Wireless Innovation Forum Contribution

All blanks ([…]) must be completed for this Submission to be given consideration. In making this submission, the Submitters agree that they are bound by the Policies and Procedures of the Software Defined Radio Forum Inc. doing Business as the Wireless Innovation Forum ("The Forum"), including but not limited to the Intellectual Property Rights Policy (Policy 007) and the Restricted and Controlled Information Policy (009).

Committee: SSC WG5 CBRS Operations
Title: Adding CBRS Root Certificates to SAS, CBSD and Domain Proxy
Short Title: Adding CBRS Root Certificates
Source: By /s/:
Idan Raz
Airspan Networks

Date: [5 January 2021]
Distribution: [Unrestricted, Members, Committee, Post on website, etc.]

Document Summary: Guideline to adding CBRS Root Certificates to the "Trusted Root CA Certificate Store" ("trust anchor stores") of SAS, CBSD and Domain Proxy

Notes of Importance: [Optional. Short statement; please limit to 50 words or less.]

Impacts/Effects: [Optional. Short statement; please limit to 50 words or less.]

Action Desired: [Optional]
Action Required for Closure: [Optional]
Desired Disposition Date: [Day Month Year]

1. Additional Copyright License

In addition to the rights and licenses granted by the undersigned pursuant to Section 4 of the IPR Policy, the undersigned hereby agrees as follows: if this Code Contribution is included in whole or in part in the Specification or Other Work Product of the Committee named above, the undersigned hereby grants the Forum and its members a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the undersigned's copyrights in its Code Contribution right to sublicense the right to implementers or users, as appropriate, of such Code Contribution to copy, modify, and redistribute such Code Contribution or included portion thereof. THIS CODE CONTRIBUTION IS PROVIDED TO THE FORUM BY THE UNDERSIGNED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED. IN NO EVENT SHALL THE UNDERSIGNED BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS CODE CONTRIBUTION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

2. Future Code Contributions (initial if appropriate)

___ The rights and licenses granted above apply to this and all future Code Contributions made by the undersigned relating to this Specification or Other Work Product.

IN WITNESS WHEREOF, the Code Contributor has executed this Contribution Agreement through its duly authorized Representative.

Member: _____

By:_____

Name:_____

Title:_____

Date:_____

Adding CBRS Root Certificates to SAS, CBSD and Domain Proxy

Version V1.0
5 January 2021

Adding CBRS Root Certificates to SAS, CBSD and Domain Proxy

The SAS<->CBSD protocol is utilizing TLS with a 2-way authentication method. For this purpose, X.509 certificate exchange occurs during the TLS connection establishment between the SAS and CBSD/DP.

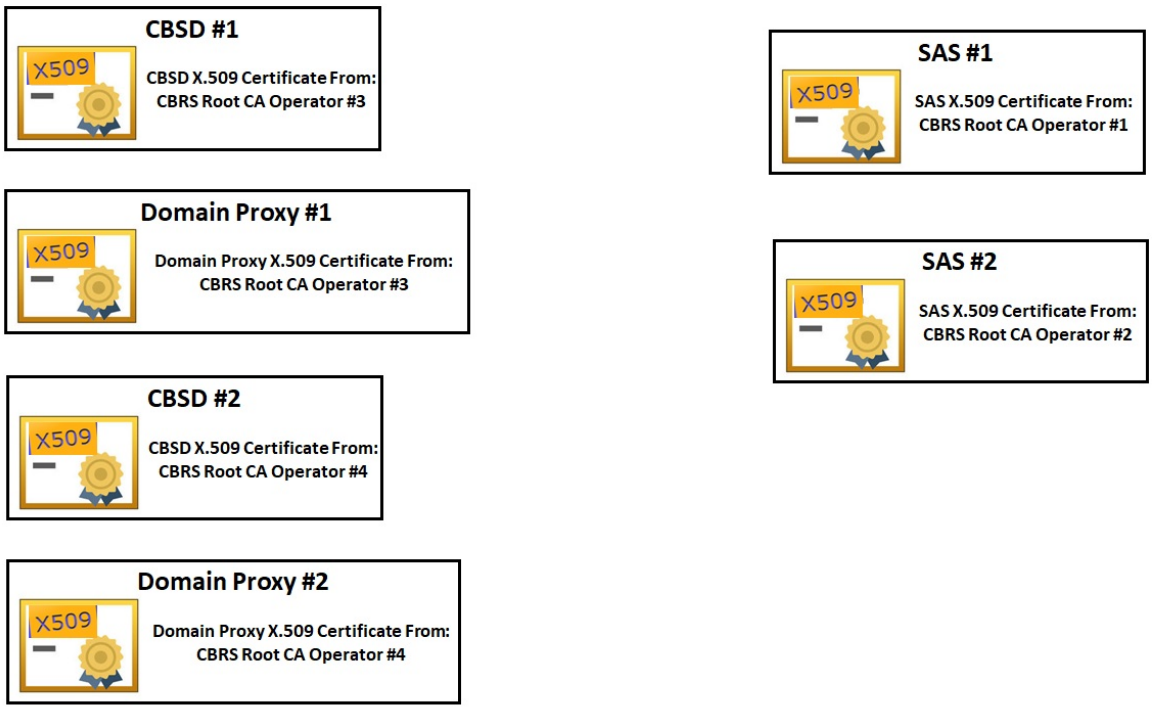
The CBSD/DP verifies the PKI chain of the SAS X.509 certificate sent to CBSD/DP during the TLS connection establishment. The SAS verifies the PKI chain of the CBSD/DP X.509 certificate sent to SAS during the TLS connection establishment. The CBSD, Domain Proxy and SAS have a "Trusted Root CA Certificate Store" where the CBRS X.509 Root certificates are stored.

