Common Payment System (CPS) System Requirements

for the Smart Columbus Demonstration Program

FINAL REPORT | December 19, 2018

Produced by City of Columbus

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Acknowledgement of Support

This material is based upon work supported by the U.S. Department of Transportation under Agreement No. DTFH6116H00013.

Disclaimer

Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the Author(s) and do not necessarily reflect the view of the U.S. Department of Transportation.

Table of Contents

List of Tables

List of Figures

Chapter 1. Introduction

This Systems Requirements Specification (SyRS) is intended to communicate the requirements of the Smart Columbus Common Payment System (CPS) project to the technical community who will specify and build the system. The SyRS is a “black-box” description of what the CPS must do, but not how it will operate. The document contains descriptions of inputs, outputs and required relationships between inputs and outputs.

1.1. DOCUMENT PURPOSE

This SyRS is the second in a series of engineering documents intended to describe the CPS, building upon the Multimodal Trip Planning Application (MMTPA)/CPS Concept of Operations (ConOps) document. The SyRS describes a set of requirements that, when realized, will satisfy the expressed needs on the CPS. This document includes the identification, organization, presentation and modification of the requirements for the CPS. These requirements are derived from the User needs, constraints and interfaces that the CPS is expected to implement. This SyRS addresses conditions for incorporating operational concepts, design constraints, and design configuration requirements, as well as the necessary characteristics and qualities of individual requirements and the set of all requirements.

This document was developed based on Institute of Electrical and Electronics Engineers (IEEE) 1233-1998 Guidance for Developing System Requirements Specifications, it and contains the following sections:

- **Chapter 1. Introduction** provides an overview of the CPS project and key elements that guide the development of this SyRS document, including an overview of the project, the stakeholders, requirements development process, and referenced materials.
- **Chapter 2. System Description** focuses on describing and extending the CPS concepts established in the ConOps, including system capabilities, conditions, constraints, and decomposing the system into its Functional Groups (FGs) for establishing requirements.
- **Chapter 3. System Requirements** contains the requirements for each FG that makes up the system.
- **Chapter 4. Engineering Principles** provides a description of engineering principles applied to the system and requirements definition process.

1.2. PROJECT SCOPE

In 2016, the U.S. Department of Transportation (USDOT) awarded $40 million to the City of Columbus, Ohio, as the winner of the Smart City Challenge. With this funding, Columbus intends to address the most pressing community-centric transportation problems by integrating an ecosystem of advanced and innovative technologies, applications, and services to bridge the sociotechnical gap and meet the needs of residents of all ages and abilities. In conjunction with the Smart City Challenge, Columbus was also awarded a $10 million grant from Paul G. Allen Philanthropies to accelerate the transition to an electrified, low-emissions transportation system.

With the award, the city established a strategic Smart Columbus program with the following vision and mission:

- **Smart Columbus Vision:** Empower residents to live their best lives through responsive, innovative, and safe mobility solutions
- **Smart Columbus Mission:** Demonstrate how Intelligent Transportation Systems (ITS) and equitable access to transportation can have positive impacts of every day challenges faced by cities.

To enable these new capabilities, the Smart Columbus program is organized into three focus areas addressing unique User needs: enabling technologies, emerging technologies and enhanced human services. The CPS primarily addresses needs in the enabling technologies program focus area.

The CPS is one of nine Smart Columbus projects. Together with the MMTPA and Event Parking Management (EPM) application, Columbus and outlying communities with shared-use transportation services will use the CPS, which will be fully integrated with the Central Ohio Transit Agency's (COTA's) Central Fare Management System (CFMS) through a shared account ledger.

The CPS will be used by Travelers to pay for multimodal trips and parking options from a single account, which will be linked to various payment media and User preferences. The CPS will be part of a single, common platform that integrates end-to-end trip-planning, booking, electronic ticketing and payment services across all modes of transportation, both public and private.

The benefits of providing Travelers with a centralized, account-based payment system are increased convenience and customer satisfaction, improved access to mobility options through integration with Transportation Providers. Travelers will be able to fund accounts using a variety of payment methods such as credit and debit cards, and cash.

Accounts may also be tied to subsidization programs such as employee benefits and pre-tax dollars or tied to loyalty programs or incentives with local merchants for qualifying multimodal trips.

Table 1: Common Payment System Project Scope describes the scope of the CPS project.

