Module 23: Leveraging Communications Technologies for Transit On-board Integration

Table of Contents

Module Description

There are a wide variety of onboard transit technologies and they are integrated using several types of communications technologies. These onboard technologies facilitate and automate operations, management, maintenance, traveler information, safety, and security functions of public transit systems. With the advent of newer communication technologies, onboard technologies can be integrated via an onboard transit architecture that is comprised of on-board devices, communications pathways (on and to/from the vehicle), functionality, and interfaces to the vehicle. Onboard devices include a mobile data terminal (MDT), vehicle logic unit (VLU) (sometimes combined with an MDT), equipment to support supervisory and support functions (e.g., ruggedized laptop), Automated Vehicle Announcement (AVA) System (covered in Modules 6 and 7), Automatic Passenger Counter (APC) System (covered in Modules 2 and 5), an Event Data Recorder System (EDRS) and Vehicle Component Monitoring (VCM) (covered in Modules 2 and 5), and Onboard Video Surveillance System (covered in Modules 2 and 5). Module 19 provides details of how to use onboard hardware and software standards and provides case studies and examples that demonstrate how to procure systems that use these standards.

1. Introduction/Purpose

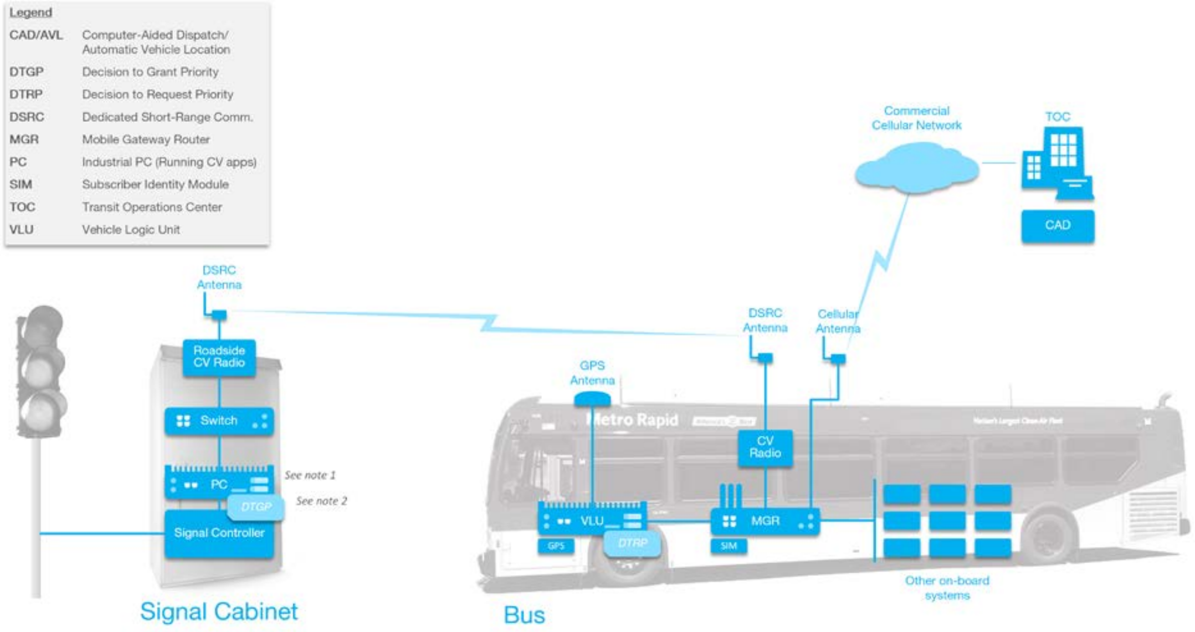
This module provides details on how to leverage current communication technologies to integrate onboard devices and provides case studies and examples that demonstrate the use of these technologies. The information in this module will help participants further understand those communication technologies that support the integration of onboard transit devices for buses, specifically Internet of Things (IoT) Gateways, Mobile Gateway Router (MGR), future second generation onboard architectures and the evolution of onboard IoT edge logic. Topics that will be covered in this module include current and future on-board architectures, IoT gateways, moving onboard functionality to the cloud, and transit agency considerations.

2. Samples/Examples

2.1. Los Angeles County Metropolitan Transportation Authority (LA Metro) Transit Signal Priority (TSP) Concepts

LA Metro conducted a TSP concept development activity that resulted in the following:

- Vehicle-to-Infrastructure (V2I) Connected Vehicle (see Figure 1)
- Vehicle-to-Infrastructure (V2I) Cellular to Isolated Signal (see Figure 2)
- Vehicle-to-Center (V2C) Cellular to Centralized TMC (see Figure 3)
- Center-to-Center (C2C) Fully Centralized TOC and TMC (see Figure 4)


Legend
CAD/AVL Computer-Aided Dispatch/ Automatic Vehicle Location
DTGP Decision to Grant Priority
DTRP Decision to Request Priority
DSRC Dedicated Short-Range Comm.
MGR Mobile Gateway Router
PC Industrial PC (Running CV apps)
SIM Subscriber Identity Module
TOC Transit Operations Center
VLU Vehicle Logic Unit
Commercial Cellular Network
TOC
CAD
DSRC Antenna
Roadside CV Radio
Switch
PC
See note 1
DTGP
See note 2
Signal Controller
Signal Cabinet
DSRC Antenna
Cellular Antenna
GPS Antenna
CV Radio
VLU
GPS
DTRP
MGR
SIM
Other on-board systems
Bus

1. Local intersection PC is required only if controller is not an Advanced Traffic Controller (ATC). If traffic agency has upgraded to ATC the BSP application and DTGP can reside on the controller.

2. DTGP functionality may reside on either PC or controller, depending on architecture.

Figure 1. V2I Connected Vehicle Concept (courtesy of Ed Alegre, LA Metro)

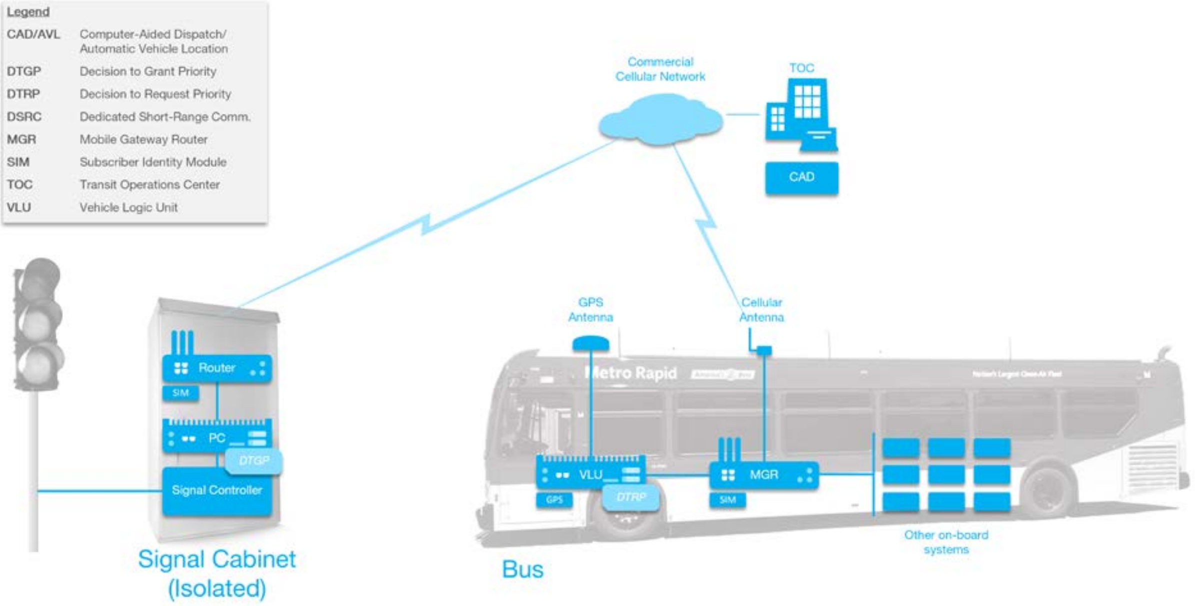

Legend
CAD/AVL Computer-Aided Dispatch/ Automatic Vehicle Location
DTGP Decision to Grant Priority
DTRP Decision to Request Priority
DSRC Dedicated Short-Range Comm.
MGR Mobile Gateway Router
SIM Subscriber Identity Module
TOC Transit Operations Center
VLU Vehicle Logic Unit
Commercial Cellular Network
TOC
CAD
Router
SIM
PC
DTGP
Signal Controller
Signal Cabinet (Isolated)
GPS Antenna
Cellular Antenna
VLU
GPS
DTRP
MGR
SIM
Other on-board systems
Bus

Figure 2. V2I Cellular to Isolated Signal (courtesy of Ed Alegre, LA Metro)

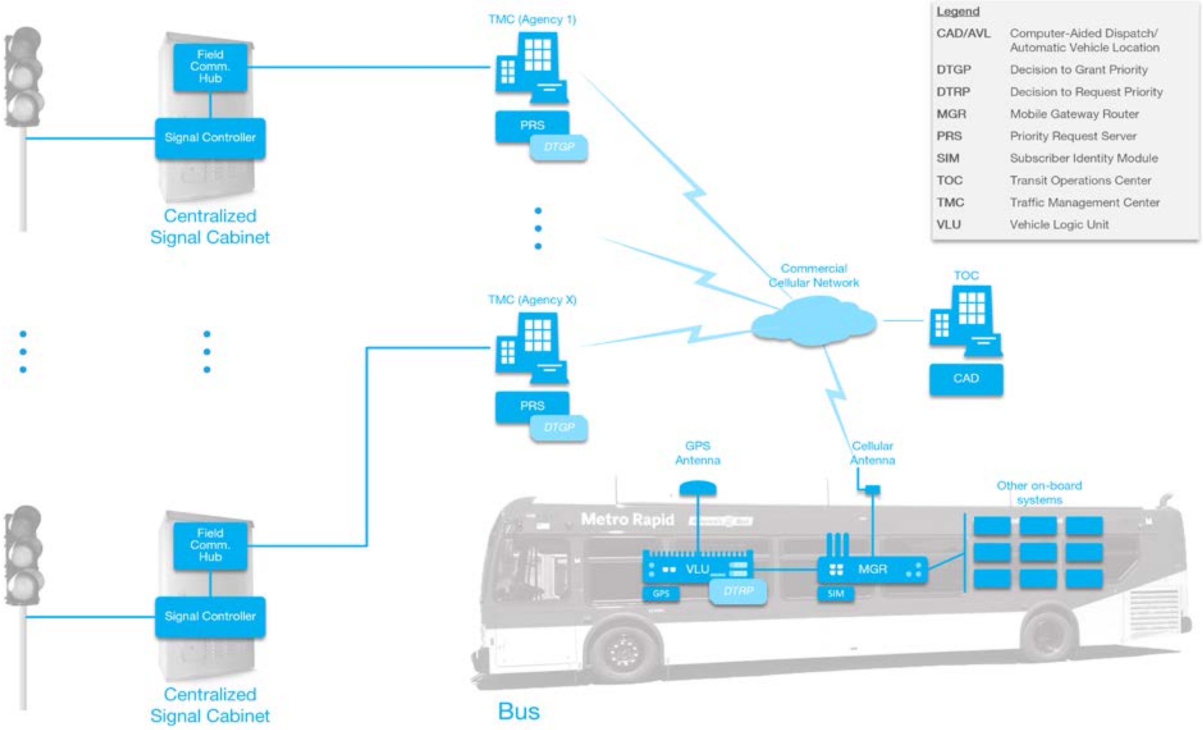

Legend
CAD/AVL Computer-Aided Dispatch/ Automatic Vehicle Location
DTGP Decision to Grant Priority
DTRP Decision to Request Priority
MGR Mobile Gateway Router
PRS Priority Request Server
SIM Subscriber Identity Module
TOC Transit Operations Center
TMC Traffic Management Center
VLU Vehicle Logic Unit
TMC (Agency 1)
Field Comm. Hub
Signal Controller
Centralized Signal Cabinet
PRS
DTGP
TMC (Agency X)
PRS
DTGP
Field Comm. Hub
Signal Controller
Centralized Signal Cabinet
Commercial Cellular Network
TOC
CAD
GPS Antenna
Cellular Antenna
Other on-board systems
Metro Rapid
VLU
GPS
DTRP
MGR
SIM
Bus

Figure 3. V2C Cellular to Centralized TMC (courtesy of Ed Alegre, LA Metro)

