:

Role	Applicable Fields
ROLE:SAS	*none*
ROLE:OPERATOR	*none*
ROLE:INSTALLER	*none*
ROLE:CBSD	FCC ID CBSD ID SERIAL CATEGORY
ROLE:PAL	ZONE FREQUENCY HEIGHT STARTDATETIME

Certificate requests with inapplicable fields shall be rejected by the CA and denied by CBRS parties as malformed.

5.4 Operation of the CBRS PKI Certificate Signing

5.4.1 CBRS Root of Trust operation

The operation of CBRS Root CAs shall be performed by entities as designated by the WInnForum. Oversight of all CBRS Root CAs shall be done by the WInnForum or its designated agent on a regular basis. CBRS Root CAs shall make it possible for the keys to be made available for the orderly transition of key custody.

In order to be honored as a CBRS Root CA, an entity shall satisfy procedural requirements related to the verification of actors within the ecosystem and be designated by the Forum. Upon this designation, the CBRS Root CA will produce a root of trust certificate according to WInnForum guidelines which shall then be honored by all CBRS ecosystem participants. CBRS Root key material shall be created using redundant sets of technology and key pairs; designated key pairs shall be selected for use in the signing of certificates by designated entities. WInnForum guidelines shall specify the key lengths, diversity, and technologies to be used by root key material (e.g. 2xRSA 4096bit and 2xECC 384bit).

There may be more than one root of trust at any particular time, but it is expected that for revoked roots of trust, the outstanding certificates issued under that trust root will be confined to a known set, and that such certificates can be re-issued under the new trust root over time. CBRS Root key material shall be secured by entities maintaining such material in

a secure offline environment as specified in detailed agreements regarding such maintenance.

A CBRS Root CA will be used to sign intermediate CA certificates as authorized and requested by the WInnForum.

5.4.2 SubCA and Intermediate CA operation

In order to operate as a subCA or an Intermediate CA in the CBRS ecosystem, an entity shall demonstrate compliance with verification procedures in advance of certificate issuance which conform to the guidelines set by the WInnForum in addition to those required by Webtrust 2.0 audit standards. Such procedures for the CA involve verifying the identity of the entity requesting the certificate along with audit reports demonstrating active Webtrust 2.0 compliance.

For SAS Provider certificates, the SAS CA shall be able to verify that the certificate being issued is for a SAS Provider which is certified by the FCC. Proper documentation of this certification should be presented to the SAS CA by the applicant, and then verified. The SAS CA shall verify all metadata in the certificate. For the organization and domain data, the authority shall verify that the metadata provided by the applicant matches that at which the SAS Provider is operating (for example, that the CN domain name for URIs exposed by the system, and that the O= organization name corresponds to the SAS name advertised by the system).

For Domain Proxy certificates, a similar level of verification is required to that of the CBSD certificates. The Domain Proxy CA shall be able to verify that the entity requesting the certificate is a valid domain proxy operator given Part 96 for domain Proxies and the domain proxy meets WInnForum specified certification requirements. These verification procedures are subject to change as the requirements for domain proxy certification become clearer.

For CBSD certificates, the CBSD Manufacturer CA shall be able to verify that the certificate being issued is for a CBSD which has successfully passed certification tests by the FCC. Such documentation necessary for verification will be presented by the applicant. The CBSD Manufacturer CA shall verify the metadata in the certificate application. The CBSD Manufacturer CA may have processes to do direct signing of per-device certificates on behalf of a CBSD manufacturer. Alternatively, CBSD manufacturers may comply with all operating procedures required by the “WebTrust Principles and Criteria for Certification Authorities 2.0” [n.5], and act as an Intermediate CA to directly issue leaf certificates to individual CBSDs.

For Professional Installer certificates, the Professional Installer CA shall be able to verify that the applicant has successfully completed an authorized training program. Such training programs will be administered by any number of accredited providers. The providers of such an accredited course, upon successful completion by an applicant, will provide to the

Professional Installer CA the required documentation of completion. The Professional Installer CA shall also verify that the course has a current accreditation status with the WInnForum or another group which is responsible for the oversight of such training courses. The Professional Installer CA shall verify that the requested lifetime of the certificate request falls within any accreditation period limits and re-training requirements of the professional installer program. Alternatively, installer accreditation program providers may comply with all operating procedures required by the "WebTrust Principles and Criteria for Certification Authorities 2.0" [n.5], and act as an Intermediate CA to directly issue leaf certificates to professional installers.

