System Requirements Specification

for

Using Third Parties to Deliver Infrastructure-to-Vehicle (I2V)

Version 1.0

Prepared by:
Southwest Research Institute
P.O. Drawer 28510
San Antonio, TX 78228-0510

January 10, 2020

Prepared by _____ **Date** 01/10/2020
Cameron Mott
Senior Research Analyst

Approved By _____ **Date** 01/10/2020
Eric Thorn, Ph.D.
Manager R&D

Revision History

Version	Date	Author (s)	Comment
0.1	11/21/2019	SwRI	Initial Draft
0.2	12/06/2019	SwRI	Improved Draft
0.3	12/12/2019	SwRI	Draft after walkthrough
1.0	01/10/2020	SwRI	Release version

Table of Contents

List of Figures

List of Tables

1. Introduction

The participants in the Connected Vehicle (CV) Pool Fund Study (PFS) group are managing large amounts of data relevant to connected and non-connected vehicles. This data can be provided to vehicle operators through third-party companies or system integrators. To help scale and standardize the distribution of this data, the CV PFS team has funded a project called "Using Third Parties to Deliver I2V." This project is focused on the system engineering and standardization of data that is transmitted from States and other infrastructure owners and operators (IOOs) to third parties and Original Equipment Manufacturers (OEMs).

Stakeholder interviews have allowed the team to gather an understanding of the breadth of efforts that are already in place (or planned) regarding the usage of vehicular data by third-party companies and OEMs. As part of this project, the team has delivered a Survey of Current Status document detailing the maturity and future plans of CV data sharing activities. The team has also prepared a Concept of Operations (ConOps) document which describes the users, user needs, functions and features, operational scenarios, constraints, and context diagrams for the CV Data Framework (CVDF). This System Requirements Specification (SyRS) document has been generated based on the ConOps and ongoing collaboration with stakeholders. It includes the system requirements necessary to guide the development of a CVDF implementation to meet the needs of the stakeholders as described in the ConOps document. The final systems engineering document will be an Interface Control Document (ICD) and will define the interfaces that are used to connect to the system.

1.1 Project Scope

The focus of this project is the standardization of communication from States and IOOs to third-party application providers or OEMs. Direct communication channels between States/IOOs and vehicles exist in the form of vehicle-to-everything (V2X) communication. This project recognizes that this will continue to occur, and in addition, there are auxiliary connections to vehicles and smart devices that are enabled through third-party connections. Existing communication from States/IOOs to third-party companies is based on an agency-by-agency and third party-by-third party arrangement, which is inefficient and complicated. This is represented in the "before" diagram shown in Figure 1-1.

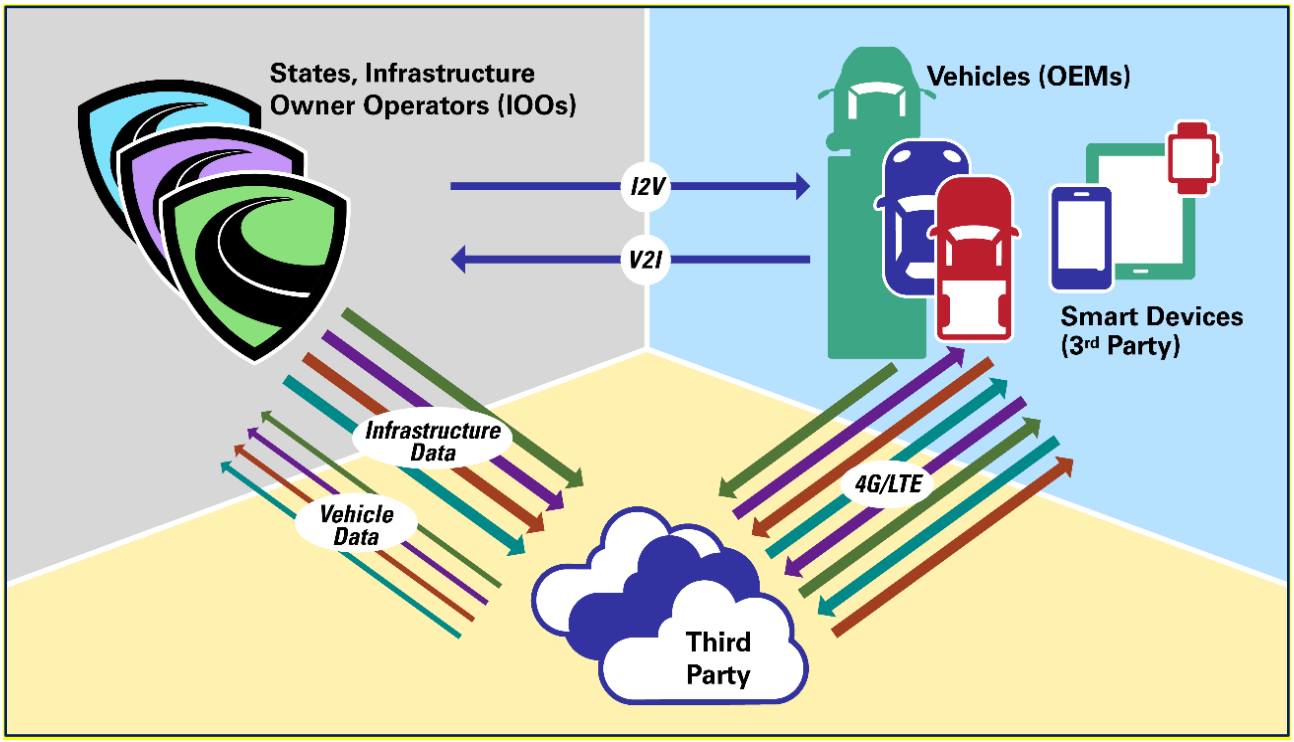

Figure 1-1: Example communication channels between states/IOOs, third-party companies, vehicles, and smart devices.