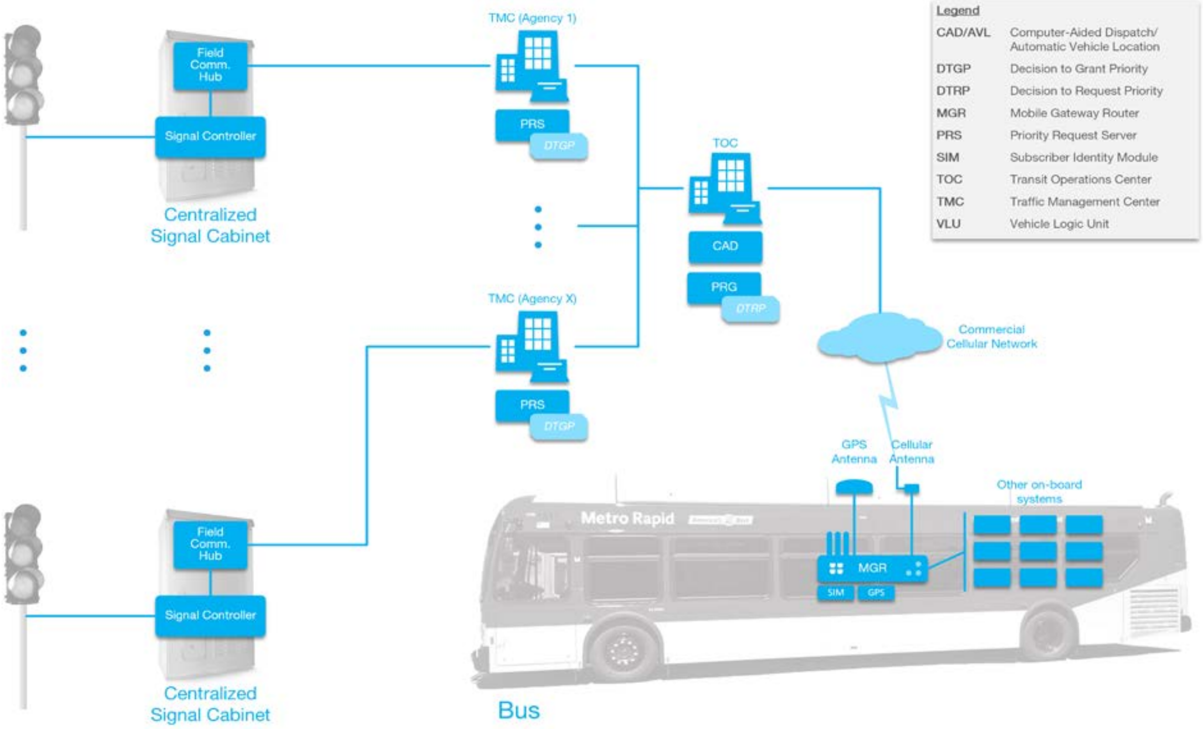
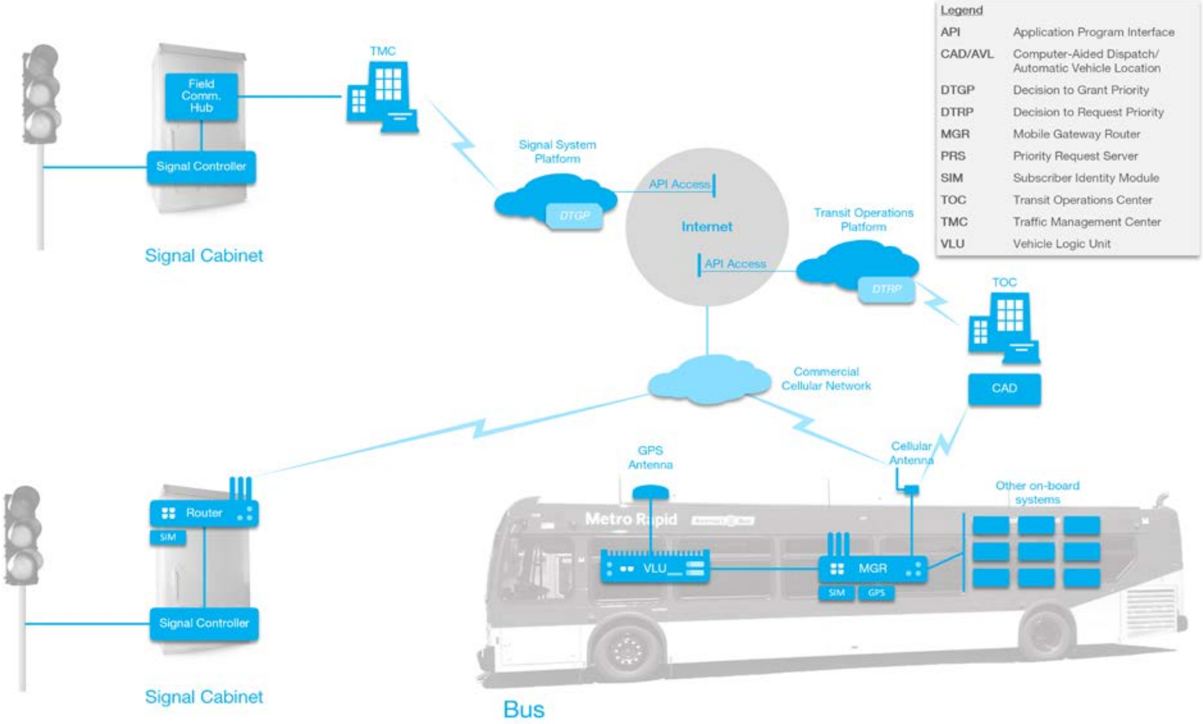

Legend
CAD/AVL Computer-Aided Dispatch/ Automatic Vehicle Location
DTGP Decision to Grant Priority
DTRP Decision to Request Priority
MGR Mobile Gateway Router
PRS Priority Request Server
SIM Subscriber Identity Module
TOC Transit Operations Center
TMC Traffic Management Center
VLU Vehicle Logic Unit
TMC (Agency 1)
Field Comm. Hub
Signal Controller
Centralized Signal Cabinet
PRS
DTGP
TOC
CAD
PRG
DTRP
TMC (Agency X)
PRS
DTGP
Field Comm. Hub
Signal Controller
Centralized Signal Cabinet
Commercial Cellular Network
GPS Antenna
Cellular Antenna
Other on-board systems
Metro Rapid
MGR
SIM
GPS
Bus

Figure 4. C2C Fully Centralized TOC and TMC (courtesy of Ed Alegre, LA Metro)

In addition to these four concepts, LA Metro developed a next generation TSP concept that has the "cloud" as the key component as shown in Figures 5, 6, and 7. For this LA Metro next-gen concept, the cloud performs four main functions:

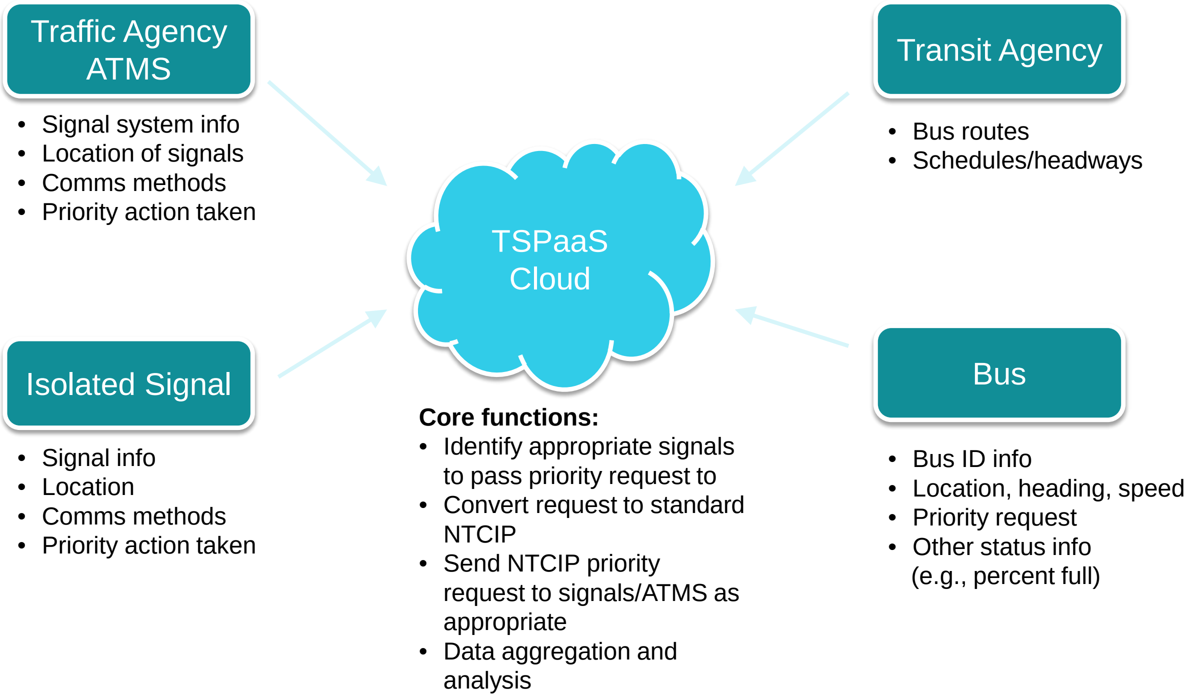
- "Communicate with all TSP clients, including individual buses, transit management system, individual signals, and the traffic agency ATMS. Correlating bus route and schedule info with signal system info and signal locations, the cloud determines the correct signals to pass priority request messages to.
- "Using this correlated information, it converts request messages to the signal controller messaging standard as appropriate (NTCIP 1211 is the usual standard).
- "Communicates the tailored priority request to the client applications at the ATMS or individual controllers.
- "Records and aggregates all actions taken on both the transit and signal side and performs analytics on the data to support performance monitoring and planning purposes."[1]



API	Application Program Interface
CAD/AVL	Computer-Aided Dispatch/ Automatic Vehicle Location
DTGP	Decision to Grant Priority
DTRP	Decision to Request Priority
MGR	Mobile Gateway Router
PRS	Priority Request Server
SIM	Subscriber Identity Module
TOC	Transit Operations Center
TMC	Traffic Management Center
VLU	Vehicle Logic Unit

Figure 5. TSP as a Service (TSPaaS) (courtesy of Ed Alegre, LA Metro)

[1] DKS Associates, "The Next Generation of Transit Signal Priority: Cloud Computing and the TSP-as-a-Service Model," presentation at 2017 ITS California Annual Meeting, September 30, 2017. Used with permission of DKS.



Core functions:

- Identify appropriate signals to pass priority request to
- Convert request to standard NTCIP
- Send NTCIP priority request to signals/ATMS as appropriate
- Data aggregation and analysis

Figure 6. TSP-as-a-Service Inputs (courtesy of Elliot Hubbard, DKS Associates)

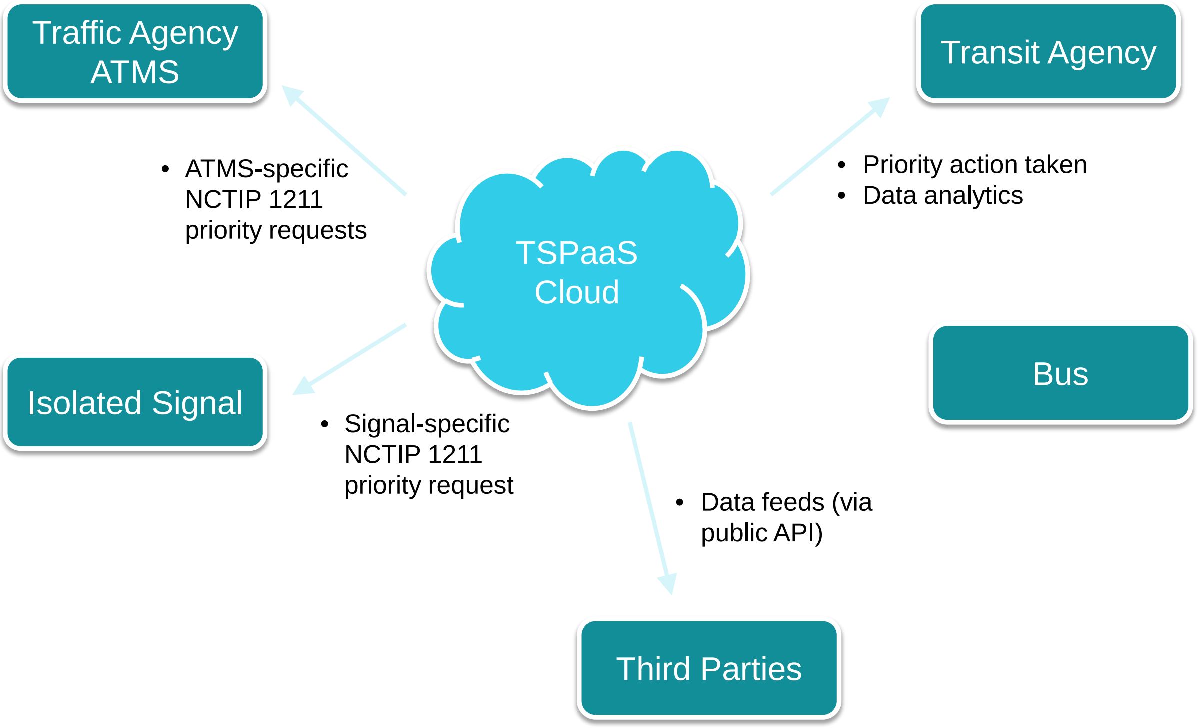

Traffic Agency ATMS
Transit Agency
• ATMS-specific NCTIP 1211 priority requests
• Priority action taken
• Data analytics
TSPaaS Cloud
Bus
Isolated Signal
• Signal-specific NCTIP 1211 priority request
• Data feeds (via public API)
Third Parties