CERT TYPE	SAS	CBSD	Domain Proxy	INSTALLER
Bearer	SAS administrators	Individual CBSDs	Domain proxy operators	Individual professional installers
Usage	Verifying machine-to-machine identity in communications with other SASs, CBSDs, domain proxies, and installers	Verifying machine-to-machine identity in communications with SASs,	Verifying machine-to-machine identity in communications with SAS	Presented to SAS when entering CBSD installation metadata
Verification requirements for issuance	Certification by the FCC	Certification by the FCC	TBD	Certification by an accredited program
Number of certificates	Small	Large	Small-Medium	Medium
Lifetime	~15 months	10 years	~15 months	~27 months

Table 5.1 Classes of SAS Ecosystem PKI Certificates

In all these cases, the authority shall verify that the applicant presents a unique name, and that an existing certificate for the same applicant name has not already been granted. If it has, the authority shall either deny the new applicant, or, if they appropriately represent the entity with the claimed name, issue a revocation for the existing certificate and then issue another. There may be a waiting period enforced while the revocation is propagated throughout the SAS ecosystem.

For CBSD OEM CA certificates (each valid for a specific FCC ID), the same applicant may have many CBSDs with simultaneously valid certificates. The CBSD Manufacturer CA shall verify that a duplicate FCC_ID intermediate signing certificate is not issued without revoking the existing certificate. Since CBSD OEM CA certificates are used as intermediates, replacement should only happen in the case of loss of control of the key material.

Any information signed into a certificate must be verified as accurate at the time it is issued. As an example, within Web PKI, this is done by validating domain names using public DNS and company information using public third-party databases (ex: D&B, Hoovers, local government databases).

Validation of actor metadata in the CBRS system must be defined before certificate issuance, and in the case of the high-volume issuance roles (CBSDs, installers) – preferably automated.

Actor metadata validation shall be performed by the CA performing the issuance of certificates (be those intermediate CAs certificates or end-entity (leaf) certificates.

The following is an example of actor metadata verification prior to issuance of Professional Installer Certificates

The definition of an ‘accredited’ professional installer, once fully defined, will likely require the completion of a training scheme and possible examination. The entity performing the accreditation (training and testing) of the installers shall be the party responsible (and authorized) for requesting the issuance of an installer certificate to that specific installer by a Professional Installer CA.

A Professional Installer CA extends interfaces to the accreditation entity allowing them to request and manage (renew, revoke) certificates for installers they certify.

All CBRS keys will have lengths of at least 2048 for RSA and 224 for ECC. These minimum length requirements will grow over time.

6 Transport Security Protocol

To protect the exchange of authorization information and communications between SAS and CBSDs, Transport Layer Security (TLS), a protocol created to provide authentication, confidentiality, and data integrity between two communicating applications, will be used in conjunction with the CBRS Public Key Infrastructure (PKI). The following sections will discuss the TLS requirements for SAS and CBSDs.

6.1 TLS Requirements for SAS

6.1.1 TLS Version Support

At a minimum TLS version 1.2 is required in SAS TLS implementations to mitigate different attacks on earlier versions. In addition, SAS should be configured to support TLS version 1.3 when that standard is finalized. SAS shall not support TLS versions 1.1, 1.0, or SSL version 3.0 or any other earlier versions of these standards.

6.1.2 Ciphersuites Support

The SAS shall be configured to only use cipher suites that are composed entirely of approved algorithms within FIPS 140-2 and NSA Suite B publications.

Here is a list of the ciphersuites which shall be supported by SAS implementations:

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

It is expected that this subset of ciphersuites will change overtime with new additions and deletions.

The SAS shall be configured to only support ciphersuites for which it has a valid certificate containing a signature providing at least 112 bits of security.

6.2 TLS requirements for CBSDs

This section provides a set of TLS requirements that a CBSD shall meet in order to adhere to these guidelines.

An individual CBSD not under the control of a domain proxy may communicate directly with the SAS to receive emission authorization. The trust responsibility of an individual CBSD is built into it by the manufacturer.

6.2.1 TLS Version Support

All CBSDs shall be configured to support TLS 1.2, and should additionally be configured to support TLS 1.3 when that standard is finalized. CBSDs shall not support any earlier TLS or SSL version.

6.2.2 Ciphersuites Support

The required cipher suites for CBSDs are the same as those for SAS listed above in section 6.1.2.

Due to long-lived deployment of CBSDs it may be difficult to enforce strong deprecations of supported ciphersuites, but it should be possible within the framework to establish limited use of deprecated ciphersuites to certificates with issued-date characteristics, so that communications using newer certificates would have to use new ciphersuites.