This project will attempt to standardize the communication between States/IOOs and third-party companies. Standardizing this data will allow the multiple streams of data from IOOs and third parties to be consistent. The data will be provided via implementations that adhere to the CVDF defined through this project. Such implementations will result in the data exchanges shown in Figure 1-2. Through these efforts, the participants in the CV PFS and others can benefit from the usage of a standardized data distribution strategy.

The scope of the project includes the interactions between the CVDF and third parties or OEMs. The focus will be on the data that will be standardized and provided through the CVDF. Data (contained in payloads) provided through the CVDF is depicted in Figure 1-3. Based on the Concept of Operations, valuable data for third parties includes (but is not limited to) Signal Phase and Timing (SPaT), MAP, Basic Safety Messages (BSMs), signal controller status, equipment location, and time synchronization data. Additional data that has been considered includes signal timing plans, pedestrian call and vehicle call information, presence detection, splits, signal cycles, work zone information, reduced speed limits, and queues. This document will propose a high-level structure for communicating this data to third party consumers; additional details will be provided in the ICD. Interactions between third parties and vehicles or user devices are considered out of scope for this project. Direct communication between States/IOOs and vehicles or user devices, as well as a back-end operation and administration of the data framework, are also considered out of scope.

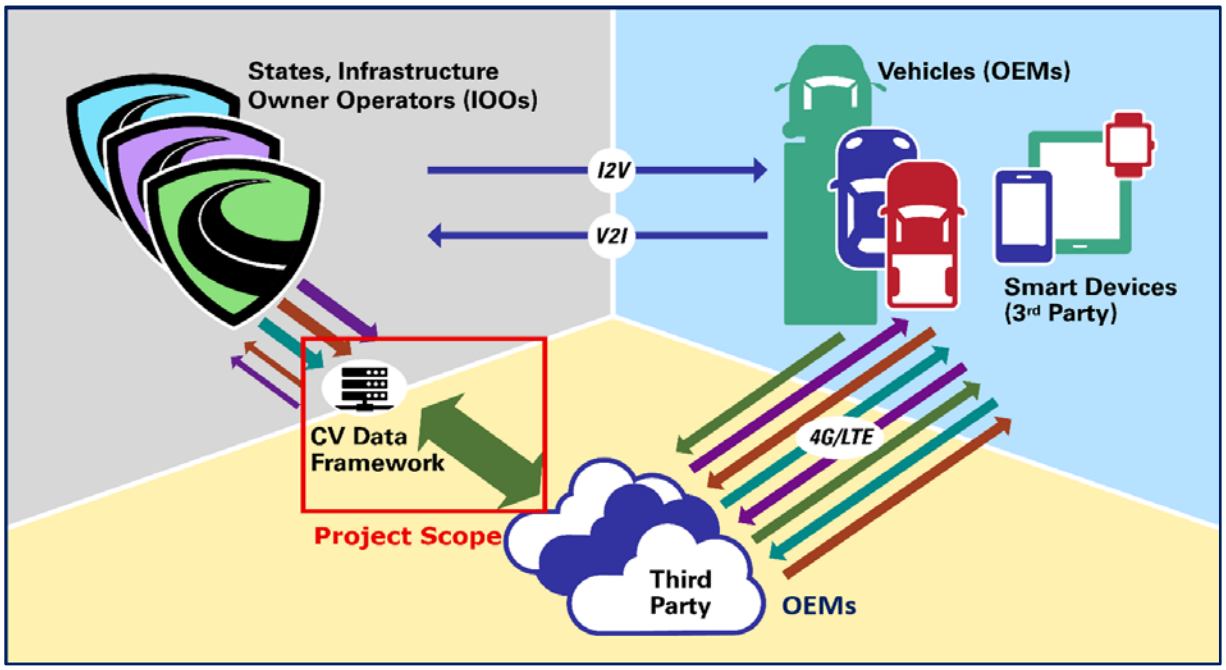

Figure 1-2: Project scope and interactions between the CVDFCV and other stakeholders

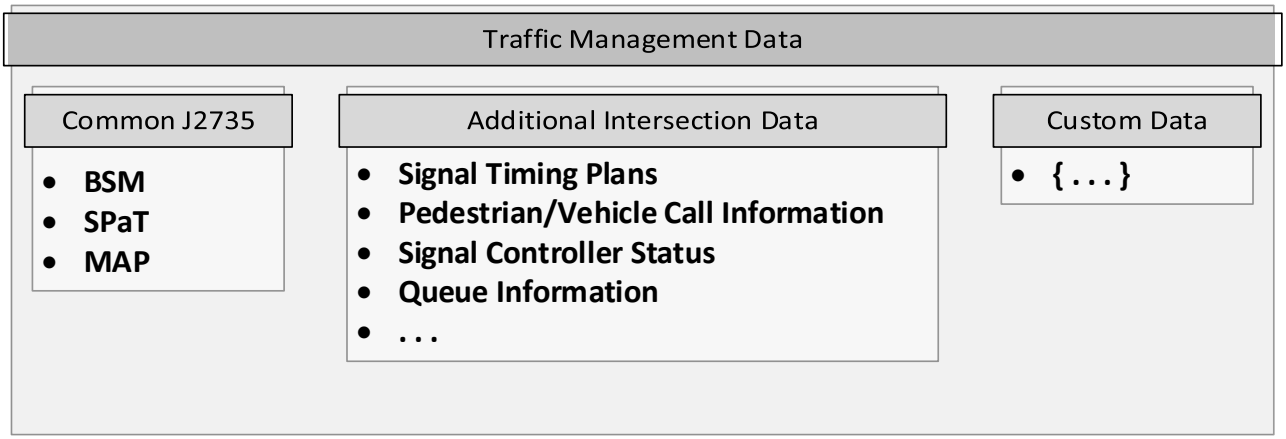

Figure 1-3: Example data that could be provided by implementations of the CVDF

1.2 Acronyms and Definitions

Table 1-1: Acronym List. provides a list of all of the acronyms used in this document. Table 1-2 defines many of the terms that are used in this document where the authors identified some potential ambiguities or confusion.