Table 1: Common Payment System Project Scope

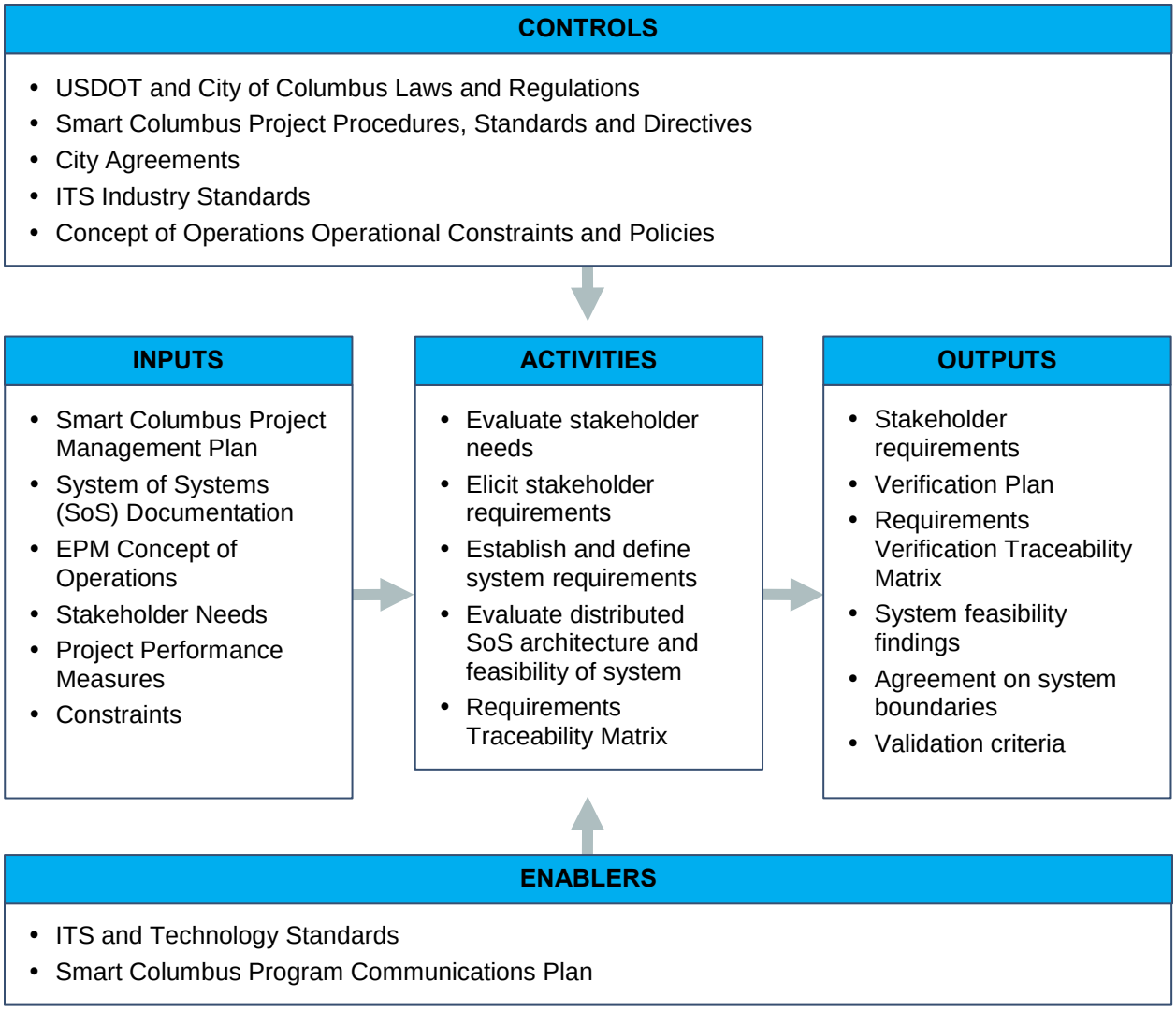
Gaps in the Existing System	Major Capability Changes in the Proposed System
Lack of comprehensive platform to plan, book, and pay for trips	• Provide Travelers with a single, integrated, convenient platform to plan, book, and pay for multimodal trips through a single app; it should not be necessary to install and maintain multiple apps to get from Point A to Point B. • Provide Travelers with incentives which may include credit toward different modes of travel based on preferences and encourage mode shifts.
Lack of control of trip and payment data; public agencies face obstacles when requesting trip data from Service Providers	• Use the Smart Columbus Operating System (OS) to store anonymous trip and payment data and make available to third-party Users; do not depend on third-party apps to provide trip planning and payment. • Utilize deep integration tools and Application Programming Interfaces (APIs) offered by Service Providers to optimize trip requests in the OS. • Centralize data in the OS to forecast economic changes and travel behavior.