The certificate chain of a CBSD communicating directly with a SAS should be an X.509 chain starting with the particular unique CBSD certificate, including a model-specific certificate, a manufacturer-specific certificate, and ending with a CBRS-CA CBSD root, any CBRS-CA working key, and a CBRS-CA root of trust.

6.3 Certificate Exchange

Participants in the CBRS PKI will validate each other's identity at the establishment of a TLS session between them using the standard TLS certificate exchange mechanism (including the possible use of session reestablishment optimization techniques).

7 Securing Key Material Within the CBSD

The responsibility of the SAS to only provide service to properly certified CBSDs requires it to verify the PKI certificate presented by a CBSD when communicating with the SAS. The corresponding key material within the CBSD must be secured in order to provide assurance that the presentation of this certificate is evidence that the CBSD is operating as certified.

When any portion of the physical instantiation of a CBSD is accessible to unauthorized persons, and it is possible that tampering with that portion of the CBSD could result in the execution of unauthorized code or in the alteration of the physical operation of the CBSD, the following requirements apply:

- The CBSD shall take measures according to reasonable industry best practices to ensure resistance to tampering (to a reasonable extent), and such that physical modifications that could result in altered operation of the CBSD by unauthorized persons should result in the CBSD terminating operation and, when possible (e.g., its communication interfaces are not damaged), the CBSD should report the tampering to an appropriate management CBSD or the SAS or both.

- The CBSD shall take measures according to reasonable industry best practices to establish reasonable industry best practices, based on a secure trusted execution environment, along with a chain of trust from the trusted execution environment through the bootstrap,firmware loading, and software loading operations, to ensure that any firmware and software that are executed in any parts of its physically-accessible instantiation are authenticated (prior to execution) by a properly certified organization (e.g., confirm, in a secure trusted execution environment, a signature of the firmware/software files according to a public key stored in a secure memory, or equivalently strong method accepted by industry best practices).

- The CBSD shall incorporate mechanisms to ensure that PKI key materials are not obtainable or usable for communications with the SAS unless the chain of trust from the trusted execution environment through the loaded and executed firmware and/or software has been established.

- The CBSD shall take measures according to reasonable industry best practices to ensure that downloading or upgrading procedures for any firmware and software that are executed in any parts of its physically-accessible instantiation are authenticated (prior to installation on the CBSD and execution) by a properly certified organization (e.g., confirm, in a secure execution environment, a signature of the firmware/software files

according to a public key stored in a secure memory, or equivalently strong method accepted by industry best practices).

When a CBSD is physically instantiated across multiple physical CBSDs, and communication protocols and procedures between those separate physical entities that implement any portion of the CBSD entity's behavior shall use reasonable industry best practices to ensure privacy, integrity, and authentication for those communications exchanges.

Any entities that are responsible for generating PKI (or similar) signed firmware or software execution images that are essential to the CBSD secure install, boot, and operation requirements shall follow best industry practices to ensure the secure storage, access, management, destruction, and ownership of all root or derived key materials for the lifetime of the CBSD. Such entities shall ensure that any access to key materials to generate signed executable code images can only be performed by certified and authorized individuals, according to certified guidelines for key material management. If transfer of ownership of, or changes in the access to, such key material occur within the reasonable lifetime expectancy of the CBSD, the responsible entities shall ensure that any new parties with access to this material will conform to these requirements. Detailed guidelines for specifying and certifying such key material owning entities shall be prepared by an authorized certification organization.

When the CBSD entity is subordinate to a Domain Proxy, the Domain Proxy [operator] is responsible for ensuring that all physical and logical hardware, firmware, and software components that comprise the CBSD functionality satisfy the previous requirements in this section on securing key material if those components are physically accessible to untrained/uncertified persons.

8 Participant Blacklisting

Due to the physical limitations of CBSD firmware, CBSD certificates will have long-lifetimes. Correspondingly, the SAS providers and/or the SAS-CA should maintain a blacklist of entities which are known to be compromised. This will also facilitate the tracking of CBSDs found to be defective for other reasons beyond leakage of key material (examples: a defective antenna or transmitter, or partially-compromised firmware which has ceased behaving according to the standard communications protocols).

Such a blacklist is very much like a certificate revocation list. Some method shall be used to communicate and exchange revoked and blacklisted certificates among system participants. CRLs (and optionally OCSP) shall be used by domain proxy operators to exchange such information, and by CBSDs if they communicate directly with a SAS to verify the certificates of SASs. SASs may use CRLs (and optionally OCSP) or other means to exchange such information. All actors in the system must check the chosen form of revocation no less frequently than weekly.