Table 1-1: Acronym list

Acronym	Definition
API	Application Programming Interface
BSM	Basic Safety Message
CV	Connected Vehicle
CVDF	CV Data Framework
EST	Eastern Standard Time
GPS	Global Positioning System
HTTPS	Hypertext Transfer Protocol over SSL
ICD	Interface Control Document
ITS	Intelligent Transportation System
IOO	Infrastructure Owner and Operator
MAP	Not an acronym, refers to the SAE J2735 message that defines geographic information
NIST	National Institute of Standards and Technology
NTCIP	National Transportation Communications for ITS Protocol
OBU	On-Board Unit
PFS	Pooled Fund Study
REST	Representational State Transfer
RSU	Roadside Unit
SAE	Society of Automotive Engineering
SPaT	Signal Phase and Timing
SSL	Secure Sockets Layer
SyRS	System Requirements Specification
TLS	Transport Layer Security
TMDD	Traffic Management Data Dictionary
TSC	Traffic Signal Controller
UTC	Coordinated Universal Time

Table 1-2: Glossary of terms

Term	Definition
Function	A goal or objective accomplished by an implementation of a product or service.
Feature	A system or subsystem that is utilized in order to achieve a function.
Infrastructure Owner Operator	Regional authority that operates deployed field equipment and is usually responsible for enabling and managing traffic within a defined geographical area.
Requirement	A necessary condition that the system needs to meet to operate as designed.
Stakeholder	An organization with an interest in utilizing the framework proposed through this project.
System Integrator	An organization that maintains the hardware/software components that provide the functionality of the system.
Third-Party Application	A commercial product provided by a company working with at least one IOO to utilize CV data and provide information to a customer of their system. OEMs may be providing this commercial product as a feature that is integrated into their vehicles.
User	An operator of the system defined in this document or one that manages an external system.
Publisher	An external system providing information to the CVDF.
Subscriber	An external system consuming data from the CVDF as described in this document.

2. Overall Description

Standardization of the CVDF external interface communication is the focus of this document. Internal data communication between CVDF subsystems is described to provide context but will not be standardized through this project and is only provided as guidance. It is expected that communication from the CVDF to an external system will be the same regardless of which external system is connected.

2.1 System Context

A system context diagram is shown in Figure 2-1. In this diagram, the external systems are communicating with the CVDF using a single connection (depicted as a dashed rectangle) with a defined application programming interface (API) that defines the input and output format. The internal subsystems are communicating data through the blue arrows, whereas a dashed blue

arrow indicates an optional data flow. Some subsystems contain optional components, which are depicted in gray. This context diagram guides the design of the following sections.