When communication to the SAS is done directly from CBSD without Domain Proxy, then the CBSD has in its "Trusted Root CA Certificate Store" the CBRS X.509 Root certificates.

When communication to the SAS is done via Domain Proxy, then the Domain Proxy has in its "Trusted Root CA Certificate Store" the CBRS X.509 Root certificates (the CBSD in this case does not have CBRS X.509 certificates).

In order for SAS to verify the PKI chain of the CBSD/DP X.509 certificate, the SAS must have in its "Trusted Root CA Certificate Store" the Root CA of the CBSD/DP X.509 certificate. In order for CBSD/DP to verify the PKI chain of the SAS X.509 certificate, the CBSD/DP must have in its "Trusted Root CA Certificate Store" the Root CA of the SAS X.509 certificate.

The CBRS Root CA certificates are Public X.509 certificates and can be transferred publicly (via e-mail, download from web server, etc.) The CBRS Root CA certificates have a public link from WInnForum for download: (https://cbrs.wirelessinnovation.org/cbrs-root-ca-operators), Because there are several CBRS Root CA Operators, then the SAS and CBSD/DP can choose different CBRS Root CA Operators (based on business considerations) to issue their CBRS X.509 certificates. The following example illustrates this:



The following combinations apply from this example:
For CBSD #1 and SAS #1 to successfully establish a TLS connection:

- SAS #1 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #3"
- CBSD #1 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #1"

For Domain Proxy #1 and SAS #1 to successfully establish a TLS connection:

- SAS #1 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #3"
- Domain Proxy #1 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #1"

For CBSD #1 and SAS #2 to successfully establish a TLS connection:

- SAS #2 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #3"
- CBSD #1 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #2"

For Domain Proxy #1 and SAS #2 to successfully establish a TLS connection:

- SAS #2 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #3"
- Domain Proxy #1 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #2"

For CBSD #2 and SAS #1 to successfully establish a TLS connection:

- SAS #1 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #4"
- CBSD #2 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #1"

For Domain Proxy #2 and SAS #1 to successfully establish a TLS connection:

- SAS #1 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #4"
- Domain Proxy #2 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #1"

For CBSD #2 and SAS #2 to successfully establish a TLS connection:

- SAS #2 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #4"
- CBSD #2 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #2"

For Domain Proxy #2 and SAS #2 to successfully establish a TLS connection:

- SAS #2 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #4"
- Domain Proxy #2 requires in its "Trusted Root CA Certificate Store" the "CBRS Root CA #2"

The above combinations lead to the following statement in section 1.3 of TS-0022 to maintain proper operation of the CBRS Ecosystem:
"Subscribers should install all WInnForum authorized CBRS Root CA certificates in their device trust anchor stores to validate received certificates."

By installing all the CBRS Root CA certificates in the "Trusted Root CA Certificate Store" ("trust anchor stores"), the CBRS Ecosystem can maintain commercial business without restricting to specific devices:

- SAS can establish TLS communication with any CBSD/DP.
- CBSD/DP can establish TLS communication with any SAS.

In the example above:

- If SAS #1 does not have "CBRS Root CA #4" in its "Trusted Root CA Certificate Store", then it cannot establish TLS connection with CBSD #2 and Domain Proxy #2 (and hence cannot have business with them).

- If CBSD #1 does not have “CBRS Root CA #2” in its “Trusted Root CA Certificate Store”, then it cannot establish TLS connection with SAS #2 (and hence cannot have business with SAS #2).

Adding a new CBRS Root CA to the “Trusted Root CA Certificate Store”:
In the CBRS Ecosystem, the following may occur:

- CBSD manufacturing process did NOT load to the CBSD “Trusted Root CA Certificate Store” with all the CBRS Root CA that exist at the time the CBSD is manufactured.
- A NEW CBRS Root CA Operator is joining the CBRS Ecosystem.

In order to allow the business flexibility in the CBRS Ecosystem of TLS connection between the various CBSD/DP and SAS, then the vendors need to have a way in their products to allow uploading additional CBRS Root CA(s) into the “Trusted Root CA Certificate Store”.
For CBSD and Domain Proxy, uploading additional CBRS Root CAs into their “Trusted Root CA Certificate Store” is typically available via the CBSD/DP Management System (or webGUI) remotely managing the device. For CBSD/DP it may also be applicable by a software upgrade where the new CBRS Root CA is embedded as part of the software (CBRS Root CA is a Public X.509 certificate).

SAS, CBSD and Domain Proxy vendors are not mandated to add a new CBRS Root CA if their existing business is satisfactory with the existing CBRS Root CA certificate(s) in their “Trusted Root CA Certificate Store”. In order to allow flexibility in their business of the CBRS Ecosystem it is recommended that SAS, CBSD and Domain Proxy vendors will be aware of new CBRS Root CA(s) joining the CBRS Ecosystem. This will allow the proper upload of the new CBRS Root CA(s) to the “Trusted Root CA Certificate Store” based on each vendor’s implementation. This way the SAS, CBSD and Domain Proxy can be up to date and will have all CBRS Root CA certificates.