

Interim SAS to SAS Protocol Technical Report-A

Historical Document WINNF-15-H-0051

Version V1.0.0
3 January 2017

TERMS, CONDITIONS & NOTICES

This document has been prepared by Working Group 3 of the Spectrum Sharing Committee 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 It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the Spectrum Sharing Committee.

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

Table of Contents

TERMS, CONDITIONS & NOTICES	i
Contributors	iii
1 Introduction	1
2 References	1
3 Definitions and Abbreviations	1
4 Architecture Model and SAS to SAS Protocol Requirements	2
5 Peer SAS Discovery	3
6 SAS to SAS Security	3
7 SAS to SAS Information Exchange Elements	4
7.1 SAS-SAS Exchange Entities and Names	4
7.2 SAS Administrator Exchange Record	6
7.3 ESC Administrator Exchange Record	7
7.4 SAS Implementation Exchange Record	7
7.5 ESC Implementation Exchange Record	8
7.6 Domain Proxy Exchange Record	8
7.7 CBSD Device Type Exchange Record	8
7.8 CBSD Exchange Record	9
7.9 Incumbent Exchange Record	9
7.10 Zone Exchange Record	10
7.11 CBSD Operator Exchange Record	10
7.12 Professional Installer Exchange Record	10
7.13 Coordination Event Exchange Record	11
8 SAS-SAS Exchange Mechanisms	11
8.1 Providing Metadata-Only in Respond to Time-Range Requests	14
8.2 Time Basis for Time-Range Requests	14
8.3 Wildcard Time-Range Requests	14
8.4 Providing Activity Dump Metadata	15

Contributors

The following individuals made significant contributions to this document:

Editors: James Ni (Federated Wireless), Greg Billock (Google)

Other Member Representatives:

- Alcatel-Lucent: Milind Buddhikot
- AT&T: Neeti Tandon
- Ericsson: Kumar Balachandran, Mark Racek
- Federated Wireless: Masoud Olfat
- Google: Greg Billock
- Key Bridge Global: Jesse Caulfield
- Motorola Solutions: David Gurney
- Nokia Networks: Anatoly Andrianov, Al Hirsbrunner, Steve Magee, Prakash Moorut
- Qualcomm: Doug Knisely
- Verizon: Max Solondz, Naseem Khan

Observers:

- NIST: Anirudha Sahoo

SAS to SAS Exchange Protocol

1 Introduction

This document is a Technical Report describing the protocol by which Spectrum Access Systems (SAS) exchange information as required by the FCC Report and Order 15-47 in order to facilitate access to the band by Citizen's Broadband Radio Service Devices (CBSDs) connected to other SASs.

SAS Administrator policies regarding coordination of operations of CBSDs by SAS, to provide a stable radio frequency environment for Priority Access Layer (PAL) licensees, and other functions required for orderly spectrum administration and the fulfillment by the SAS of the responsibilities given it under Part 96 are not discussed in this interim report.

2 References

- [1] "SAS Functional Architecture," Working Document WINNF-15-P-0047, Version V0.3.6, 12 June 2015.
- [2] "Report and Order and Second Further Notice of Proposed Rulemaking," FCC, FCC 15-47, April 17, 2015.
- [3] "CBRS Communications Security Technical Report," Wireless Innovation Forum WINNF-15-P-0065 (In Development).
- [4] "The application/json Media Type for JavaScript Object Notation (JSON)" RFC 4627.

3 Definitions and Abbreviations

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 this rule part. 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. [2]

Spectrum Access System (SAS): A system that authorizes and manages use of spectrum for the Citizens Broadband Radio Service in accordance with subpart F in [2].

4 Architecture Model and SAS to SAS Protocol Requirements

Figure 1 reproduces the notional SAS system architecture as agreed by the Spectrum Sharing Committee for use by all working groups.