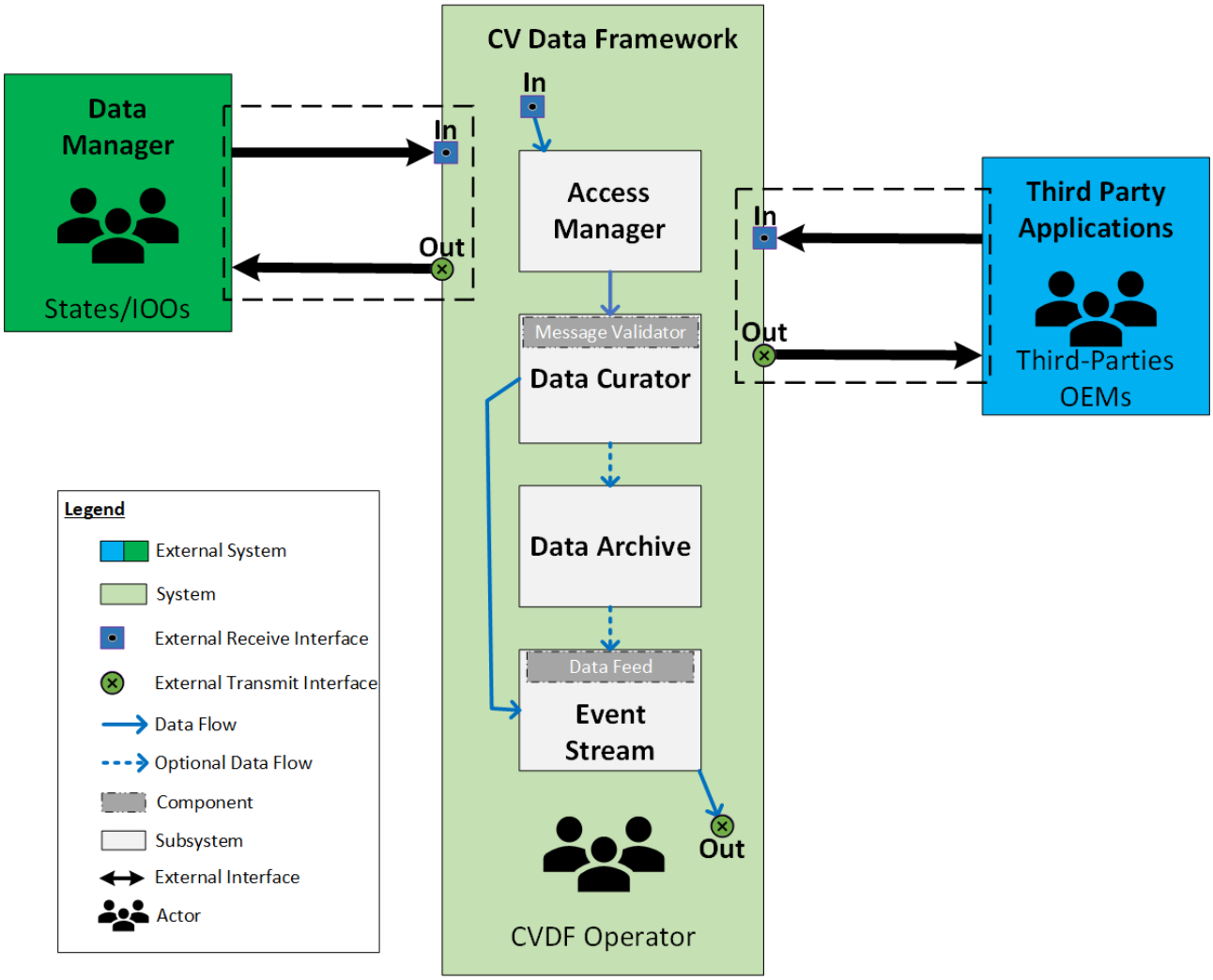

Figure 2-1: CVDF system context diagram

2.2 System Functions

The CVDF supports the following major system functions:

- Receive and provide common J2735 messages including but not limited to BSM, SPaT, and MAP.
- Receive and provide additional intersection data including but not limited to signal timing plans, pedestrian call and vehicle call information, signal controller status, and queue information.

- Receive and provide custom data that does not adhere to an externally defined communication standard but is defined and made available by the CVDF operator.
- Verify the authenticity of input data.
- Manage an authorized recipients list.
- Provide event-based data to authorized recipients.
- Secure outbound and inbound connections to the system.
- Optionally provide the ability to archive data.
- Optionally provide archived data to authorized recipients.
- Optionally aggregate data from multiple sources.

2.3 Operating Environment

The operating environment will be largely left up to the implementers of the framework. No operating system or hardware platforms will be specifically required. Software subsystems must coexist inside of an implementation. The CVDF system must define and make available the schema (in the form of an API) that dictates the external interfaces for communicating with the CVDF.

2.4 Design and Implementation Constraints

Implementers should be aware of the following constraints when designing their system: data timeliness, data reliability, GPS availability, GPS resolution, and data rates. The timeliness of data has been identified as a constraint for some subscribers focused on implementing applications concerning timing, safety, and synchronization. To effectively deliver these applications, data must be provided with minimal latency. Similarly, subscribers of all types will rely on the data provided from the framework to be at least as reliable as the source device's output. Required values must be present so that applications can be designed around them. Personally Identifiable Information (PII) may be removed so that the subscriber does not have to worry about the ramifications of accidentally exposing PII. GPS availability and resolution will conform to the defined on-board system performance requirements in SAE J2945/1[1] to provide an accuracy of 1.5m at 1 sigma. Maps should contain reference points that allow RSUs to estimate the location of the broadcast area. Finally, different message types and subscription agreements will dictate the minimum and maximum data refresh rates which need to be considered by implementers to ensure that all subscription models can be fulfilled, or the limits of the system need to be clearly communicated with the subscribers before agreements are drafted.

[1] https://saemobilus.sae.org/content/j2945/1_201603

2.5 Assumptions and Dependencies

Data timeliness expectations depend on network link speeds and equipment communication processing buffer timings. It is assumed that data can be delivered from infrastructure equipment, be processed by the CVDF, then received by the data subscriber in sub-1-second intervals consistently, regardless of the scale of the system. It is assumed that all signalized intersections will have access to GPS signals when weather conditions permit, or if blocked by infrastructure, a solution to report location data will be implemented such as a pre-configured location or the usage of a reradiation signal. Additionally, if a GPS signal is unavailable then timing information will be made available through a network time protocol system.

3. External Interface Requirements

The external interfaces to the CVDF may connect to systems managed by external users (OEMs, third parties, or IOOs). Each external interface shall have the same set of requirements, which are listed in Table 3-1. References to requirements throughout this document are structured according to the following guidelines:

- <REQ> or <OPT>: REQ for requirements, OPT for optional recommendations.
- <Sublabel>: Short, three letter label for the high-level category of the entry.
- <Major number>: The major number is incremented for every major capability captured by a requirement.
- <Minor number>: The minor number starts with 0 for the first major capability and is incremented by every entry that supports a major capability.
- <Optional sub-number>: Sub-numbers are created when an entry supports a minor capability.

Table 3-1: External interface requirements

ReqID	Requirement
REQ-EXT-1.1	The CVDF shall collect data from any number of external systems.
REQ-EXT-1.2	The CVDF shall add timestamps to data received by the CVDF system's host machine from an external system.
REQ-EXT-1.3	The CVDF shall enable connections with external systems through a standardized web service using one or both of the following: • REST (preferred) • GraphQL

ReqID	Requirement
REQ-EXT-1.4	The CVDF shall collect data at variable rates from publishers.
REQ-EXT-1.5	The CVDF shall collect data only from authorized publishers.
REQ-EXT-1.6	The CVDF shall provide schemas that describe the format of the data available from the external interfaces.
REQ-EXT-1.7	The CVDF shall only collect information from external interfaces that comply with the defined schema.
REQ-EXT-1.7.1	The CVDF schemas shall contain information identifying the sender.
REQ-EXT-1.7.2	The CVDF schemas shall contain the message creation time as reported by the external system.
REQ-EXT-1.7.3	The CVDF schemas shall contain information regarding the time synchronization source that was used for encoding the message creation time.
REQ-EXT-1.7.4	The CVDF schemas shall contain information identifying a geographical region in which it is applicable.
REQ-EXT-1.7.5	The CVDF schemas shall populate header fields that identify whether the provider has requested the information to be restricted to a minimum subscriber permission level.
REQ-EXT-2.1	The CVDF shall transmit data to any number of external systems.
REQ-EXT-2.2	The CVDF shall only publish data to authenticated external systems.
REQ-EXT-2.3	The CVDF shall provide schemas that describe the format of the data provided to subscribers of the external interfaces.
REQ-EXT-2.4	The CVDF shall only publish data to subscribers with appropriate subscription permissions.