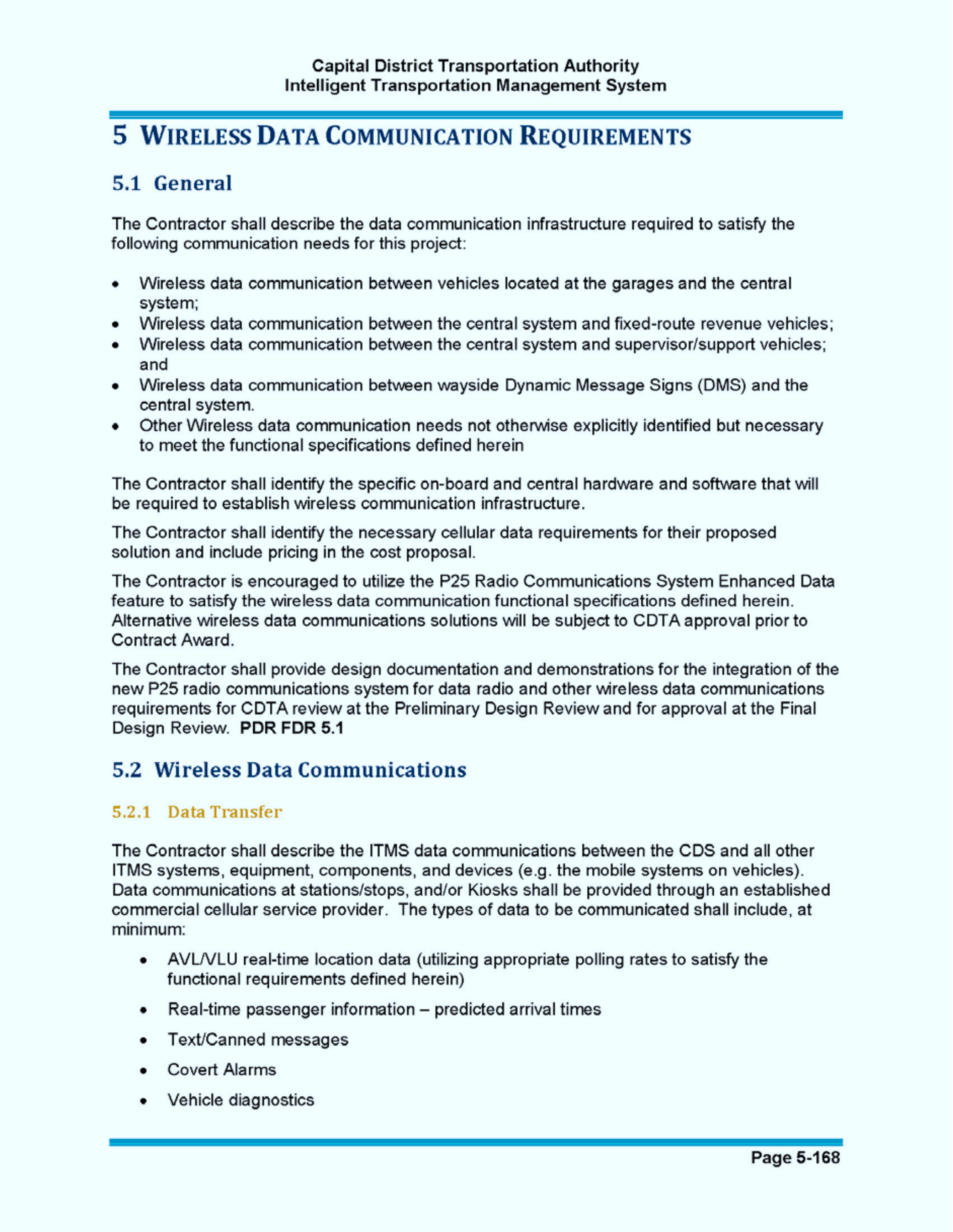
Figure 7. TSP-as-a-Service Outputs (courtesy of Elliot Hubbard, DKS Associates)

2.2. Capital District Transportation Authority (CDTA) Intelligent Transportation Management System (ITMS) – Albany, NY

The Capital District Transportation Authority (CDTA) in Albany, NY conducted a major procurement to replace their aging CAD/AVL system. Within this procurement, there was a requirement for On-Board Mobile Routers/ Wireless Gateways. The requirement for On-board Mobile Gateway Routers (OMGRs) was included in the specifications in Section 5.2.3. This section of the specifications is contained on the next five pages.

Other portions of Request for Proposal referring to the OMGRs are as follows:

- Open Payment System Infrastructure – The Contractor shall partner with SPXGenfare to integrate open payments through CDTA's new FastFare® ® electronic Fareboxes via the Contractor's ITMS on-board mobile gateway router. The purpose of this interface is to provide customers with on-board payment card transactions in real time.
- On BusPlus vehicles, Clever Devices IVN and mobile routers transmit vehicle location data to CD's central prediction system (BusTime server).
- As described in section 5 "Wireless Data Communication Requirements," CDS wireless communications with ITMS on-board ITMS equipment, components, and devices shall be via the wireless mobile routers on-board vehicles and wireless access points at each operating division and select transit stations within the CDTA service area where CDTA has wide-area networking infrastructure.
- *4.7.3 On-Board Customer Wi-Fi.* The Contractor shall provide on-board Wi-Fi enabled Internet access to customers as part of the ITMS On-board Mobile Gateway/Router (OMGR) on all CDTA vehicles.



5 Wireless Data Communication Requirements

5.1 General

The Contractor shall describe the data communication infrastructure required to satisfy the following communication needs for this project:

- Wireless data communication between vehicles located at the garages and the central system;
- Wireless data communication between the central system and fixed-route revenue vehicles;
- Wireless data communication between the central system and supervisor/support vehicles; and
- Wireless data communication between wayside Dynamic Message Signs (DMS) and the central system.
- Other Wireless data communication needs not otherwise explicitly identified but necessary to meet the functional specifications defined herein

The Contractor shall identify the specific on-board and central hardware and software that will be required to establish wireless communication infrastructure.

The Contractor shall identify the necessary cellular data requirements for their proposed solution and include pricing in the cost proposal.

The Contractor is encouraged to utilize the P25 Radio Communications System Enhanced Data feature to satisfy the wireless data communication functional specifications defined herein. Alternative wireless data communications solutions will be subject to CDTA approval prior to Contract Award.

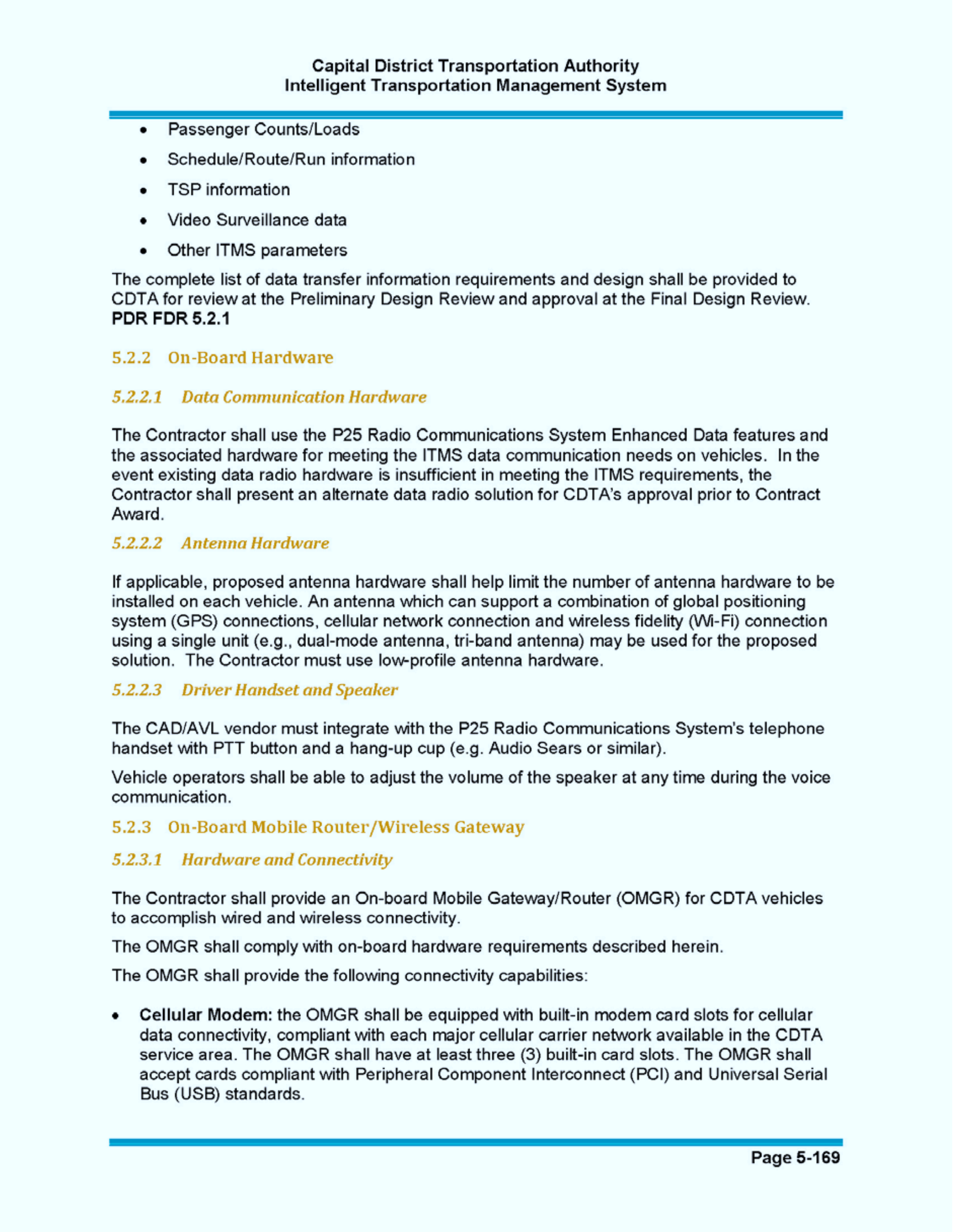
The Contractor shall provide design documentation and demonstrations for the integration of the new P25 radio communications system for data radio and other wireless data communications requirements for CDTA review at the Preliminary Design Review and for approval at the Final Design Review. **PDR FDR 5.1**

5.2 Wireless Data Communications

5.2.1 Data Transfer

The Contractor shall describe the ITMS data communications between the CDS and all other ITMS systems, equipment, components, and devices (e.g. the mobile systems on vehicles). Data communications at stations/stops, and/or Kiosks shall be provided through an established commercial cellular service provider. The types of data to be communicated shall include, at minimum:

- AVL/VLU real-time location data (utilizing appropriate polling rates to satisfy the functional requirements defined herein)
- Real-time passenger information – predicted arrival times
- Text/Canned messages
- Covert Alarms
- Vehicle diagnostics



- Passenger Counts/Loads
- Schedule/Route/Run information
- TSP information
- Video Surveillance data
- Other ITMS parameters

The complete list of data transfer information requirements and design shall be provided to CDTA for review at the Preliminary Design Review and approval at the Final Design Review. **PDR FDR 5.2.1**

5.2.2 On-Board Hardware

5.2.2.1 Data Communication Hardware

The Contractor shall use the P25 Radio Communications System Enhanced Data features and the associated hardware for meeting the ITMS data communication needs on vehicles. In the event existing data radio hardware is insufficient in meeting the ITMS requirements, the Contractor shall present an alternate data radio solution for CDTA's approval prior to Contract Award.

5.2.2.2 Antenna Hardware

If applicable, proposed antenna hardware shall help limit the number of antenna hardware to be installed on each vehicle. An antenna which can support a combination of global positioning system (GPS) connections, cellular network connection and wireless fidelity (Wi-Fi) connection using a single unit (e.g., dual-mode antenna, tri-band antenna) may be used for the proposed solution. The Contractor must use low-profile antenna hardware.

5.2.2.3 Driver Handset and Speaker

The CAD/AVL vendor must integrate with the P25 Radio Communications System's telephone handset with PTT button and a hang-up cup (e.g. Audio Sears or similar).

Vehicle operators shall be able to adjust the volume of the speaker at any time during the voice communication.

5.2.3 On-Board Mobile Router/Wireless Gateway

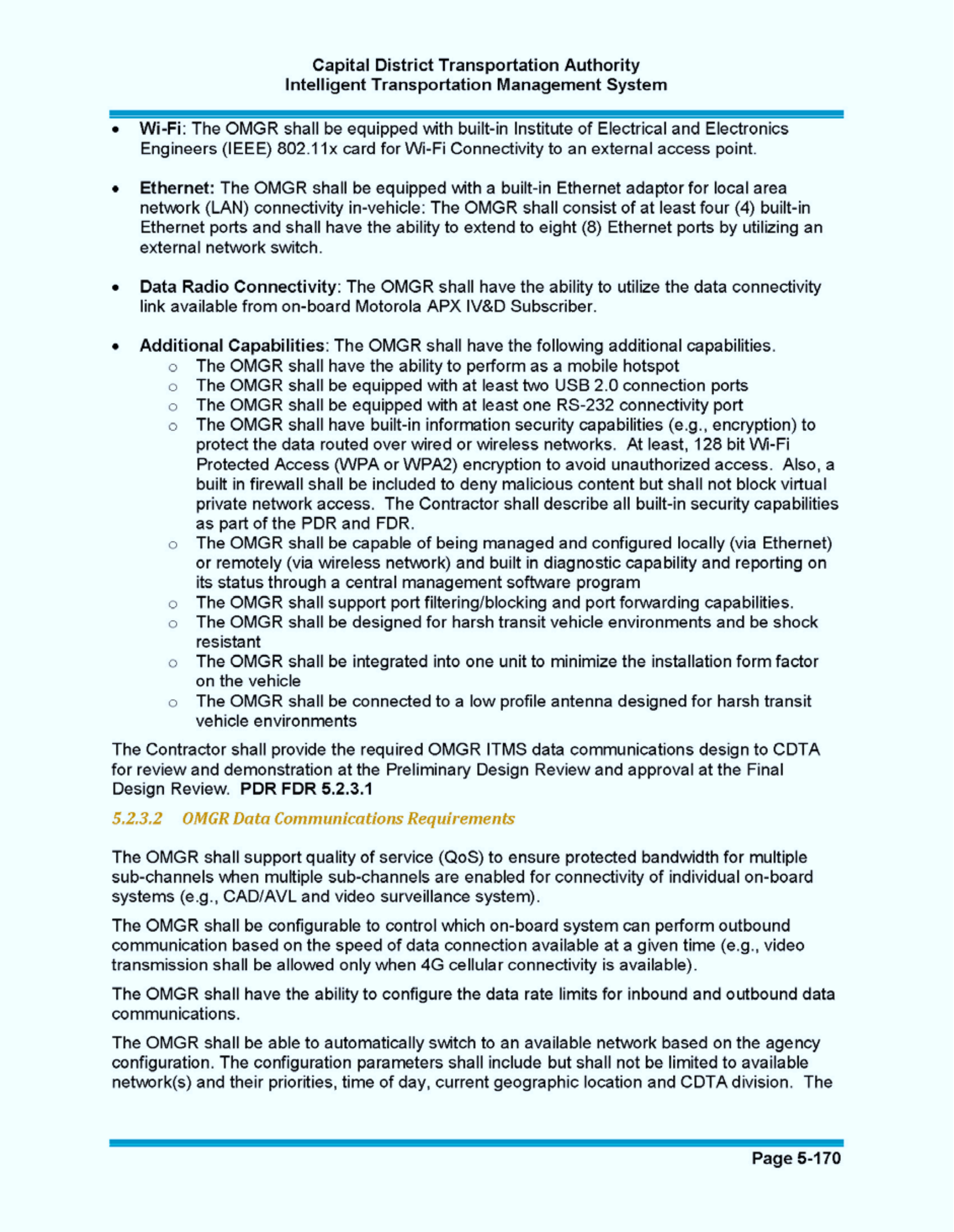
5.2.3.1 Hardware and Connectivity

The Contractor shall provide an On-board Mobile Gateway/Router (OMGR) for CDTA vehicles to accomplish wired and wireless connectivity.