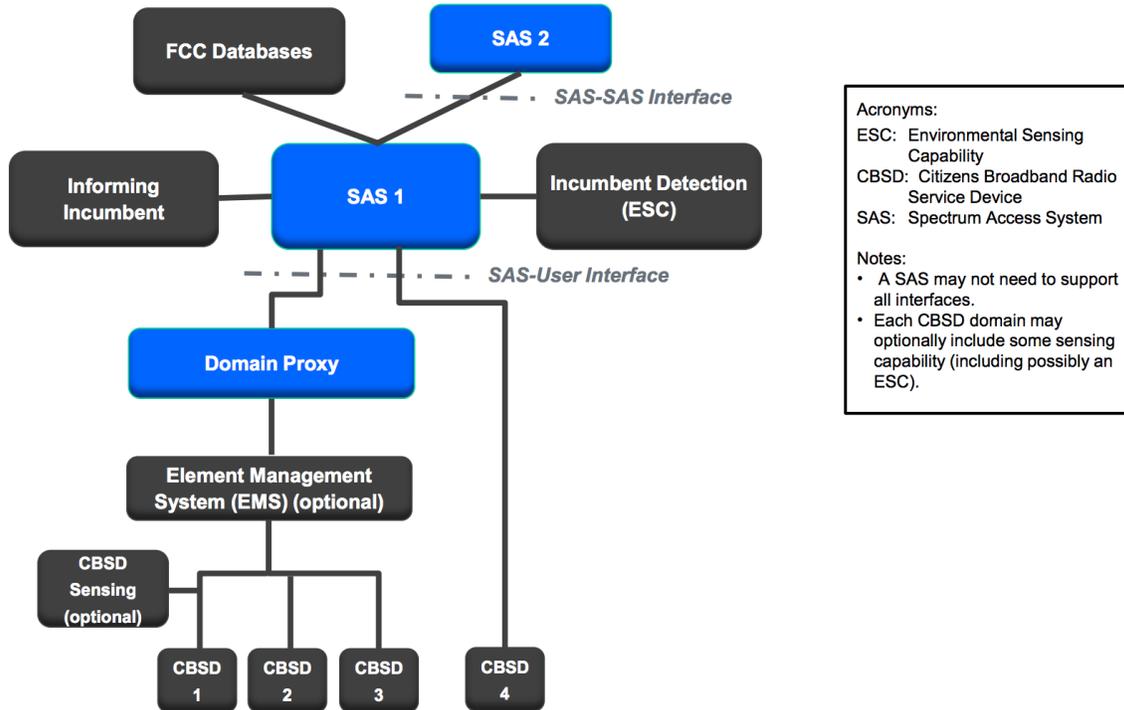


Figure 1. SAS Notional Architecture

The SAS to SAS interface defines the methods and protocols that govern the communication, coordination and information exchange between two SAS implementations. The requirements on these interfaces are set forth in the Part 96 rules in section 96.55, 96.61, and 96.63. They include these relevant requirements:

- Cooperate to develop a standardized process for coordinating operations with other SASs, avoiding any conflicting assignments, maximizing shared use of available frequencies, ensuring continuity of service to all registered CBSDs, and providing the data collected pursuant to section 96.55. [[2]: 96.63(h)]
- Coordinate with other SAS Administrators including, to the extent possible, sharing information, facilitating non-interfering use by CBSDs connected to other SASs, maximizing available General Authorized Access (GAA) frequencies by assigning Priority Access Licenses (PALs) to similar channels in the same geographic regions, and other functions necessary to ensure that available spectrum is used efficiently consistent with this part. [[2]: 96.63(i)]

- Communications between CBSDs and an SAS, between an ESC and an SAS, between individual CBSDs, and between different SASs, must be secure to prevent corruption or unauthorized interception of data. An SAS must be protected from unauthorized data input or alteration of stored data. [[2]: 96.61(b)]
- SAS Administrators must make all information necessary to effectively coordinate operations between and among CBSDs available to other SAS Administrators. [[2]: 96.55(a)(2)]

This Technical Report adopts the approach of specifying information exchange items which satisfy these requirements by virtue of being capable of providing a complete representation of all Part 96 information collected by the SAS with other SASs. There is some such information which in practice may not be exchanged between two particular SASs. But since two SASs may wish to exchange such information for value-added services even if it is not required to be exchanged, the protocol includes exchange definitions for such information items. Due to the variety of circumstances in which these records are exchanged, all fields are optional except the ID (which is the primary key for the record).

5 Peer SAS Discovery

The discovery of SAS peers is out of scope of the SAS-SAS protocol, and will be accomplished in proprietary ways by individual SAS administrators. However, such discovery will be facilitated by records stored within the SAS itself related to its SAS peers, and retrievable via the SAS-SAS protocol. Thus a new peer need only discover a subset of currently operating SASs to then retrieve information about all operating SASs. Such a subset may be maintained in a well-known location and made available to a new SAS administrator during the certification process.