3.1 Data Elements for External Interface

The data elements in the external interface include a header and a payload that can contain other standardized messages or CVDF customized messages. Expected standardized messages include the SAE J2735 generic MessageFrame as well as more specific MapData and SignalPhaseAndTimingMessage. NTCIP 1202, 1218, 12xx, and TMDD v3 payloads are also

expected to be supported. Table 3-2 captures the structure of a message sent by a CVDF to subscribers.

Table 3-2: Example high-level message structure for an outgoing external message

Message Portion	Data Element
Header	Source
	Authentication token
	Location/region
	Distribution restrictions
	Timestamp and time source
Payload	Standardized or Custom message
Verification	Signature

A representation of the high-level message structure is represented in Figure 3-1 below.

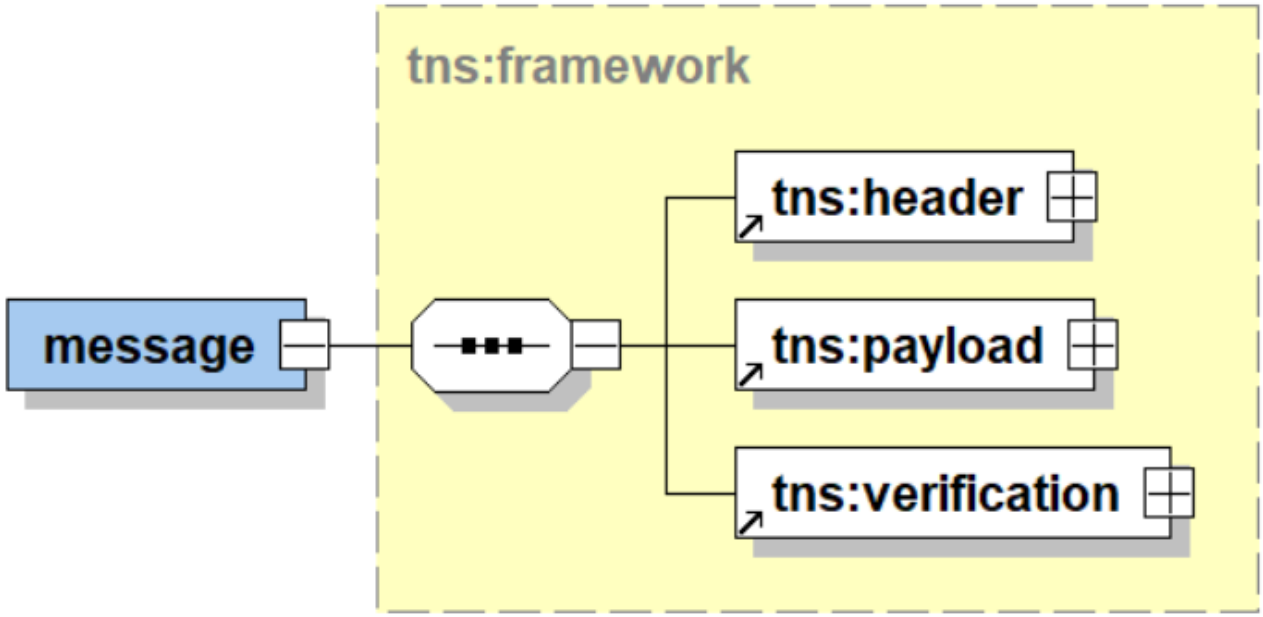

Figure 3-1: CVDF high-level message structure

Each of the high-level message components have additional subcomponents as represented in Figure 3-2.