The OMGR shall comply with on-board hardware requirements described herein.

The OMGR shall provide the following connectivity capabilities:

- **Cellular Modem:** the OMGR shall be equipped with built-in modem card slots for cellular data connectivity, compliant with each major cellular carrier network available in the CDTA service area. The OMGR shall have at least three (3) built-in card slots. The OMGR shall accept cards compliant with Peripheral Component Interconnect (PCI) and Universal Serial Bus (USB) standards.



- **Wi-Fi**: The OMGR shall be equipped with built-in Institute of Electrical and Electronics Engineers (IEEE) 802.11x card for Wi-Fi Connectivity to an external access point.

- **Ethernet:** The OMGR shall be equipped with a built-in Ethernet adaptor for local area network (LAN) connectivity in-vehicle: The OMGR shall consist of at least four (4) built-in Ethernet ports and shall have the ability to extend to eight (8) Ethernet ports by utilizing an external network switch.

- **Data Radio Connectivity**: The OMGR shall have the ability to utilize the data connectivity link available from on-board Motorola APX IV&D Subscriber.

- **Additional Capabilities**: The OMGR shall have the following additional capabilities.
    - The OMGR shall have the ability to perform as a mobile hotspot
    - The OMGR shall be equipped with at least two USB 2.0 connection ports
    - The OMGR shall be equipped with at least one RS-232 connectivity port
    - The OMGR shall have built-in information security capabilities (e.g., encryption) to protect the data routed over wired or wireless networks. At least, 128 bit Wi-Fi Protected Access (WPA or WPA2) encryption to avoid unauthorized access. Also, a built in firewall shall be included to deny malicious content but shall not block virtual private network access. The Contractor shall describe all built-in security capabilities as part of the PDR and FDR.
    - The OMGR shall be capable of being managed and configured locally (via Ethernet) or remotely (via wireless network) and built in diagnostic capability and reporting on its status through a central management software program
    - The OMGR shall support port filtering/blocking and port forwarding capabilities.
    - The OMGR shall be designed for harsh transit vehicle environments and be shock resistant
    - The OMGR shall be integrated into one unit to minimize the installation form factor on the vehicle
    - The OMGR shall be connected to a low profile antenna designed for harsh transit vehicle environments

The Contractor shall provide the required OMGR ITMS data communications design to CDTA for review and demonstration at the Preliminary Design Review and approval at the Final Design Review. **PDR FDR 5.2.3.1**

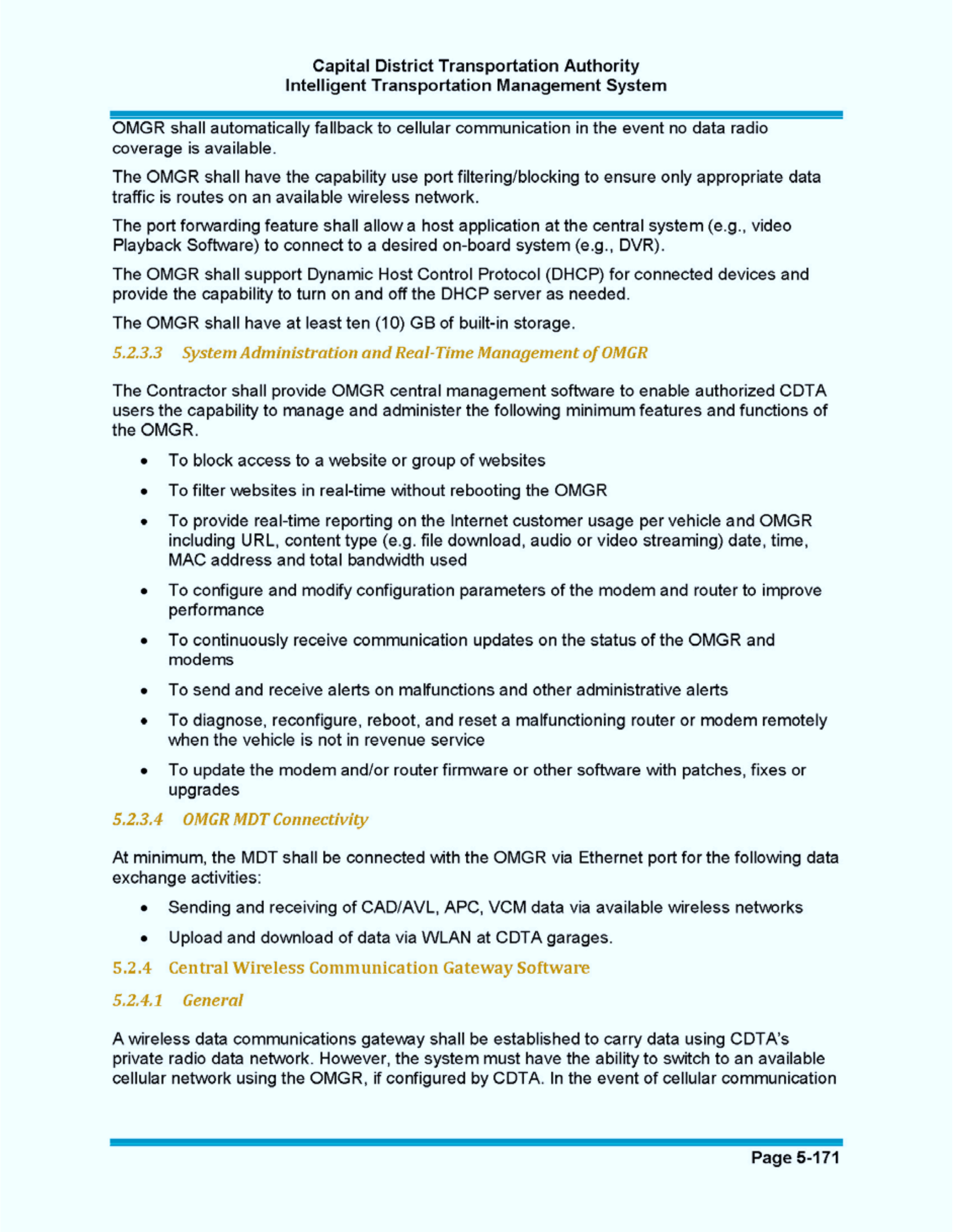
5.2.3.2 OMGR Data Communications Requirements

The OMGR shall support quality of service (QoS) to ensure protected bandwidth for multiple sub-channels when multiple sub-channels are enabled for connectivity of individual on-board systems (e.g., CAD/AVL and video surveillance system).

The OMGR shall be configurable to control which on-board system can perform outbound communication based on the speed of data connection available at a given time (e.g., video transmission shall be allowed only when 4G cellular connectivity is available).

The OMGR shall have the ability to configure the data rate limits for inbound and outbound data communications.

The OMGR shall be able to automatically switch to an available network based on the agency configuration. The configuration parameters shall include but shall not be limited to available network(s) and their priorities, time of day, current geographic location and CDTA division. The



OMGR shall automatically fallback to cellular communication in the event no data radio coverage is available.

The OMGR shall have the capability use port filtering/blocking to ensure only appropriate data traffic is routes on an available wireless network.

The port forwarding feature shall allow a host application at the central system (e.g., video Playback Software) to connect to a desired on-board system (e.g., DVR).

The OMGR shall support Dynamic Host Control Protocol (DHCP) for connected devices and provide the capability to turn on and off the DHCP server as needed.

The OMGR shall have at least ten (10) GB of built-in storage.

5.2.3.3 System Administration and Real-Time Management of OMGR

The Contractor shall provide OMGR central management software to enable authorized CDTA users the capability to manage and administer the following minimum features and functions of the OMGR.

- To block access to a website or group of websites
- To filter websites in real-time without rebooting the OMGR
- To provide real-time reporting on the Internet customer usage per vehicle and OMGR including URL, content type (e.g. file download, audio or video streaming) date, time, MAC address and total bandwidth used
- To configure and modify configuration parameters of the modem and router to improve performance
- To continuously receive communication updates on the status of the OMGR and modems
- To send and receive alerts on malfunctions and other administrative alerts
- To diagnose, reconfigure, reboot, and reset a malfunctioning router or modem remotely when the vehicle is not in revenue service
- To update the modem and/or router firmware or other software with patches, fixes or upgrades

5.2.3.4 OMGR MDT Connectivity

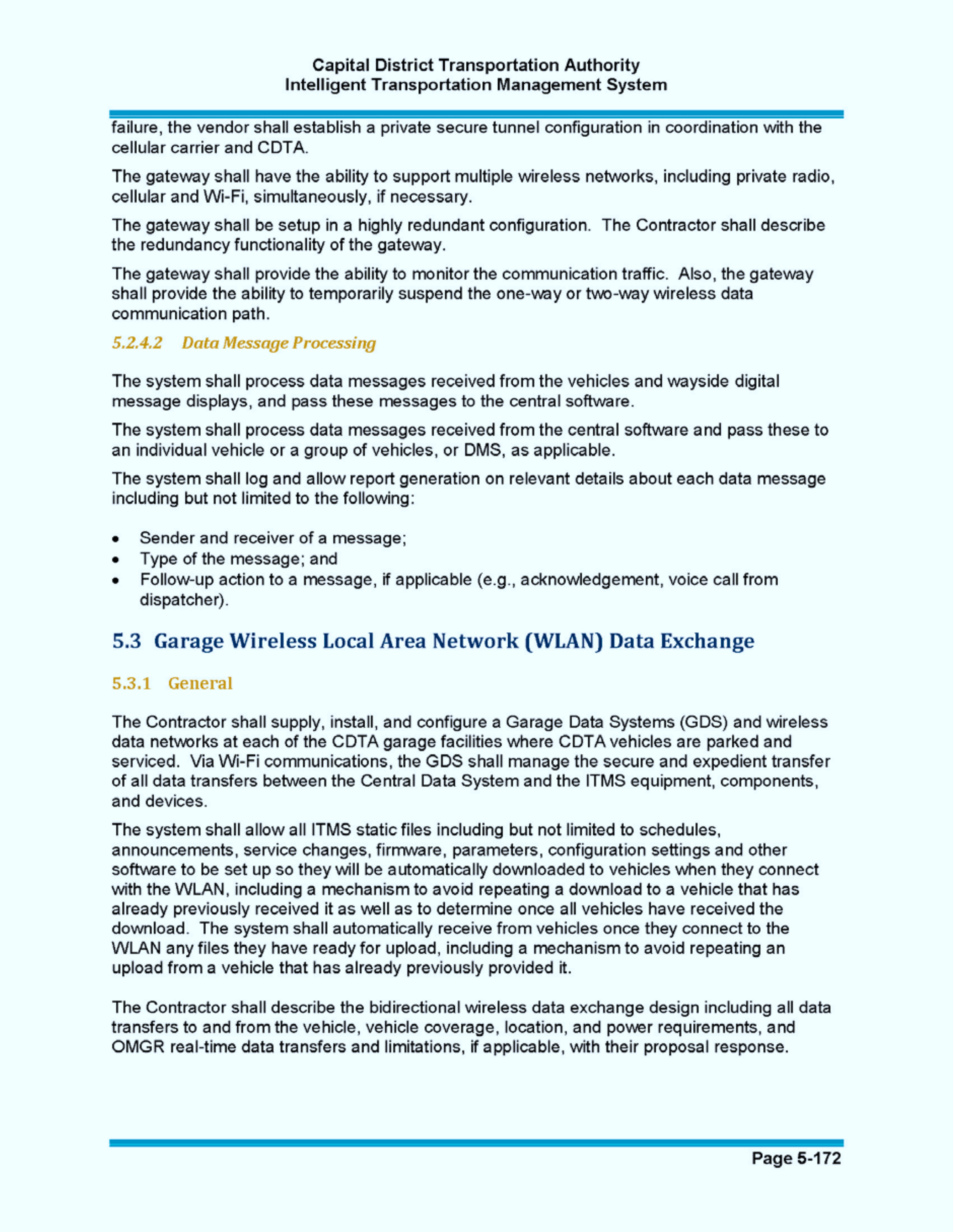
At minimum, the MDT shall be connected with the OMGR via Ethernet port for the following data exchange activities:

- Sending and receiving of CAD/AVL, APC, VCM data via available wireless networks
- Upload and download of data via WLAN at CDTA garages.

5.2.4 Central Wireless Communication Gateway Software

5.2.4.1 General

A wireless data communications gateway shall be established to carry data using CDTA's private radio data network. However, the system must have the ability to switch to an available cellular network using the OMGR, if configured by CDTA. In the event of cellular communication



failure, the vendor shall establish a private secure tunnel configuration in coordination with the cellular carrier and CDTA.

The gateway shall have the ability to support multiple wireless networks, including private radio, cellular and Wi-Fi, simultaneously, if necessary.