6 SAS to SAS Security

The SAS to SAS transport method and protocol has two essential requirements. First of all, it must guarantee the transport security requirement as to be addressed in later sections. Secondly, it needs to satisfy a general purpose requirement that allows broad applications and easy adoption. Transport Layer Security (TLS) over TCP/UDP socket satisfies both these requirements.

SAS implementations shall verify all communications with other SAS peers are done using the mechanisms described in the Spectrum Sharing Committee Working Group 2 Communications Security Technical Report [3]. Specifically, SASs shall only accept such communications when made using TLS communications using a currently-valid certificate identifying the counterparty as a certified SAS.

7 SAS to SAS Information Exchange Elements

The current document only describes the format of exchange elements and is not binding for the SAS to share all the data elements. The requirement on the minimum set of parameters to be exchanged between SASs to maintain a stable radio environment will be determined based on co-existence studies of various defined scenarios.

The SAS-SAS protocol is built upon the exchange of data records representing the current status of Part 96 entities known to one SAS and communicated to another SAS. Such communication may happen on a state change in a particular entity (e.g. a CBSD offered a frequency grant, or an enforcement action taken by the FCC, or a change in incumbent activity learned by a SAS), or upon request by a proper SAS counterparty (e.g. when a new SAS enters the peer group, or recovers from a service outage and requests incremental information).

These data records summarize data related to specific Part 96 entities as defined in the rules and present within each SAS implementation’s data store. The format of the SAS-SAS protocol imposes no constraints on the data storage of any SAS implementation: it is strictly an exchange format for metadata related to particular entities known to the system and about which information is exchanged to achieve the functional objectives required to be performed by the SAS administrator.

As subjects of information exchange, each Part 96 entity will be referred to by a globally unique name within the SAS ecosystem. Such names will be constructed of a sequential list of name tokens, allowing for the SAS namespace to include currently-existing namespaces when possible for maximum interoperability with existing naming schemes. For example, entities corresponding to device types will use FCC IDs associated with the equipment authorization process as a name token to uniquely refer to such device types. Entities corresponding to CBSDs will make use of serial numbers as required to be presented in the registration process to uniquely refer to particular CBSDs.

As a shorthand, these token sequences will be represented using a ‘/’ separator character. So a particular CBSD name will be represented as “cbsd/FCC_ID/SERIAL_NUMBER”.

7.1 SAS-SAS Exchange Entities and Names

Part 96 Entity	Description
SAS Administrators	Manage specific SAS implementations. There may be many implementations maintained by a single SAS administrator. Names will be of the form “admin/sas/\$ADMINISTRATOR” where the second token is chosen by the administrator and verified to be unique in the SAS Certificate Authority (SAS-CA) certificate issuance process.

ESC Administrators	Manage specific ESC implementations. Names will be of the form “admin/esc/\$ADMINISTRATOR” and verified to be unique in the SAS-CA certificate issuance process.
SAS Implementations	A particular SAS implementation. Names will be of the form “sas/\$ADMIN/\$IMPLEMENTATION” where the second token is the name of the administrator and the third token is chosen by the SAS administrator and verified unique by the SAS-CA certificate issuance process.
ESC Implementations	A particular ESC implementation. Names are of the form “esc/\$ADMIN/\$IMPLEMENTATION” where the second token is the name of the administrator and the third token is chosen by the ESC administrator and verified unique by the SAS-CA certificate issuance process.
CBSD device types	Particular equipment certified for operation in the CBRS band. Certification will be by the FCC and reflected in a unique FCC_ID number. This will be verified during the SAS-CA certificate issuance process. Names will be of the form “cbstd-type/\$FCC_ID” where the second token is the FCC ID assigned in the FCC equipment authorization process.
CBSDs	Specific devices which will operate in the CBRS band and gain spectrum use authorizations from the SAS. Names will be of the form “cbstd/\$FCC_ID/\$SerialNumber” where the second token is the FCC ID associated with the CBSD device type as certified by the FCC, and the third token is chosen by the device manufacturer and guaranteed by that manufacturer to be unique within the FCC ID namespace scope.
Incumbents	Specific incumbent devices (FSS earth stations or grandfathered wireless broadband service installations) which are known to the SAS. Names will be of the form “incumbent/\$SOURCE/\$ID” and have names taken from a closed set drawn from FCC databases. For example, “incumbent/ibfs/KA261” would refer to a particular call sign for an FSS earth station present in the IBFS database.
Zones	Geographical areas with various meanings within the SAS. For example, census tracts (PAL areas), WISP protection areas, ad hoc protection zones, etc. Such zones will have names of the form “zone/\$CREATOR/\$ID” where the second token takes on values representing either the SAS or ESC administrator responsible for the creation of the zone, or a predefined token related to static government-sourced information defining geographical zones. The third token takes on values assigned by the creator or assigned using a pre-existing namespace.
CBSD operators	Entities which operate CBSDs. The SAS is required to track particular information related to such entities as received during the CBSD registration process. Operators will have names of the