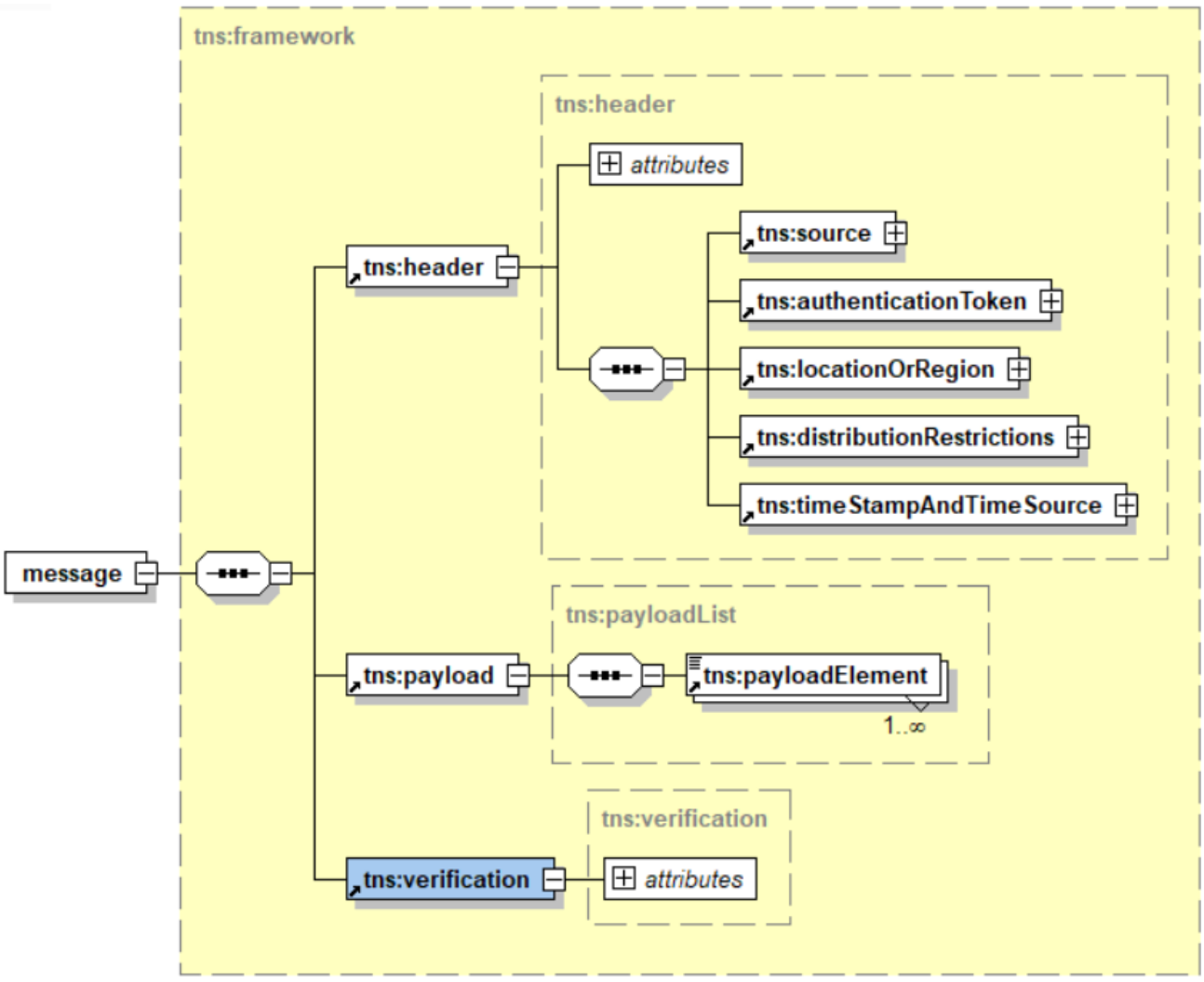

Figure 3-2: CVDF medium-level message structure

3.1.1 Supported Applications

In order to support the applications identified as valuable by previous project efforts, specific message payloads are defined in this document. Pending feedback from stakeholders, applications defined in Table 3-3 will require specific message payloads for messages provided

by the CVDF. For additional context on many of these applications, refer to the ConOps from this project.

Table 3-3: Software application reference table

Application Reference Name	Application Name	Description
ECOS	Eco Approach and Departure at Signalized Intersections	An application that allows connected vehicles to optimize the time spent and fuel consumed in order to traverse an intersection.
EECOS	Extended Eco-Approach at Signalized Intersection	Similar to the ECOS but extends the scope of the application to encompass multiple intersections along a traveler's route, the intersection timing plans of those intersections, and historical traffic data related to the traveler's route.
RLVW	Red Light Violation	An application that will provide awareness to a connected vehicle and its driver that based on their current trajectory they will pass the stop bar of the intersection during a stop and remain phase.
PEDX	Pedestrian in Crosswalk	An application that will provide awareness to a connected vehicle and its driver that the vehicle is approaching an area where a pedestrian has requested a walk signal.
SPP	Signal Preemption and Priority	An application that allows authorized vehicles to request a change in phase status to receive a favorable signal to clear an intersection in a timelier manner.
LTA	Left Turn Assist	An application that will alert a connected vehicle and its driver that an oncoming vehicle has a permissive green turning signal and may legally be occupying their through movement lane.

4. Internal System Features

In this section, each internal subsystem and its components are outlined including: a brief description, the priority of implementation, the sequence of events following a user interaction, and the associated functional requirements. The requirements that are attributed to each subsystem need to be met by a CVDF implementation, though the subsystem names and individual subsystem functionality are left to the implementer.

The subsystem names are summarized below along with an indication of whether or not the modules are optional:

- Access Manager [Required]
- Data Curator [Required]
    - Message Validator (Optional)
- Data Archive (Optional)
- Event Stream [Required]
    - Data Feed (Optional)

4.1 Access Manager

The access manager's function is to authenticate each user and that user's ability or inability to submit subscription and/or provider query requests to the system. The access manager will allow CVDF operator administrators to create, edit, or delete an account identity. CVDF operator administrators will grant each account the minimum required privileges necessary through the access manager. The access manager will create a session for each user per connection. Once a user is granted a connection session, queries may be submitted through that connection and will be passed through the access manager into the system to be routed by the data curator.

4.1.1 Priority

An access manager feature is of high priority to the CVDF as a protective barrier between the users of the system and the internal subsystems to prevent unauthorized access and enhance security.

4.1.2 Stimulus/Response Sequences

When a new connection is made to the system, the access manager shall be invoked and the user shall be identified, authenticated, and authorized if possible. If the user is unable to be identified, the access manager will prompt the new user to create an identity for future use within the system. Administrators of the system can elevate user privileges based on external subscription contracts, provider contracts, or aspects of the connection itself. If a user is successfully identified by the system, they will be given access to edit or delete their accounts and submit subscription and/or provider query requests.

4.1.3 Functional Requirements

The functional requirements for the access manager are shown in Table 4-1.

Table 4-1: Access Manager functional requirements

Requirement ID	Description
REQ-IAM-1.1	The access manager shall provide an access control system.