The gateway shall be setup in a highly redundant configuration. The Contractor shall describe the redundancy functionality of the gateway.

The gateway shall provide the ability to monitor the communication traffic. Also, the gateway shall provide the ability to temporarily suspend the one-way or two-way wireless data communication path.

5.2.4.2 Data Message Processing

The system shall process data messages received from the vehicles and wayside digital message displays, and pass these messages to the central software.

The system shall process data messages received from the central software and pass these to an individual vehicle or a group of vehicles, or DMS, as applicable.

The system shall log and allow report generation on relevant details about each data message including but not limited to the following:

- Sender and receiver of a message;
- Type of the message; and
- Follow-up action to a message, if applicable (e.g., acknowledgement, voice call from dispatcher).

5.3 Garage Wireless Local Area Network (WLAN) Data Exchange

5.3.1 General

The Contractor shall supply, install, and configure a Garage Data Systems (GDS) and wireless data networks at each of the CDTA garage facilities where CDTA vehicles are parked and serviced. Via Wi-Fi communications, the GDS shall manage the secure and expedient transfer of all data transfers between the Central Data System and the ITMS equipment, components, and devices.

The system shall allow all ITMS static files including but not limited to schedules, announcements, service changes, firmware, parameters, configuration settings and other software to be set up so they will be automatically downloaded to vehicles when they connect with the WLAN, including a mechanism to avoid repeating a download to a vehicle that has already previously received it as well as to determine once all vehicles have received the download. The system shall automatically receive from vehicles once they connect to the WLAN any files they have ready for upload, including a mechanism to avoid repeating an upload from a vehicle that has already previously provided it.

The Contractor shall describe the bidirectional wireless data exchange design including all data transfers to and from the vehicle, vehicle coverage, location, and power requirements, and OMGR real-time data transfers and limitations, if applicable, with their proposal response.

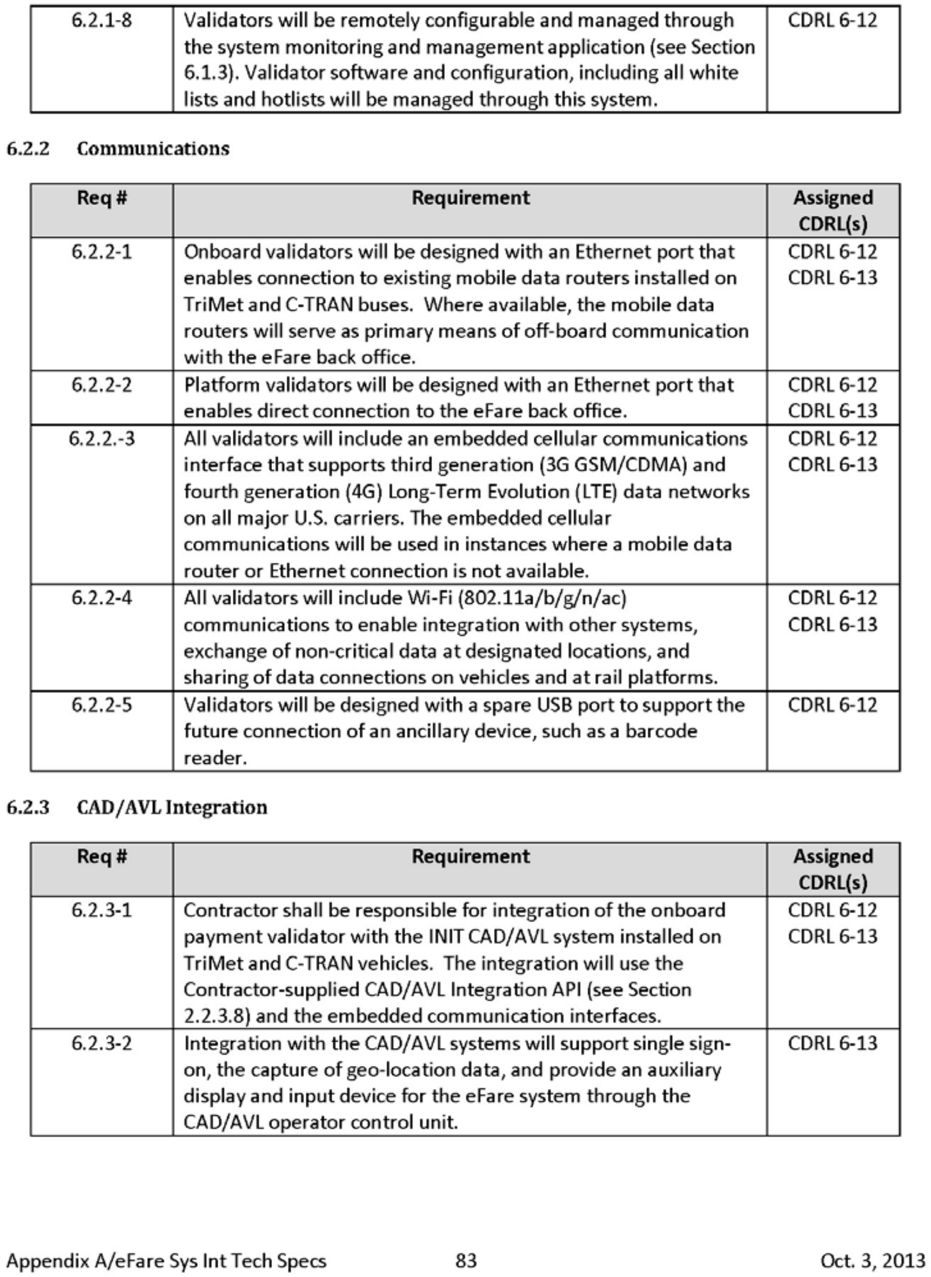
2.3. Tri-County Metropolitan Transportation District of Oregon (TriMet) Hop Fastpass – Portland, OR

"The Tri-County Metropolitan Transportation District of Oregon (TriMet), the primary public transportation provider in Portland, [Oregon] utilized a novel approach to build the Hop Fastpass, its public transit payment system that first launched in 2017 and has steadily added new features."[2]

The next four pages show relevant portions of the specifications. The conceptual system diagram is shown on the page following the relevant portion of the specifications.

Another key requirement in the specifications is as follows: "The eFare system will be built using an account-based, open payment architecture with key system interfaces based on Application Programming Interfaces (APIs) that are published by the Contractor and fully owned or licensed by TriMet."

[2] APTA MOBILITY INNOVATION PILOT OF THE MONTH: TriMet's Hop Fastpass—Open Architecture in Fare Payment, webinar conducted on June 27, 2019



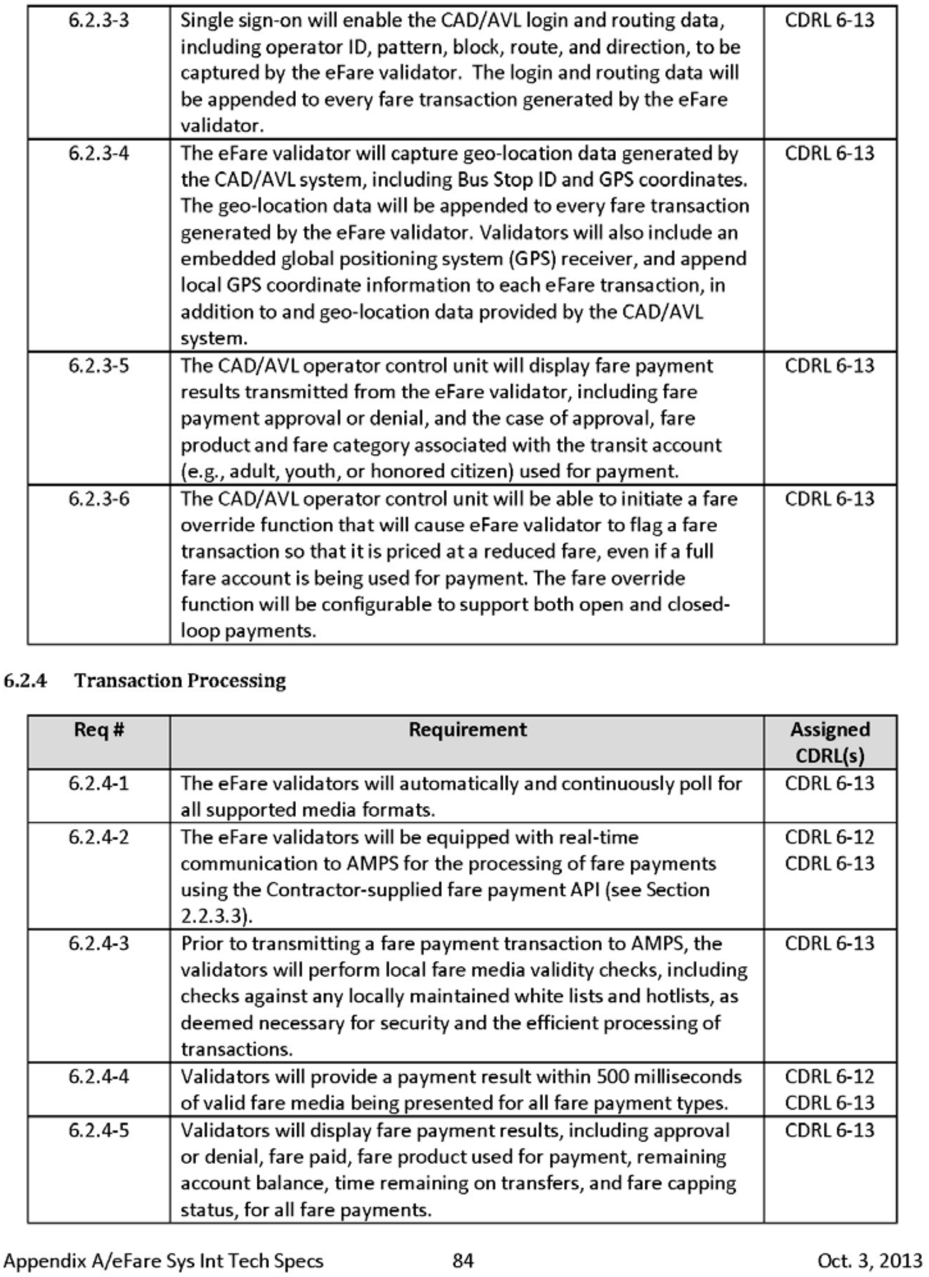
6.2.1-8	Validators will be remotely configurable and managed through the system monitoring and management application (see Section 6.1.3). Validator software and configuration, including all white lists and hotlists will be managed through this system.	CDRL 6-12

6.2.2 Communications

Req #	Requirement	Assigned CDRL(s)
6.2.2-1	Onboard validators will be designed with an Ethernet port that enables connection to existing mobile data routers installed on TriMet and C-TRAN buses. Where available, the mobile data routers will serve as primary means of off-board communication with the eFare back office.	CDRL 6-12 CDRL 6-13
6.2.2-2	Platform validators will be designed with an Ethernet port that enables direct connection to the eFare back office.	CDRL 6-12 CDRL 6-13
6.2.2.-3	All validators will include an embedded cellular communications interface that supports third generation (3G GSM/CDMA) and fourth generation (4G) Long-Term Evolution (LTE) data networks on all major U.S. carriers. The embedded cellular communications will be used in instances where a mobile data router or Ethernet connection is not available.	CDRL 6-12 CDRL 6-13
6.2.2-4	All validators will include Wi-Fi (802.11a/b/g/n/ac) communications to enable integration with other systems, exchange of non-critical data at designated locations, and sharing of data connections on vehicles and at rail platforms.	CDRL 6-12 CDRL 6-13
6.2.2-5	Validators will be designed with a spare USB port to support the future connection of an ancillary device, such as a barcode reader.	CDRL 6-12