	form “operator/\$SAS/\$ID” where the second token is the name of a SAS administrator with which a particular operator is registered, and the third token is chosen uniquely by that SAS administrator.
Domain Proxies	Entities operating networks of CBSDs. From the point of view of Part 96, such entities are a particular kind of CBSD operator, but since they have different certification and capability sets within the SAS ecosystem they are referred to separately with names of the form “domain/\$ID”. Here the second token is chosen by the domain proxy operator and verified unique by the SAS-CA certificate issuance process.
Professional Installers	Entities vouching for particular CBSD metadata. Names are of the form “installer/\$INSTALLER” where the second token is chosen by the installer and verified unique by the SAS-CA certificate issuance process.
Coordination events	Part 96 rules require formal exchange of information regarding a wide range of events, such as GAA/FSS arrangements, PAL/PAL arrangements, enforcement actions by FCC, etc. Names for particular coordination events will be assigned by the SAS administrator in which the coordination event is registered and follow the format “coordination/\$SAS/\$ID” where the second token is equivalent to a valid SAS administrator name and the third token is chosen uniquely by that SAS administrator within this namespace.

Together these entities compose the full spectrum of entities about which Part 96 requires that SAS exchange information. For each entity, the SAS-SAS protocol defines a full set of information which the SAS possesses (according to Part 96 requirements) about such an entity in order to fulfill its function.

Note that some entities have their unique names governed by the SAS-CA certificate issuance process, while other names can be created dynamically within a more tightly scoped part of the namespace and are the responsibility of that creator to ensure uniqueness. The SAS-CA processes will ensure namespace uniqueness of these names, and will also be disambiguated against each other such that the same actor with different roles will use the same name, and no separate actor in a different role can re-use a token from another namespace. (That is, an ESC operator could not adopt the name of a SAS operator, even though they would still be unique: the SAS-CA will enforce selection from a merged unique namespace.)

7.2 SAS Administrator Exchange Record

These records provide contact information for SAS administrators.

Field	Field Description
ID	SAS Administrator name
Name	Human-readable name of the SAS administrator
Contact Information	Human readable contact information (e.g. phone number, address)
FCC Information	e.g. first certification date

7.3 ESC Administrator Exchange Record

These records provide contact information for ESC administrators.

Field	Field Description
ID	ESC Administrator name
Name	Human-readable name of the ESC administrator
Contact Information	Human readable contact information (e.g. phone number, address)
FCC Information	e.g. first certification date

7.4 SAS Implementation Exchange Record

These records provide human and machine contact information for SAS implementations, as well as machine-consumable authentication information for the SAS.

Field	Field Description
ID	SAS implementation name
Name	Human-readable name of the SAS implementation
Administrator	Name of SAS administrator
Contact Information	Human readable contact information (e.g. phone number, address)
Public Key	X.509 key for the SAS implementation
Certification Date	The date the SAS was certified by FCC
Certification Phase	“1” or “2” depending on how the SAS is certified
ESC	The name of the ESC this SAS is using, if it is phase 2
URL	Human-facing public URL for this SAS
SAS-SAS URL	Machine-addressable base URL for this SAS for discovery of the SAS-SAS endpoint
SAS-CBSD URL	Machine-addressable base URL for this SAS for discovery of the SAS-CBSD endpoint

7.5 ESC Implementation Exchange Record

These records provide contact and certification information on a particular ESC implementation.