Gaps in the Existing System	Major Capability Changes in the Proposed System
Fewer mobility options for unbanked Users, and Users without access to smartphones	• Improve mobility for all Travelers with access to different modes of transportation, such as car-sharing, and options for door-to-door service; provide personalized trip itineraries. • Allow unbanked Travelers to fund CPS accounts using reloadable prepaid debit cards not tied to checking accounts, or by loading cash into their CPS accounts at COTA Ticket Vending Machines (TVMs), COTA ticket offices or retail locations (Kroger, etc.). • Allow Travelers without smartphones to access an Interactive Voice Response (IVR) system that allows use of a touch-tone phone to request a pre-purchased trip pickup.
Lack of incentives for Service Providers to be part of a Mobility as a Service (MaaS) solution	• Allow for seamless payments integration. • Service Providers will increase “customer-centric” focus through partnership with Smart Columbus and willingness to improve mobility options for the public. • Access to comprehensive trip data captured in the OS may lead to better decision making and better customer service and give new insights on travel usage in the Columbus region. • Provide opportunity for Service Providers to grow business by linking to larger regional transit systems (COTA) through MMTPA. • Allow for potential cost reduction by integrating with the CPS to streamline payment services.

Source: City of Columbus

1.3. REQUIREMENTS PROCESS

The requirements established for this project will govern the CPS development cycle and are an essential factor in further defining and clarifying the scope and feasibility of development for the system. This process will also provide the basis for the technical description of deliverables in the form of a system-level specification and defined interfaces at the system boundaries. **Figure 1: Common Payment System Stakeholder Requirements Definition Process** provides a high-level view of the project’s stakeholder requirements definition process.



Source: City of Columbus

Figure 1: Common Payment System Stakeholder Requirements Definition Process

1.4. REFERENCES

Table 2: References contains documents, literature, and working group sessions used to gather input for this document.

Table 2: References

Document Number	Title	Revision	Publication Date
FHWA-JPO-17-518	Smart Columbus Systems Engineering Management Plan (SEMP) for Smart Columbus Demonstration Program https://rosap.ntl.bts.gov/view/dot/34764	–	Jan.16, 2018

Document Number	Title	Revision	Publication Date
–	Beyond Traffic: The Smart City Challenge – Phase 2 – Volume 1: Technical Application https://www.columbus.gov/WorkArea/DownloadAsset.aspx?id=2147487896	–	May 24, 2016
1233-1998	IEEE Guidance for Developing System Requirements Specifications https://ieeexplore.ieee.org/document/741940	–	1998
INCOSE-TP-2003-002-03.2.2	INCOSE Systems Engineering Handbook https://www.incose.org/products-and-publications/se-handbook	3.2.2	2011
–	Systems Engineering Guidebook for Intelligent Transportation Systems https://www.fhwa.dot.gov/cadiv/segb/files/segbversion3.pdf	3.0	2009
FHWA-JPO-17-527	Concept of Operations for the Event Parking Management Project for the Smart Columbus Demonstration Program https://smart.columbus.gov/uploadedFiles/Projects/SCC-B-EPM-ConOps-Final_For%20Posting.pdf	2.0	June 27, 2018
FHWA-JPO-17-523	Concept of Operations for the Multimodal Trip Planning Application/Common Payment System for the Smart Columbus Demonstration Program https://smart.columbus.gov/uploadedFiles/Projects/MMTP-CPS%20ConOps%208.30.18.pdf	2.0	Aug. 10, 2018
–	OS https://www.smartcolumbusos.com/	–	–
–	Smart Columbus Data Privacy Plan https://www.smartcolumbusos.com/	–	–
–	Payment Card Industry Data Security Standards https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf	3.2.1	May 2018
–	ISO/IEC 14443 Cards and security devices for personal identification – Contactless proximity objects https://www.iso.org/standard/73599.html	–	2018
–	ISO/IEC 15426-2 Information technology – Automatic identification and data capture techniques – Bar code verifier conformance specification https://www.iso.org/standard/57022.html	–	2015
–	ISO/IEC 18092 Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol https://www.iso.org/standard/56692.html	–	2013

Document Number	Title	Revision	Publication Date
–	ISO/IEC 21481 Information technology – Telecommunications and information exchange between systems – Near Field Communication Interface and Protocol https://www.iso.org/standard/56855.html	–	2012
–	ISO/IEC 15415 Information technology – Automatic identification and data capture techniques – Bar code symbol print quality test specification – Two-dimensional symbols https://www.iso.org/standard/54716.html	–	2011
–	Web Content Accessibility Guidelines https://www.w3.org/TR/WCAG/	2.1	June 2018