6.2.3 CAD/AVL Integration

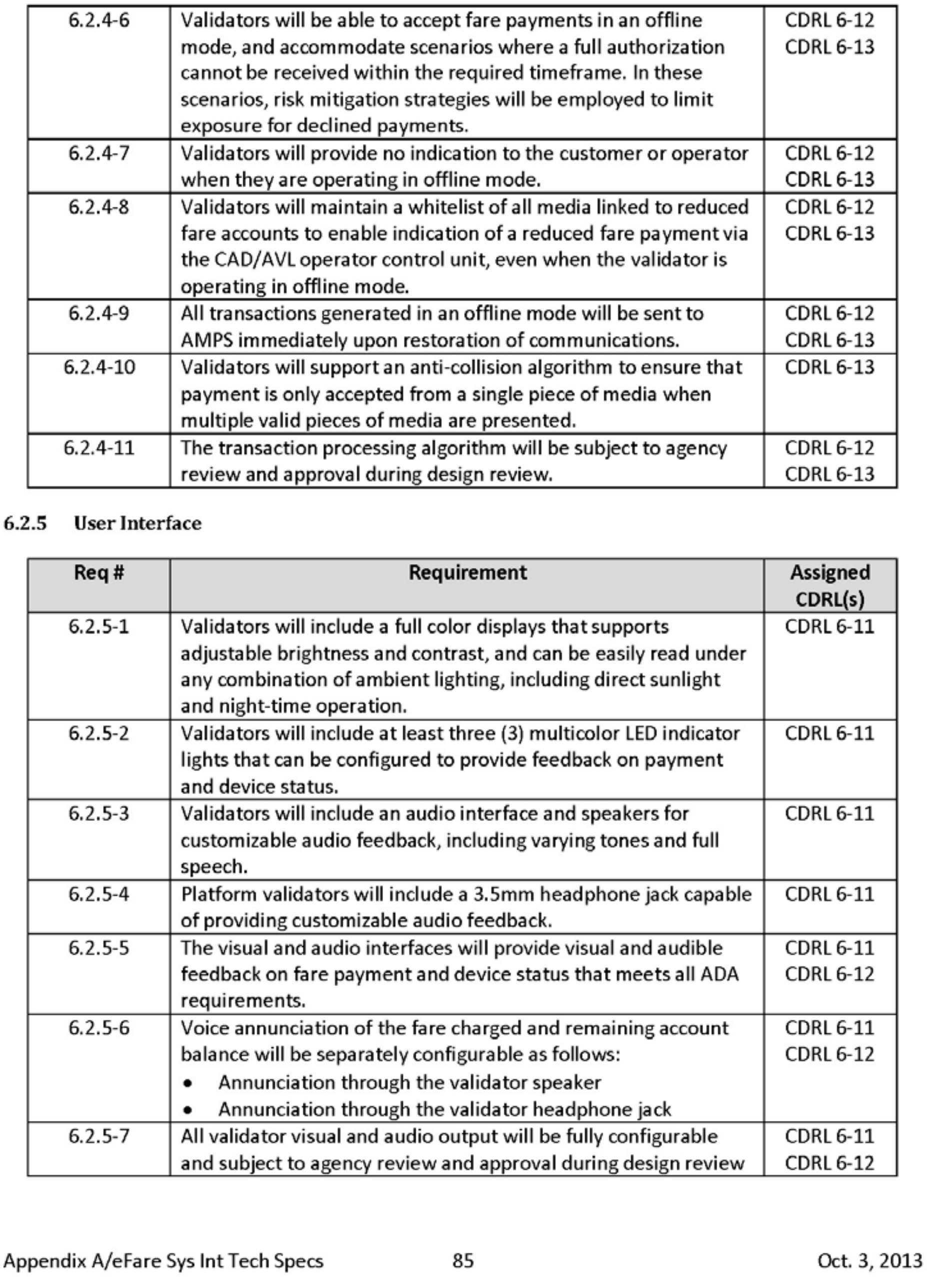
Req #	Requirement	Assigned CDRL(s)
6.2.3-1	Contractor shall be responsible for integration of the onboard payment validator with the INIT CAD/AVL system installed on TriMet and C-TRAN vehicles. The integration will use the Contractor-supplied CAD/AVL Integration API (see Section 2.2.3.8) and the embedded communication interfaces.	CDRL 6-12 CDRL 6-13
6.2.3-2	Integration with the CAD/AVL systems will support single sign-on, the capture of geo-location data, and provide an auxiliary display and input device for the eFare system through the CAD/AVL operator control unit.	CDRL 6-13



6.2.3-3	Single sign-on will enable the CAD/AVL login and routing data, including operator ID, pattern, block, route, and direction, to be captured by the eFare validator. The login and routing data will be appended to every fare transaction generated by the eFare validator.	CDRL 6-13
6.2.3-4	The eFare validator will capture geo-location data generated by the CAD/AVL system, including Bus Stop ID and GPS coordinates. The geo-location data will be appended to every fare transaction generated by the eFare validator. Validators will also include an embedded global positioning system (GPS) receiver, and append local GPS coordinate information to each eFare transaction, in addition to and geo-location data provided by the CAD/AVL system.	CDRL 6-13
6.2.3-5	The CAD/AVL operator control unit will display fare payment results transmitted from the eFare validator, including fare payment approval or denial, and the case of approval, fare product and fare category associated with the transit account (e.g., adult, youth, or honored citizen) used for payment.	CDRL 6-13
6.2.3-6	The CAD/AVL operator control unit will be able to initiate a fare override function that will cause eFare validator to flag a fare transaction so that it is priced at a reduced fare, even if a full fare account is being used for payment. The fare override function will be configurable to support both open and closed-loop payments.	CDRL 6-13

6.2.4 Transaction Processing

Req #	Requirement	Assigned CDRL(s)
6.2.4-1	The eFare validators will automatically and continuously poll for all supported media formats.	CDRL 6-13
6.2.4-2	The eFare validators will be equipped with real-time communication to AMPS for the processing of fare payments using the Contractor-supplied fare payment API (see Section 2.2.3.3).	CDRL 6-12 CDRL 6-13
6.2.4-3	Prior to transmitting a fare payment transaction to AMPS, the validators will perform local fare media validity checks, including checks against any locally maintained white lists and hotlists, as deemed necessary for security and the efficient processing of transactions.	CDRL 6-13
6.2.4-4	Validators will provide a payment result within 500 milliseconds of valid fare media being presented for all fare payment types.	CDRL 6-12 CDRL 6-13
6.2.4-5	Validators will display fare payment results, including approval or denial, fare paid, fare product used for payment, remaining account balance, time remaining on transfers, and fare capping status, for all fare payments.	CDRL 6-13

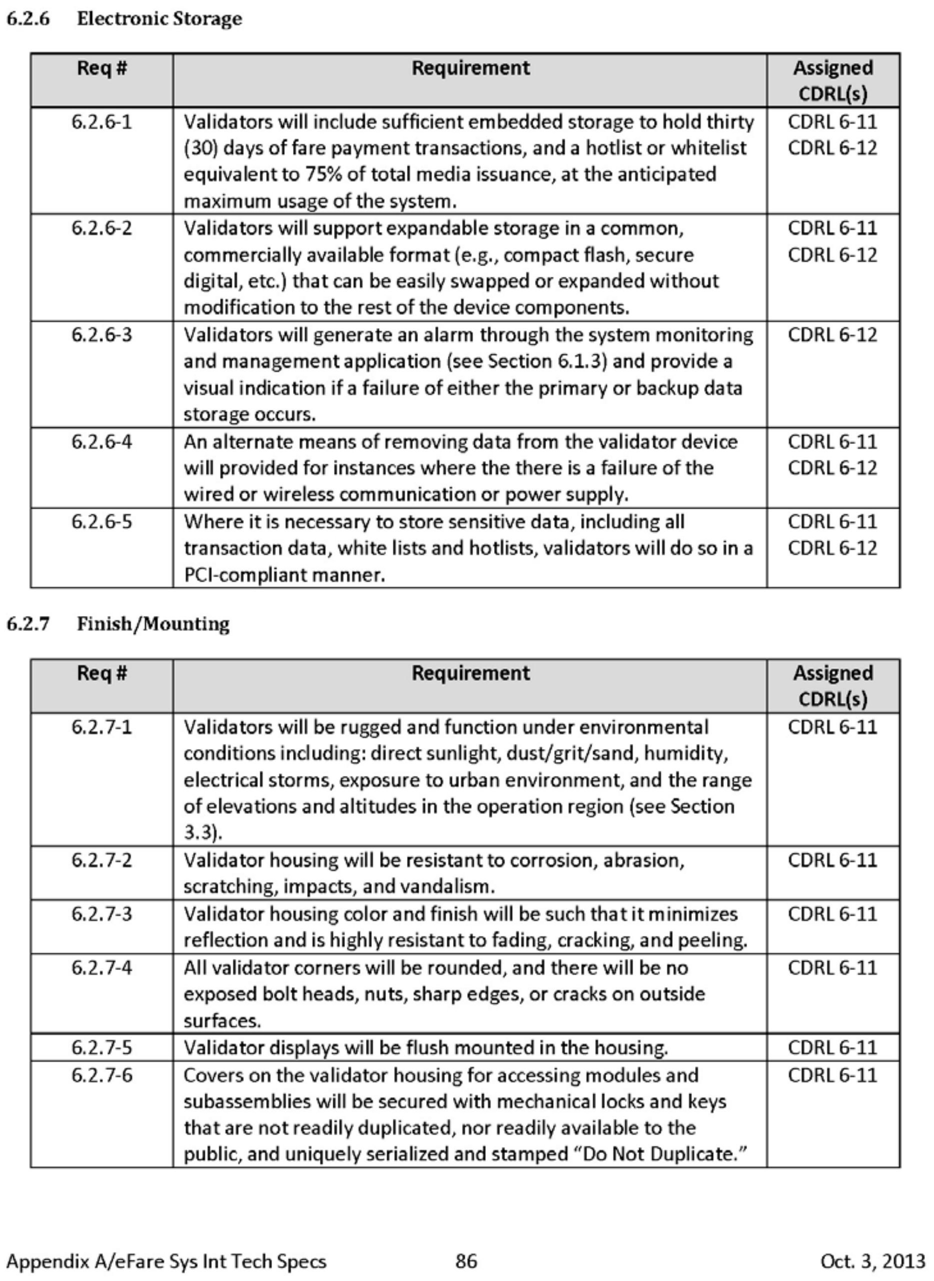


6.2.4-6	Validators will be able to accept fare payments in an offline mode, and accommodate scenarios where a full authorization cannot be received within the required timeframe. In these scenarios, risk mitigation strategies will be employed to limit exposure for declined payments.	CDRL 6-12 CDRL 6-13
6.2.4-7	Validators will provide no indication to the customer or operator when they are operating in offline mode.	CDRL 6-12 CDRL 6-13
6.2.4-8	Validators will maintain a whitelist of all media linked to reduced fare accounts to enable indication of a reduced fare payment via the CAD/AVL operator control unit, even when the validator is operating in offline mode.	CDRL 6-12 CDRL 6-13
6.2.4-9	All transactions generated in an offline mode will be sent to AMPS immediately upon restoration of communications.	CDRL 6-12 CDRL 6-13
6.2.4-10	Validators will support an anti-collision algorithm to ensure that payment is only accepted from a single piece of media when multiple valid pieces of media are presented.	CDRL 6-13
6.2.4-11	The transaction processing algorithm will be subject to agency review and approval during design review.	CDRL 6-12 CDRL 6-13

6.2.5 User Interface

Req #	Requirement	Assigned CDRL(s)
6.2.5-1	Validators will include a full color displays that supports adjustable brightness and contrast, and can be easily read under any combination of ambient lighting, including direct sunlight and night-time operation.	CDRL 6-11
6.2.5-2	Validators will include at least three (3) multicolor LED indicator lights that can be configured to provide feedback on payment and device status.	CDRL 6-11
6.2.5-3	Validators will include an audio interface and speakers for customizable audio feedback, including varying tones and full speech.	CDRL 6-11
6.2.5-4	Platform validators will include a 3.5mm headphone jack capable of providing customizable audio feedback.	CDRL 6-11
6.2.5-5	The visual and audio interfaces will provide visual and audible feedback on fare payment and device status that meets all ADA requirements.	CDRL 6-11 CDRL 6-12
6.2.5-6	Voice annunciation of the fare charged and remaining account balance will be separately configurable as follows: • Annunciation through the validator speaker • Annunciation through the validator headphone jack	CDRL 6-11 CDRL 6-12
6.2.5-7	All validator visual and audio output will be fully configurable and subject to agency review and approval during design review	CDRL 6-11 CDRL 6-12

Appendix A/eFare Sys Int Tech Specs 85 Oct. 3, 2013



6.2.6 Electronic Storage

Req #	Requirement	Assigned CDRL(s)
6.2.6-1	Validators will include sufficient embedded storage to hold thirty (30) days of fare payment transactions, and a hotlist or whitelist equivalent to 75% of total media issuance, at the anticipated maximum usage of the system.	CDRL 6-11 CDRL 6-12
6.2.6-2	Validators will support expandable storage in a common, commercially available format (e.g., compact flash, secure digital, etc.) that can be easily swapped or expanded without modification to the rest of the device components.	CDRL 6-11 CDRL 6-12
6.2.6-3	Validators will generate an alarm through the system monitoring and management application (see Section 6.1.3) and provide a visual indication if a failure of either the primary or backup data storage occurs.	CDRL 6-12
6.2.6-4	An alternate means of removing data from the validator device will provided for instances where the there is a failure of the wired or wireless communication or power supply.	CDRL 6-11 CDRL 6-12
6.2.6-5	Where it is necessary to store sensitive data, including all transaction data, white lists and hotlists, validators will do so in a PCI-compliant manner.	CDRL 6-11 CDRL 6-12

6.2.7 Finish/Mounting

Req #	Requirement	Assigned CDRL(s)
6.2.7-1	Validators will be rugged and function under environmental conditions including: direct sunlight, dust/grit/sand, humidity, electrical storms, exposure to urban environment, and the range of elevations and altitudes in the operation region (see Section 3.3).	CDRL 6-11
6.2.7-2	Validator housing will be resistant to corrosion, abrasion, scratching, impacts, and vandalism.	CDRL 6-11
6.2.7-3	Validator housing color and finish will be such that it minimizes reflection and is highly resistant to fading, cracking, and peeling.	CDRL 6-11
6.2.7-4	All validator corners will be rounded, and there will be no exposed bolt heads, nuts, sharp edges, or cracks on outside surfaces.	CDRL 6-11
6.2.7-5	Validator displays will be flush mounted in the housing.	CDRL 6-11
6.2.7-6	Covers on the validator housing for accessing modules and subassemblies will be secured with mechanical locks and keys that are not readily duplicated, nor readily available to the public, and uniquely serialized and stamped "Do Not Duplicate."	CDRL 6-11