Field	Field Description
ID	ESC implementation name
Name	Human-readable name of the ESC
Administrator	Name of the ESC administrator
Contact Information	Human readable contact information (e.g. phone number, address)
Certification Date	When the ESC was certified

7.6 Domain Proxy Exchange Record

These records provide contact (human and machine) and certification status information on a particular domain proxy. (Note that in this case acceptance of the possibility of interference from federal radar will be implicit in other processes.)

Field	Field Description
ID	Domain Proxy name
Name	Human-readable name of the domain proxy operator
Contact Information	Human readable contact information (e.g. phone number, address)
Public Key	X.509 key for the domain proxy
Certification Information	The date the domain proxy was certified (and possibly other related certification information)

7.7 CBSD Device Type Exchange Record

These records provide information regarding the certification status and equipment characteristics for a particular device type. A device type corresponds to a specific equipment authorization process.

Field	Field Description
ID	Device Type name
Name	Human-readable name of the equipment (e.g. model name)
Manufacturer	Human-readable name of the equipment manufacturer
Contact Information	Human readable contact information (e.g. phone number, address)
Public Key	X.509 key assigned to this model

Certification Information	The date the equipment was certified (and possibly other related certification information such as OOBE class, maximum number of grants, etc)
Device Characteristics	Other operating parameters provided by the manufacturer, such as the air interface type, antenna characteristics, etc.

7.8 CBSD Exchange Record

These records provide for the exchange of registration and authorization information about particular CBSDs.

Field	Field Description
ID	CBSD name
Public Key	X.509 key for this device
Installation Parameters	Registration data for this CBSD as collected by the SAS, including any operator ID information and PAL authorization information
Operating Parameters	Any spectrum grants outstanding to the CBSD

7.9 Incumbent Exchange Record

These records provide for the exchange of information regarding the current status of incumbents in the CBRS band. Ordinarily this information will be separately ingested by each SAS implementation. The exchange record is public, and therefore can be made available for testing, and also an informing incumbent may be able to alter some parameters more rapidly within the ecosystem than it would take to update FCC databases, thus that updated information would need to be shared with other SASs. In addition, the coordination record exchange requires identification of counterparties to any coordination event; providing this information provides that formal reference.

Field	Field Description
ID	Incumbent name
Deployment Parameters	Parameters from FCC database entries related to this incumbent, including location, antenna configuration, etc.
Operating Parameters	Any frequency use information or other faster-changing operating information regarding the incumbent. (e.g. pointing angles for an informing incumbent)

7.10 Zone Exchange Record

These records allow for exchange of geographical information (such as ad hoc protection zone definitions) in such a way that they can be referred to compactly by name in other records.

Field	Field Description
ID	Zone name
Name	Human-readable name for this zone
Creator	The identity of the creator of this domain (human-readable, may not refer to another Part 96 entity)
KML	The KML definition of the zone as a placemark with a multi-geometry contained in it, which will contain one or more polygons

7.11 CBSD Operator Exchange Record

These records allow for exchange of contact information regarding CBSD operators.

Field	Field Description
ID	Operator name
Name	Human-readable name of the CBSD operator
Contact Information	Human readable contact information (e.g. phone number, address)
Acknowledgement of Interference from Federal Radars	Human-readable representation of the state of such an acknowledgement

7.12 Professional Installer Exchange Record

These records allow for exchange of contact information (human and machine) regarding professional installers and their current credentials.

Field	Field Description
ID	Installer name
Name	Human-readable name of the professional installer
Public Key	X.509 key of the installer
Certification Status	Information from the certification status of the installer, such as certification date, last training, certification program, and other relevant information

7.13 Coordination Event Exchange Record

These records allow for exchange of data regarding particular coordination events in the band. Such events have a relatively large range of possibility, so the records are modeled on representing a kind of generic human-readable email type notification system, with an accompanying extensible property which will enable frequent interactions to be automated using machine-readable metadata.

It is expected that such coordination events would be dealt with manually by and large until some experience is built up around particular common coordination events, which can then be defined as machine-readable extensions. Some extensions may be predefined during the certification process to account for time-sensitive coordination requirements.