8.1 SAS management of credential blacklist

It is expected that certificate holders that have short-lifetime certificates will rotate their certificates on a short-term basis to keep their long-term keys off-line in higher security storage, and to mitigate any damage caused by a leaked key. Since the response of an organization to a key material leak will be revocation accompanied by a key rotation, it is not expected that the OCSP service will have anything significant to add in the way of security enhancement for counter-party communications. That is, mitigating a discovered breach will be simultaneously notified and fixed.

The SAS providers shall maintain and share with each other blacklists of certificates which are known to be compromised or otherwise rendered untrustworthy. The presence of specific CBSD certificates, or certificates issued by any party in the PKI on this blacklist, indicates that no SAS provider should permit requests from a party presenting that credential to succeed.

In the event of device compromise, a CBSD must be re-provisioned with a new identity represented by new key material to mitigate possible loss of private key material. A domain proxy or SAS provider on the blacklist should re-provision a key from the CBRS CA to fix whatever key leakage compromised it. An operator should re-issue any trusted installer keys to fix the key leakage.

This blacklist is maintained as a cooperative effort by SAS providers. As such, they may choose to use a CRL-like blacklist exchange, build the exchange of such records into the SAS-SAS exchange protocol, or use an OCSP-like solution for managing that information. The requirement is that a SAS shall check a reasonably up-to-date (no more than 1 week old) blacklist as part of the authentication of any incoming request from any counterparty.

9 Security Procedures and Best Practices

There will be many procedures necessary to maintain the integrity of the CBRS CA PKI. The goal of this section of the document is not to recapitulate the best practices for CA management, or to provide an exhaustive list of such procedures, but most to point out those processes which are critical to maintaining the trust boundary of the system such that participants have a checklist to make sure they have accounted for their various duties to that trust boundary.

9.1 All Participants

- Standardize, manage, and update application protocols and ciphersuites supported
- Standardize and update namespace(s) used and the requirements and conventions around the naming from section 6.4

9.2 CBRS Certificate Authorities (signers of other certificates, including intermediates)

- CA key material management - generation, backup, distribution, destruction, rotation (new CAs)

- Handling cert enrollment requests and cert issuance from downstream CAs, SAS providers, domain proxy operators, and original equipment manufacturers (OEMs)
- Handling revocation requests and revocation data generation from SAS, domain proxy, OEM CAs and from SAS and domain proxy and OEM parties
- Disaster recovery
- Audit logs of all operations
- Provide support for audits performed by a party to be designated by the industry group
- Comply with and maintain independent audits of all operating procedures required by the "WebTrust Principles and Criteria for Certification Authorities 2.0" [n.5]

9.3 SAS Providers

- Key material management - generation, backup, distribution, destruction, rotation (including the addition of new CAs)
- Request enrollment or revocation with SAS-CA
- Handle enrollment requests and cert issuance from SAS services, domain proxy services, trusted installers
- Revocation requests and revocation data generation (blacklist, CRLs)
- Disaster recovery of SAS and domain proxy credentials
- Audit logs of all operations
- Provide support for audits performed by a party to be designated by the industry group

9.4 Domain Proxy and SAS services

- Key management for services - generation, backup, destruction, rotation
- Request enrollment or revocation with SAS, domain proxy, or OEMs
- Manage trust stores
- Manage revocation blacklists published by SAS, domain proxy, and OEMs

9.5 CBSD OEMs

- Key material management - CBSD key generation and cert installation on secure element
- Audit logs and support audits performed by a party to be designated by the industry group
- CA functions assuming that they are managing a PKI

9.6 Network Operators

- Field service a CBSD to change key material after a key breach

9.7 Professional Installer Programs

- Maintain correct procedures for accreditation of professional installers and validation of their credentials to certificate-issuing bodies

10 History

Document history		
V 0.3.0	July 24th 2015	Skeleton of Technical Report based on WINNF-15-I-0031
V 0.3.1	Sep 28, 2015	Add section on certificate attributes and SAS-CA from WINNF-15-I-0078
V 0.3.2	Oct 22, 2015	Add more detail on certificate extension formatting
V 0.3.3	Dec 4, 2015	Consistency and language edits. Fine tune extension content definitions.
V 0.3.4	Jan 26, 2016	Added contributions from CA technical experts on PKI structure
V 0.3.5	May 6, 2016	Consistency fixes, re-organize root CA discussion into authorization and operation pieces. Defer discussion of root authorization to further work, eliminate Operating CA from hierarchy.
V 0.3.6	June 16, 2016	Finalize edits to PKI structure, firmware security, and CRL sections.