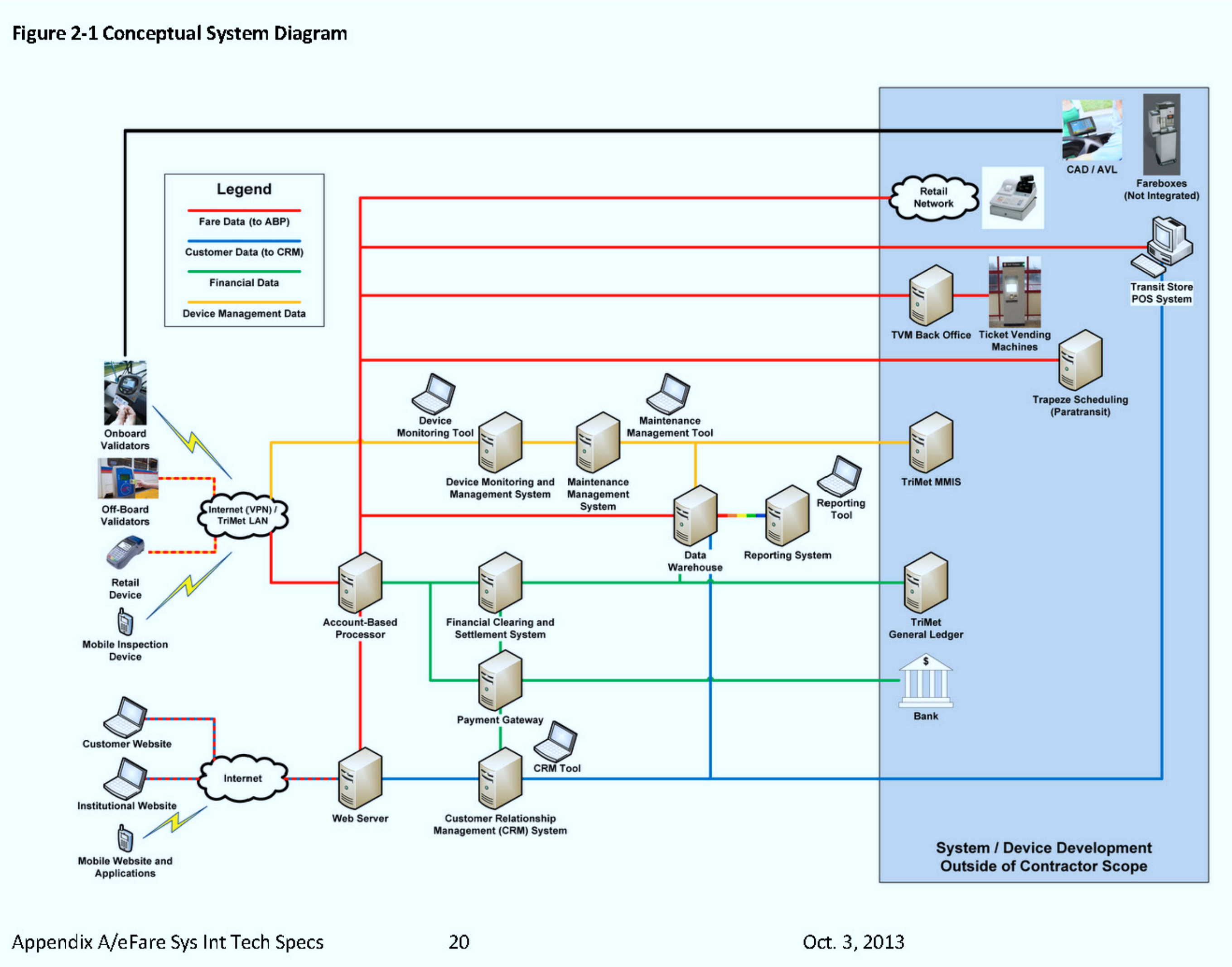


Figure 2-1 Conceptual System Diagram

Appendix A/eFare Sys Int Tech Specs 20 Oct. 3, 2013

3. Reference to Other Standards

3.1. IEEE 802.11

802.11 [and 802.11x] refers to a family of specifications developed by the IEEE for wireless [local area network] LAN (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

There are several specifications in the 802.11 family:

- 802.11 — applies to wireless LANs and provides 1 or 2 [megabits per second] Mbps transmission in the 2.4 [gigahertz] GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- 802.11a — an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- 802.11b (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- 802.11e — a wireless draft standard that defines the Quality of Service (QoS) support for LANs, and is an enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. 802.11e adds QoS features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards.
- 802.11g — applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands.
- 802.11n — 802.11n builds upon previous 802.11 standards by adding multiple-input multiple-output (MIMO). The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding schemes like Alamouti coding. The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g.
- 802.11ac — 802.11ac builds upon previous 802.11 standards, particularly the 802.11n standard, to deliver data rates of 433Mbps per spatial stream, or 1.3Gbps in a three-antenna (three stream) design. The 802.11ac specification operates only in the 5 GHz frequency range and features support for wider channels (80MHz and 160MHz) and beamforming capabilities by default to help achieve its higher wireless speeds. This standard is being used currently for new wireless access points (WAPs) in transit garages and facilities in order to upload or download data and software updates.

- 802.11ac Wave 2 — 802.11ac Wave 2 is an update for the original 802.11ac spec that uses [multiple user] MU-MIMO technology and other advancements to help increase theoretical maximum wireless speeds for the spec to 6.93 Gbps.

- 802.11ad — 802.11ad is a wireless specification under development that will operate in the 60GHz frequency band and offer much higher transfer rates than previous 802.11 specs, with a theoretical maximum transfer rate of up to 7Gbps (Gigabits per second).

- 802.11ah— Also known as Wi-Fi HaLow, 802.11ah is the first Wi-Fi specification to operate in frequency bands below one gigahertz (900 MHz), and it has a range of nearly twice that of other Wi-Fi technologies. It's also able to penetrate walls and other barriers considerably better than previous Wi-Fi standards.

- 802.11r - 802.11r, also called Fast Basic Service Set (BSS) Transition, supports VoWi-Fi handoff between access points to enable VoIP roaming on a Wi-Fi network with 802.1X authentication. [3]

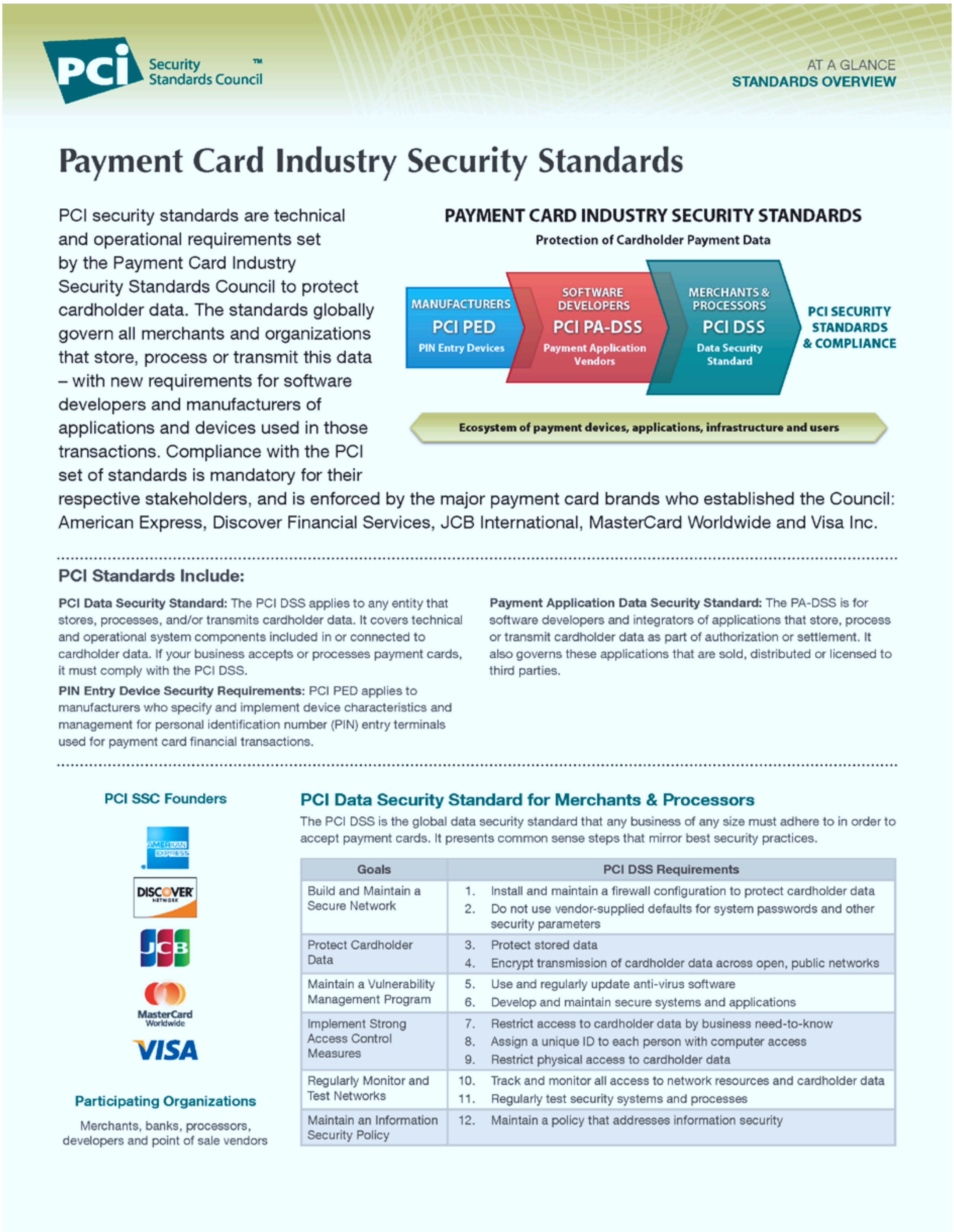
- 802.11p is one of the recent approved amendments to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE). It appended some enhancements to the latest version of 802.11 that required to support applications of Intelligent Transportation Systems (ITS). This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band.[4]

3.2. Payment Card Industry Security Standards

Information regarding these standards are shown in the next two pages.

[3] http://www.webopedia.com/TERM/8/802_11.html

[4] http://www.iaeng.org/publication/WCECS2014/WCECS2014_pp691-698.pdf



PCI Security Standards Council™

AT A GLANCE
STANDARDS OVERVIEW

Payment Card Industry Security Standards

PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process or transmit this data – with new requirements for software developers and manufacturers of applications and devices used in those transactions. Compliance with the PCI set of standards is mandatory for their respective stakeholders, and is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data

MANUFACTURERS
PCI PED
PIN Entry Devices

SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors

MERCHANTS & PROCESSORS
PCI DSS
Data Security Standard

PCI SECURITY STANDARDS & COMPLIANCE

Ecosystem of payment devices, applications, infrastructure and users

PCI Standards Include:

PCI Data Security Standard: The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. If your business accepts or processes payment cards, it must comply with the PCI DSS.

PIN Entry Device Security Requirements: PCI PED applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions.

Payment Application Data Security Standard: The PA-DSS is for software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement. It also governs these applications that are sold, distributed or licensed to third parties.

PCI SSC Founders

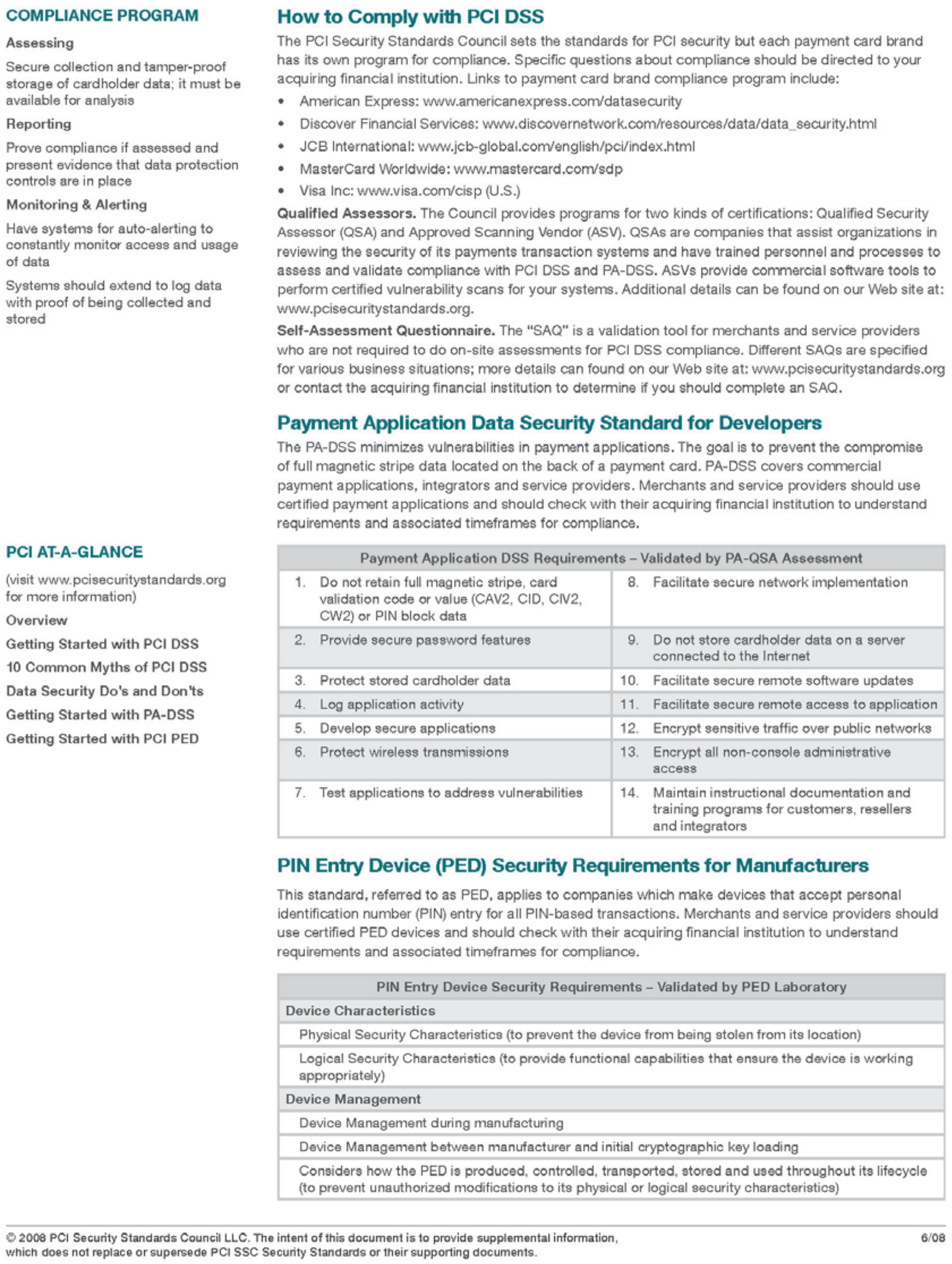
Participating Organizations

Merchants, banks, processors, developers and point of sale vendors

PCI Data Security Standard for Merchants & Processors

The PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents common sense steps that mirror best security practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security



COMPLIANCE PROGRAM

Assessing

Secure collection and tamper-proof storage of cardholder data; it must be available for analysis

Reporting

Prove compliance if assessed and present evidence that data protection controls are in place

Monitoring & Alerting

Have systems for auto-alerting to constantly monitor access and usage of data

Systems should extend to log data with proof of being collected and stored

PCI AT-A-GLANCE

(visit www.pcisecuritystandards.org for more information)

Overview

Getting Started with PCI DSS

10 Common Myths of PCI DSS

Data Security Do's and Don'ts

Getting Started with PA-DSS

Getting Started with PCI PED

How to Comply with PCI DSS

The PCI Security Standards Council sets the standards for PCI security but each payment card brand has its own program for compliance. Specific questions about compliance should be directed to your acquiring financial institution. Links to payment card brand compliance program include:

- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: www.discovernetwork.com/resources/data/data_security.html
- JCB International: www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: www.mastercard.com/sdp
- Visa Inc: www.visa.com/cisp (U.S.)