Field	Field Description
ID	Coordination event name
Name	Human-readable reference to the event (need not be unique), similar to an email subject line
Creator	Who initiated this coordination event, may refer to a non-part-96 entity, such as an FSS operator
Creation Date	When the event was created
Expiration Date	If the coordination event is regarding an expiring condition (e.g. activation of an ad hoc protection zone), the time this coordination record expires
Description	Human-readable description of the coordination event, similar to an email body
Coordination Type	A machine-readable code for facilitating automated handling for particular types of coordination events (e.g.: an interference report by an incumbent, or the activation of a particular pre-existing ad hoc zone)
Coordination Device	If the coordination event involves a device, this is that name (e.g. a CBSD ID or an incumbent ID)
Coordination Zone	If the coordination event involves a particular zone, this is that zone ID (e.g. the activation or creation of an ad hoc protection zone)
Coordination Data	Machine-readable extensible anchor for any other metadata needed for automated handling of particular coordination events

8 SAS-SAS Exchange Mechanisms

The SAS-SAS protocol will support three types of mechanisms (individual records, time-based ranges of records, and a full activity dump) for exchanging the information elements described in Section 7. Each of these will provide both a “pull” and a “push” variant. When

using a “pull” variant, a requesting SAS will send a message to a peer SAS requesting a particular record or set of records. The peer SAS then responds with the requested information. Using the “push” variant, the peer SAS will pro-actively provide information to a client when those records change. The details of whether two particular SAS implementations use the push or pull mechanism is left up to those specific implementations and what works best for them. The protocol provides for both but only one variant may be used, or one variant for some information elements and the other for others.

All requests will be conducted over Hypertext Transfer Protocol (HTTP: RFC 2616, 7230, 7540). For all mechanisms, push and pull variants, and information elements exchanged, Uniform Resource Locators (URLs) requested or used for push notifications will be constructed based on a single base SAS-SAS URL which can be discovered by each SAS in the peer group. For the “pull” variant, the SAS-SAS protocol uses the HTTP GET method, and constructs a url for requests following the procedure described in this section. It then issues that request to the peer and receives a JSON-formatted reply containing the data requested (or any error messages the request may trigger). For the “push” variant, the SAS-SAS protocol uses the HTTP POST method. The source SAS constructs a url for the notification following the procedure described in this section. It then issues the notification to the peer using that url, and using a JSON-formatted content containing the notification data.

The mechanism of the full activity dump is different. Instead of the full dump being made available as a direct result to the query, a query by a peer will return a JSON-formatted message containing metadata about the current activity dump provided by the source SAS, including a url where the peer can request the full dump. Since preparing such dumps is a costly and time-consuming matter for a source SAS, it will be done periodically on a schedule determined by the source SAS and then the resulting activity dump made available to any peer requesting it. This dump is intended to serve as a source of current status for any new SAS which joins the peer group. As such, the dump may not be prepared until requested by a peer, and the peer may need to wait an interval before requesting the dump from the source SAS.

Information Element Type	URL construction
SAS Administrators	<u>Individual Records</u> Pull: GET \$BASE_URL/sas_admin?id=\$ID Push: POST \$BASE_URL/sas_admin?id=\$ID <u>Time-range records</u> Pull: GET \$BASE_URL/sas_admin?start=\$T1&end=\$T2 Push: POST \$BASE_URL/sas_admin?start=\$T1&end=\$T2
ESC Administrators	<u>Individual Records</u> Pull: GET \$BASE_URL/esc_admin?id=\$ID Push: POST \$BASE_URL/esc_admin?id=\$ID <u>Time-range records</u>