Requirement ID	Description
REQ-IAM-1.2	The access manager shall authenticate users in a secure way, so that other internal subsystems can verify the authentication for the duration of a session.
REQ-IAM-1.3	The access manager shall allow CVDF operator administrators to modify the access control system and the underlying information contained in the system.
REQ-IAM-1.4	The access manager shall verify a user's identity using trusted cryptography standards and current best practices.
REQ-IAM-1.5	The access manager shall protect the privacy and data integrity of the connections to third parties. This is accomplished by encrypting data sent over public networks using at least Transport Layer Security (TLS) v1.2, sanitizing user input which could lead to an unauthorized access, providing non-confirmatory responses to invalid user login attempts, and any precautionary measures deemed necessary by system implementers to protect user information.
REQ-IAM-1.6	The access manager shall verify and create cryptographic signatures.
REQ-IAM-1.7	The access manager shall store references to where a subscriber may access the information that they have requested in agreement with the CVDF system operators.
REQ-IAM-1.8	The access manager shall update access control system permissions to reflect the subscription agreements made between the CVDF and its users.
REQ-IAM-1.9	The access manager shall allow users to access specific event stream access connections in accordance with the active access control system permissions.

4.2 Data Curator

The data curator handles and routes all incoming requests. Optionally, the curator may perform message validation by parsing the payload's data elements and validating the data contained in the payload. The data curator ensures consistency throughout the framework and validates the conformity to provided schemas. This in turn increases efficiency of data processing throughout (and through) the system.

4.2.1 Priority

The data curator is of high priority to the CVDF system because it provides central communication and routing to all other subsystems.

4.2.2 Stimulus/Response Sequences

Once a session connection is established by the access manager, user request queries shall be passed to the data curator to be handled internally. Depending on the type of request query and user privilege level the data curator will resolve the request query appropriately. Third parties can interact with the CVDF through any combination of three different avenues: one-time push (POST request query), one-time pull (GET request query), and data streams which consist of push and pull queries for known resource subsets whose states are expected to be updated at predetermined intervals. Archive data storage and retrieval support is optional, but if implemented by the system it will be supported by the defined interaction avenues. All messages are associated with a specific subset of underlying resources.

One-time push queries are requests to instantiate an instance and/or update the state of a specific subset of resources. One-time pull queries are requests to confirm or deny the existence and/or the state of specific resources, based on the CVDF's perspective. Both one-time push and pull queries occur when information about a resource is considered valuable and becomes available or is required at non-deterministic times. For resource information that is expected to be updated at deterministic times, data streams provide consistent status updates in real-time. Data streams can be established during a one-time push or pull query to decrease the number of future queries required to keep information current.

4.2.3 Functional Requirements

The functional requirements for the data curator are shown in Table 4-2.

Table 4-2: Data Curator functional requirements

Requirement ID	Description
REQ-IDC-1.1	The data curator shall ensure all required metadata elements are valid and populated before messages can be routed anywhere.
REQ-IDC-1.1.1	The data curator shall notify the publisher when provided data is invalid.
OPT-IDC-1.2	The data curator may modify metadata values based on subscription/publication agreements or flags within the message. For example: changing EST time to UTC time.
REQ-IDC-1.3	The data curator shall validate high-level message construction and formatting such as conformity to standardized schemas.
OPT-IDC-1.4	The data curator may implement a payload validator.

Requirement ID	Description
OPT-IDC-1.5	The data curator may sanitize input data to remove PII.

4.3 Data Archive

A data archive is an optional subsystem in the CVDF. If implemented, the data archive allocates long term storage for messages that are designated to be archived and manages previously archived messages. The data archive will store and retrieve messages that the data curator identifies but will not be responsible for any payload validation. The data archive should monitor for data corruption so that if data is identified as corrupted, it can either be restored from backup or discarded.

4.3.1 Priority

The data archive has a low priority to the CVDF, because the archive may not need to be implemented by the CVDF (or at all). The CVDF may be granted read access to an archive database that is maintained by a separate entity and can provide an avenue to third parties who are interested in the data without actually implementing a database within the framework. If there is no data archive, the CVDF may only provide real-time data to the subscribers of the system.

4.3.2 Stimulus/Response Sequences

After data providers/subscribers are authenticated by the access manager and their requests to store/retrieve data are processed by the data curator, the data archive will fulfill those requests.

4.3.3 Functional Requirements

The functional requirements for the data archive are shown in Table 4-3.

Table 4-3: Data Archive functional requirements

Requirement ID	Description
OPT-IDA-1.1	If implemented, the data archive would handle valid external provider requests to archive data and valid external subscriber requests to access archived datadata.

4.4 Event Stream

The event stream is a buffer between the data curator and the data subscriber third party. The event stream buffer is directionally output biased; only the data curator can write to it and only data subscribers can read from it. The data curator will forward available relevant data to the event stream which will publish the data in such a way that all pertinent subscribers will have access to the update. The event stream will populate an additional metadata field in the outer message frame which will provide timing information for each message received by the buffer.

4.4.1 Priority

It is a high priority for the CVDF system to implement an event stream feature so that consumers have the ability to build on top of, and contribute to, the framework's connectivity.

4.4.2 Stimulus/Response Sequences

When data is transmitted by the system, the event stream manages and populates the web connection with the data that is provided by the data curator subsystem. The event stream ensures that the connection to the subscriber stays open and accessible. Additionally, the event stream will populate the time a message was published.

4.4.3 Functional Requirements

The functional requirements for the event stream are captured in Table 4-4.

Table 4-4: Event Stream functional requirements

Requirement ID	Description
REQ-IES-1.1	An event stream shall be accessible and responsive for at least 95% of five-minute intervals in a given region yearly.
REQ-IES-1.2	An event stream shall operate a timing mechanism dependent on at least a stratum-2 device.
OPT-IES-1.2.1	If possible, an event stream shall operate a timing mechanism dependent on a stratum-1 device.
REQ-IES-1.3	An event stream shall only operate in an outbound direction.
OPT-IES-1.4	An aggregate feed component may be implemented to combine disparate individual payloads into an outbound message.
REQ-IES-1.5	An event stream shall be able to open and sustain a connection to the subscriber when directed to by the access manager.
REQ-IES-1.6	An event stream shall be able to publish data to multiple subscribers concurrently.