Qualified Assessors. The Council provides programs for two kinds of certifications: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs are companies that assist organizations in reviewing the security of its payments transaction systems and have trained personnel and processes to assess and validate compliance with PCI DSS and PA-DSS. ASVs provide commercial software tools to perform certified vulnerability scans for your systems. Additional details can be found on our Web site at: www.pcisecuritystandards.org.

Self-Assessment Questionnaire. The "SAQ" is a validation tool for merchants and service providers who are not required to do on-site assessments for PCI DSS compliance. Different SAQs are specified for various business situations; more details can found on our Web site at: www.pcisecuritystandards.org or contact the acquiring financial institution to determine if you should complete an SAQ.

Payment Application Data Security Standard for Developers

The PA-DSS minimizes vulnerabilities in payment applications. The goal is to prevent the compromise of full magnetic stripe data located on the back of a payment card. PA-DSS covers commercial payment applications, integrators and service providers. Merchants and service providers should use certified payment applications and should check with their acquiring financial institution to understand requirements and associated timeframes for compliance.

Payment Application DSS Requirements – Validated by PA-QSA Assessment	
1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CIV2, CVV2) or PIN block data	8. Facilitate secure network implementation
2. Provide secure password features	9. Do not store cardholder data on a server connected to the Internet
3. Protect stored cardholder data	10. Facilitate secure remote software updates
4. Log application activity	11. Facilitate secure remote access to application
5. Develop secure applications	12. Encrypt sensitive traffic over public networks
6. Protect wireless transmissions	13. Encrypt all non-console administrative access
7. Test applications to address vulnerabilities	14. Maintain instructional documentation and training programs for customers, resellers and integrators

PIN Entry Device (PED) Security Requirements for Manufacturers

This standard, referred to as PED, applies to companies which make devices that accept personal identification number (PIN) entry for all PIN-based transactions. Merchants and service providers should use certified PED devices and should check with their acquiring financial institution to understand requirements and associated timeframes for compliance.

PIN Entry Device Security Requirements – Validated by PED Laboratory
Device Characteristics
Physical Security Characteristics (to prevent the device from being stolen from its location)
Logical Security Characteristics (to provide functional capabilities that ensure the device is working appropriately)
Device Management
Device Management during manufacturing
Device Management between manufacturer and initial cryptographic key loading
Considers how the PED is produced, controlled, transported, stored and used throughout its lifecycle (to prevent unauthorized modifications to its physical or logical security characteristics)

6/08

4. Case Studies

There are no new case studies in this module in addition to the following three presented in the module:

- Case study of procuring and implementing CAD/AVL system using a mobile router/ wireless gateway as part of the Capital District Transportation Authority (CDTA) (Albany, NY) Intelligent Transportation Management System (ITMS)
- Case study of procuring system requiring on-board integration and transaction processing as part of the Tri-County Metropolitan Transportation District of Oregon (TriMet) (Portland, OR) Hop Fastpass
- Case study of migrating to using current communication technology at Alameda-Contra Costa Transit District (AC Transit) in Oakland, CA

5. Glossary

Term	Definition
Automatic vehicle location (AVL)	The central software used by dispatchers for operations management that periodically receives real-time updates on fleet vehicle locations. In most modern AVL systems this involves an onboard computer with an integrated Global Positioning System receiver and mobile data communications capability.
Computer-aided Dispatch (CAD)	CAD software integrates transit operations by giving transit dispatchers and supervisors' decision support tools to manage the operating environment.
Global System for Mobile communication (GSM)	GSM is a digital mobile network that is widely used by mobile phone users in Europe and other parts of the world. GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot.
Infrastructure as a Service (IaaS)	Cloud layer offering that enables a self-service model for managing virtualized data center infrastructure. Customers pay for on-demand access to pre-configured computing resources, such as network, storage, and operating systems.
Internet of Things (IoT)	The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.
Internet Protocol (IP)	A set of rules governing the format of data sent over the Internet or other network.
Long Term Evolution (LTE)	LTE is a standard for 4G wireless broadband technology that offers increased network capacity and speed to mobile device users. It also provides reduced latency, scalable bandwidth capacity and backward-compatibility with existing GSM and UMTS technology.

Term	Definition
Mobile Gateway Router (MGR) [also known as On-board MGR and mobile access router]	Wireless gateways work in the cellular radio space and add intelligence to the activity of connecting a device to the internet. They will translate a private local IP to a public network IP assigned by the cellular service carrier. The gateway connects a local private device or local private network to the carrier's public network and the internet. Mobile gateway routers perform all the functions of a wireless gateway, and add sophisticated routing capabilities as well as multiple Ethernet and/or WLAN connections. These capabilities involve port forwarding or mapping and port routing. The single public IP assigned from the carrier may be mapped in the router so that one port of the single public IP is mapped to a camera, another to a sensor, and another to manage the router, and another to a locally connected network for web access. Often these two devices can be combined into one and referred to as an on-board mobile gateway router (OMGR).
Open Systems Interconnection (OSI)	The OSI model is a conceptual framework that describes the functions of a networking or telecommunication system.
Platform as a Service (PaaS)	Cloud layer offering that provides tools and other computing infrastructure, enabling organizations to focus on building and running web applications and services. PaaS environments primarily support developers, operations, and hybrid teams.
Quality of service (QoS)	QoS is a family of evolving Internet standards that provides ways to give preferential treatment to certain types of Internet Protocol (IP) traffic.
Software as a Service (SaaS)	Applications hosted by a third party and usually delivered as software services over a web browser that is accessed on the client's side.
Transit signal priority (TSP)	TSP is a general term for a set of operational improvements that use technology to reduce dwell time at traffic signals for transit vehicles by holding green lights longer or shortening red lights.
Universal Mobile Telecommunications Service (UMTS)	UMTS is a third-generation (3G) broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps).
Vehicle logic unit (VLU)	Typically, the VLU within the mobile data terminal (MDT) provides the processing power needed to support automation, single point log-on, and other onboard transit ITS applications.
Wide area network (WAN)	A computer network in which the computers connected may be far apart, generally having a radius of half a mile or more.

6. References

- Module 19 **On-board Transit Management Systems for Buses**. Module 19 can be found at https://www.pcb.its.dot.gov/StandardsTraining/modtransit19/ppt/mt19ppt.pdf

- Anthony Incorvati, Axis Communication, "Innovations in IP Video," presented at APTA BUS 2018, May 8, 2018.

- https://usatcorp.com/faqs/difference-wireless-modem-wireless-gateway-wireless-router/

- https://usatcorp.com/faqs/difference-wireless-modem-wireless-gateway-wireless-router/

- Don Murphy, IBI Group, "Emerging On-board Transit Architectures & Implications: An Exciting Opportunity," presentation at the 2018 ITS California Annual Meeting

- Metro Transit Agency Keeps GPS Connected for Accurate Real-Time Information," Cradlepoint Case Study, https://web-qa.cradlepoint.com/sites/default/files/valley-ride-cs-3.pdf

- Elliot Hubbard, DKS, "The Next Generation of Transit Signal Priority: Cloud Computing and the TSP-as-a-Service Model," presented at the 2017 ITS California Annual Meeting

- "Next Generation Bus Signal Priority," by Ed Alegre, Los Angeles County Metropolitan Transportation Authority (LA Metro) at an ITS California Meeting

- APTA MOBILITY INNOVATION PILOT OF THE MONTH: TriMet's Hop Fastpass—Open Architecture in Fare Payment, webinar conducted on June 27, 2019

- "Portland/Vancouver eFare System Integrator Technical Specifications," Oct. 3, 2013

- "The role of connectivity in overhauling bus operations and improving rider experience," Intelligent Transport, September 3, 2019 issue, pp. 48-50

- Ahsan Baig, Chief Information and Technology Officer, Alameda-Contra Costa Transit District "Connected Bus - Digital Journey For Analog Voice," presentation at 2019 ITS California Annual Meeting, September 9-11, 2019, Los Angeles, CA

- Portland Bureau of Transportation, Ubiquitous Mobility for Portland, Proposal for U.S. Department of Transportation Beyond Traffic: The Smart City Challenge, Volume 1: Technical Application, May 24, 2016

- Shaheen, Susan, PhD; Totte, Hannah and Stocker, Adam, "Future of Mobility White Paper," https://escholarship.org/uc/item/68g2h1qv, 2018, DOI: 10.7922/G2WH2N5D

- Virginia Tech Transportation Institute (VTTI), University of Virginia (UVA) Center for Transportation Studies and Morgan State University (MSU), "Applications of Connected Vehicle Infrastructure Technologies to Enhance Transit Service Efficiency and Safety," prepared for the

Research and Innovative Technology Administration (RITA); U.S. Department of Transportation (US DOT), September 30, 2016

- Gabriel Lopez-Bernal, Carol Schweiger, Amy Jacobi and John L. Craig, Transit Traveler Information Infrastructure Mobility Application: Operational Concept, prepared for USDOT ITS-Joint Program Office, June 2015

- "'INFOtransit': The future of onboard communications," July 1, 2017 Posted in https://busride.com/category/transit/

- "Utah Transit Authority Improves Operations and the Passenger Experience for 2 Million Residents," Sierra Wireless Case Study

- Salem Area Mass Transit District Request for Proposal RFP 19-001, Intelligent Transportation System (Comprehensive CAD/AVL)

- Steven E. Polzin, Ph.D., "Implications to Public Transportation of Emerging Technologies," prepared for National Center for Transit Research, November 2016

- Steve Mazur, "Mission Critical Communications for Transportation," Digi Blog, October 11, 2018, https://www.digi.com/

- DKS Associates, "The Next Generation of Transit Signal Priority: Cloud Computing and the TSP-as-a-Service Model," 2017 ITS California Annual Meeting, September 20, 2017

- Sierra Wireless, "Utah Transit Authority Improves Operations and the Passenger Experience for 2 Million Residents," Case Study, June 22, 2016

- Capital District Transportation Authority (CDTA) Request for Proposals (RFP), "Intelligent Transportation Management System (ITMS)," Proposal Number: CDTA IT-57-1000

- Digi, "Making the Connection in Transportation: How Transit Operators Can Consolidate Cellular Connectivity for Smarter, Safer, and More Efficient Operations," White Paper

- Ed Alegre, LA Metro, "Multi Modal Planning and Piloting Connected Vehicles in the Los Angeles Region," 2018 ITS CA Annual Conference and Exhibition

- Lilee Systems, "TransAir™ STS-1020: Our Most Powerful Gateway," https://www.lileesystems.com/sts/

7. Study Questions

Which one of these differences between SAE J1939 and J1708 is NOT true?

Answer Choices:

a) J1939 is much faster than J1708

b) J1939 permits a connection of more devices than J1708

c) J1939 is based on the Controller Area Network (CAN)

d) J1939 covers the same number of OSI layers as J1708

What is the difference between Generation 1.5 and 2.0 of on-board architectures?

Answer Choices:

a) The mobile gateway router (MGR) was introduced in Generation 2

b) Not all on-board devices are IP-ready in Generation 1.5

c) On-board analytics & “smarts” stay on-board in Generation 2

d) Ethernet is no longer used in Generation 2

CDTA’s selection of an On-board Mobile Router/Wireless Gateway included which considerations?

Answer Choices:

a) Need to operate both private and public networks for internal data transfer and public Wi-Fi

b) Flexibility to handle multiple inputs, antennae and multiple SIM cards for redundancy

c) Hardware needed to be already deployed and proven to be reliable

d) All of the above

Which one of these benefits has been experienced by AC Transit due to their implementation of multiple technology communications?

Answer Choices:

a) Limit service area coverage

b) Provide a path for technology evolution

c) Eliminate LMR assets

d) Reduce the number of FCC licenses

Icons to be used in ITS PCB Standards Training PowerPoints

A key of these icons that may be found in the PowerPoint presentations.

1) **Background information:** General knowledge that is available elsewhere and is outside the module being presented. This will be used primarily in the beginning of slide set when reviewing information readers are expected to already know.

2) **Tools/Applications:** An industry-specific item a person would use to accomplish a specific task, and applying that tool to fit your need.

3) **Remember:** Used when referencing something already discussed in the module that is necessary to recount.

4) **Refer to Student Supplement:** Items or information that are further explained/detailed in the Student Supplement.

SUPPLEMENT

5) **Example:** Can be real-world (case study), hypothetical, a sample of a table, etc.

Checklist: Use to indicate a process that is being laid out sequentially.