	<p>Pull: GET \$BASE_URL/esc_admin?start=\$T1&end=\$T2 Push: POST \$BASE_URL/esc_admin?start=\$T1&end=\$T2</p>
SAS Implementations	<p><u>Individual Records</u> Pull: GET \$BASE_URL/sas?id=\$ID Push: POST \$BASE_URL/sas?id=\$ID</p> <p><u>Time-range records</u> Pull: GET \$BASE_URL/sas?start=\$T1&end=\$T2 Push: POST \$BASE_URL/sas?start=T1&end=\$T2</p>
ESC Implementations	<p><u>Individual Records</u> Pull: GET \$BASE_URL/esc?id=\$ID Push: POST \$BASE_URL/esc?id=\$ID</p> <p><u>Time-range records</u> Pull: GET \$BASE_URL/esc?start=\$T1&end=\$T2 Push: POST \$BASE_URL/esc?start=T1&end=\$T2</p>
CBSD Device Types	<p><u>Individual Records</u> Pull: GET \$BASE_URL/cbsd_type?id=\$ID Push: POST \$BASE_URL/cbsd_type?id=\$ID</p> <p><u>Time-range records</u> Pull: GET \$BASE_URL/cbsd_type?start=\$T1&end=\$T2 Push: POST \$BASE_URL/cbsd_type?start=T1&end=\$T2</p>
CBSDs	<p><u>Individual Records</u> Pull: GET \$BASE_URL/cbsd?id=\$ID Push: POST \$BASE_URL/cbsd?id=\$ID</p> <p><u>Time-range records</u> Pull: GET \$BASE_URL/cbsd?start=\$T1&end=\$T2 Push: POST \$BASE_URL/cbsd?start=T1&end=\$T2</p>
Incumbents	<p><u>Individual Records</u> Pull: GET \$BASE_URL/incumbent?id=\$ID Push: POST \$BASE_URL/incumbent?id=\$ID</p> <p><u>Time-range records</u> Pull: GET \$BASE_URL/incumbent?start=\$T1&end=\$T2 Push: POST \$BASE_URL/incumbent?start=T1&end=\$T2</p>
Zones	<p><u>Individual Records</u> Pull: GET \$BASE_URL/zone?id=\$ID Push: POST \$BASE_URL/zone?id=\$ID</p> <p><u>Time-range records</u> Pull: GET \$BASE_URL/zone?start=\$T1&end=\$T2</p>

	Push: POST \$BASE_URL/zone?start=T1&end=\$T2
CBSD Operators	<u>Individual Records</u> Pull: GET \$BASE_URL/operator?id=\$ID Push: POST \$BASE_URL/operator?id=\$ID <u>Time-range records</u> Pull: GET \$BASE_URL/operator?start=\$T1&end=\$T2 Push: POST \$BASE_URL/operator?start=T1&end=\$T2
Domain Proxies	<u>Individual Records</u> Pull: GET \$BASE_URL/domain?id=\$ID Push: POST \$BASE_URL/domain?id=\$ID <u>Time-range records</u> Pull: GET \$BASE_URL/domain?start=\$T1&end=\$T2 Push: POST \$BASE_URL/domain?start=T1&end=\$T2
Wildcard Retrieval for time-range records	<u>Time-range records</u> Pull: GET \$BASE_URL/any?start=\$T1&end=\$T2 Push: POST \$BASE_URL/any?start=T1&end=\$T2
Full activity dump	Pull: GET \$BASE_URL/dump Push: POST \$BASE_URL/dump

8.1 Providing Metadata-Only in Respond to Time-Range Requests

The requesting SAS may provide only identifying metadata for records in response to time-range requests, depending on arrangements between the peers. This is because peers using the push variant will ordinarily be tracking changes quite closely. They will still periodically issue time-range requests to make sure no data was dropped, but in most cases this will only provide verification. As such, such data may be clipped to the minimum required to identify a notification (e.g. ID and activity timestamp).

8.2 Time Basis for Time-Range Requests

The time parameters and interpretation in the SAS-SAS requests are to be interpreted in the frame of reference of the SAS supplying the data. So in a “pull” request, the time parameters are interpreted in the time reference frame of the server SAS (not the client).

8.3 Wildcard Time-Range Requests

The wildcard retrieval and notification methods may return or provide identifying metadata only, since they are intended to provide a requester with all activity during a given period. The concept of operations is that a peer may request all IDs changed within a given period, then request the current record status by ID for any changed record. Since all IDs are globally

unique and indicate their type within their encoding, no additional type information besides the ID needs to be attached in a notification or reply.

8.4 Providing Activity Dump Metadata

A SAS may wait until a /dump request to generate a full activity dump. The peer may then need to wait to request the url advertised in the dump. (A SAS may use the push variant to advertise to the requester when the dump becomes available.)

The metadata prepared in response to the full dump request includes the following fields:

Field	Field Description
URL	The retrieval URL at which the peer can retrieve the activity dump must be retrieved within the TLS context from the peer
Generation Date-Time	The date and time at which the activity dump was generated; the dump is guaranteed to include the effects of all activity up to and including this time
Checksum	The cryptographic checksum and method for the activity dump
Size	The size of the dump file in bytes
Description	Any additional human-readable description the source SAS may wish to attach