4.5 Message Validator

A message validator is an optional extension to the data curator. If implemented, the message validator would provide an additional layer of scrutiny to input data. The message validator's focus will be on the proper encoding of the message frame payloads and accuracy of the associated metadata, as opposed to the data curators focus on high-level message frame construction. As part of this focus, the message validator will identify, flag, and discard any malicious or invalid data that may be provided to the system. If less than desirable data is found, the message validator may take remediation actions, including dropping the message, removing the undesirable data, or limiting that provider's privileges if necessary.

4.5.1 Priority

Implementing a message validator is a low to medium priority for the CVDF system, because it is not required but would add data reliability to the system.

4.5.2 Stimulus/Response Sequences

After a provider's connection is authenticated through the access manager and data is collected by the system, the message validator shall parse the message and check it for validity. Depending on the source of the data and any timeliness constraints identified by the system's consumers, data may or may not be validated before being transmitted via the event stream. Regardless of system constraints, the message validator should run in between the curator and data archive in order to validate all messages prior to archiving. Data originating from the data archive does not need to be validated again unless data corruption is identified as a risk by the system administrators.

4.5.3 Functional Requirements

Since the message validator is an optional component, all requirements are flagged as optional recommended entries. When a message validator is present, the recommendations should be respected. The functional recommendations for the Message Validator are shown in Table 4-5.

Table 4-5: Message Validator functional recommendations

Requirement ID	Description
OPT-IMV-1.1	If implemented, the message validator would have the ability to decode a subset of the message encodings that are defined in the framework's schema.
OPT-IMV-1.2	If implemented, the message validator would be able to confirm or deny that metadata encoding tags were correctly provided.
OPT-IMV-1.3	If implemented, the message validator would be sufficiently isolated from the rest of the system to protect from malicious payload injections.
OPT-IMV-1.4	If implemented, the message validator would be capable of flagging suspicious packets.
OPT-IMV-1.5	If implemented, the message validator, when provided with a supported payload encoding, would be able to check encoded information against metadata associated with the message.
OPT-IMV-1.6	If implemented, the message validator would have the ability to verify signatures of entire message frames and subsections of messages.

Requirement ID	Description
OPT-IMV-1.7	If implemented, the message validator would communicate with the access manager when a message provider supplies undesirable inputs.

4.6 Data Feed

A data feed will communicate with the access manager to deliver enhanced real-time or archived event stream data to active subscribers via the event stream, depending on current subscription agreements. The data feed is an optional component of the event stream.

4.6.1 Priority

A data feed is of low priority for the CVDF system to implement. It is an optional feature that is responsible for data aggregation and enhancement.

4.6.2 Stimulus/Response Sequences

When a subscription is created that plans to utilize the data feed for data enhancement or aggregation, the access manager notifies the data feed and the event stream. If the subscription relies on archived messages, the data feed will retrieve pertinent messages from the archive. If the subscription relies on real-time information, then the data feed will rely on data updates as input from the data curator before applying any enhancements to it. Regardless of the source of information the data feed will process the messages if they fulfill the requirements of the subscription agreement, enhance them, combine the results into a standalone message that includes the inputs, and publish the result to subscribers via an internet connection.

4.6.3 Functional Requirements

Since the Data Feed is an optional component, all requirements are flagged as optional recommended entries. When a data feed is present, the recommendations should be respected. The functional recommendations for the data feed are shown in Table 4-6.

Table 4-6: Data Feed functional recommendations

Requirement ID	Description
OPT-IDF-1.1	If implemented, the data feed would be able to create enhanced data message outputs based on real-time and/or archived data messages if an archive is available.
OPT-IDF-1.2	If implemented, the data feed would be able to publish information into an open event stream web connection.
OPT-IDF-1.3	If implemented, the data feed would normalize units and scales for data in the header or appropriate customized payloads to an agreed-upon common reference and or accuracy as defined by the system integrator

Requirement ID	Description
	based on the ICD. For example: all geolocation points shall be stored in absolute decimal degree units with at least a meter resolution.
OPT-IDF-1.4	If implemented, the data feed would possess the ability to accept and execute modular functions created by authorized, audited, and trusted external users, subject to approval by CVDF administrator operators.

5. Nonfunctional Requirements

This section describes requirements related to the performance and security attributes for the CVDF system that are separate from the functional requirements. Each subsection is separated by a set of nonfunctional requirements. They were generated using stakeholder recommended functionality for the CVDF that not all external systems may be able to meet.

5.1 Performance Requirements

The performance requirements are capabilities the system needs to provide under various scenarios. This includes any latency and data throughput of the messages being exchanged throughout the system. Each performance requirement is listed in Table 5-1.

Table 5-1: Performance requirements

Requirement ID	Description
REQ-PRF-1.1	Data identified by external users as “low-latency data” shall be sent to other external users with minimal delay from the time it was received by the system.
OPT-PRF-1.2	The system may archive common J2735 messages for some pre-determined duration.
OPT-PRF-1.3	The system may archive additional standardized intersection data for some pre-determined duration.
OPT-PRF-1.4	The system may archive additional non-standardized custom data for some pre-determined duration.

5.2 Security Requirements

Security requirements refer to any data security or privacy issues for the protection of CV data that passes through the CVDF. It is expected that appropriate data protection policies will be in place for both the implementers of the CVDF and external systems. Authentication is required, encryption is optional but recommended for internal data at rest. The specific method for authentication is left to the implementer and may leverage existing standards such as HTTPS or TLS. Each of the external systems need to authenticate their identity with the CVDF. Encryption

techniques are also left to the implementer and should leverage appropriate standardized encryption techniques such as those approved by NIST. The security requirements are shown in Table 5-2.

Table 5-2: Security requirements

Requirement ID	Description
REQ-SEC-1.1	The CVDF shall authenticate communication with external systems.
OPT-SEC-1.2	The CVDF may encrypt data at rest within the system.