Source: City of Columbus

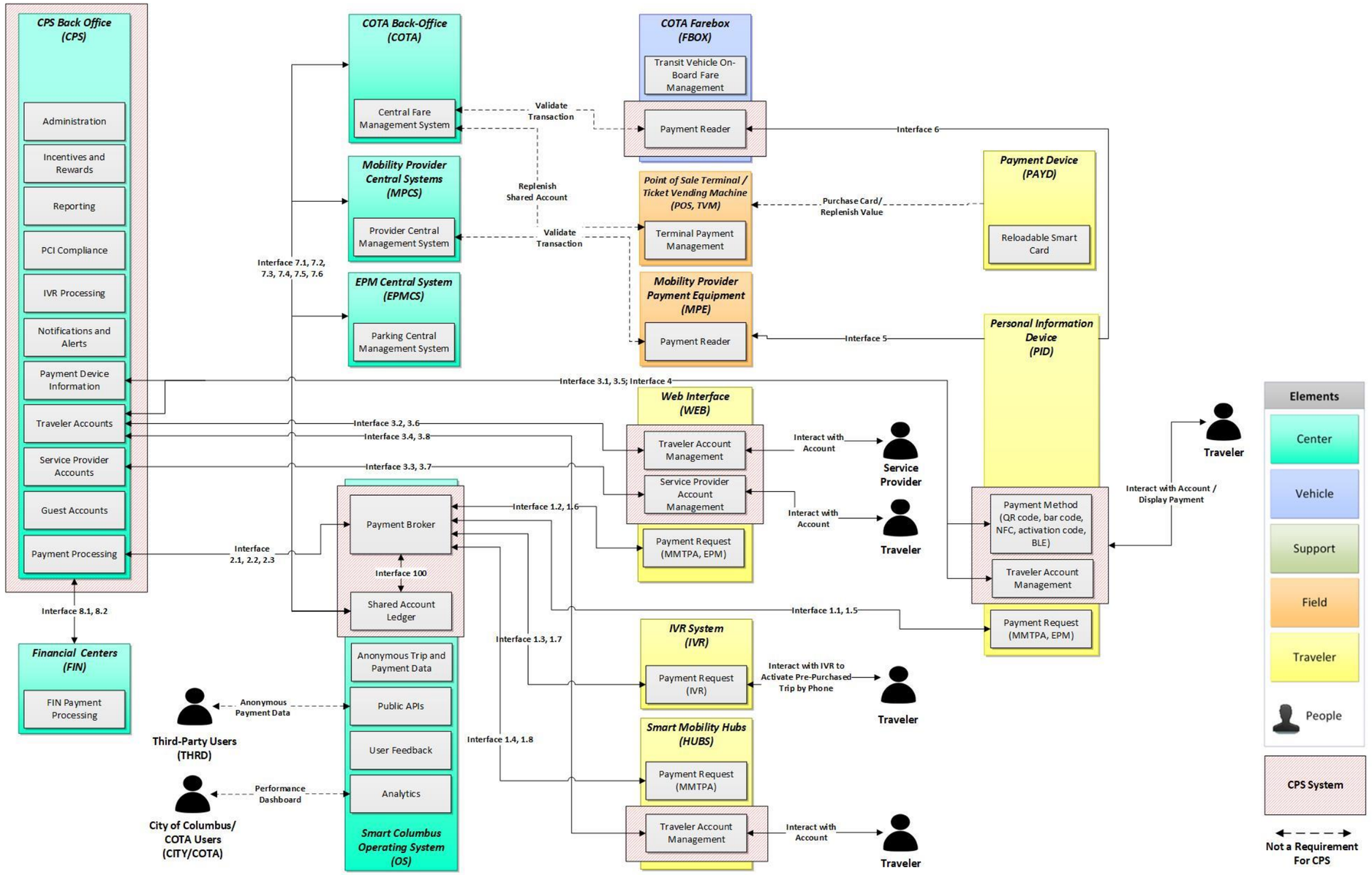
Chapter 2. System Description

2.1. SYSTEM CONTEXT

The CPS is a combination of subsystems that work together to integrate payments for both public and private transportation and parking systems. Requests for payment shall flow through a payment broker which will reside in the OS. The broker will be responsible for directing payment requests to the CPS payment processor and for capturing anonymous trip and payment data for analytics. Travelers shall access the CPS through seamless integration with the MMTPA and EPM to pay for transportation and parking services, or through an IVR System, kiosks at Smart Mobility Hubs (HUBS), or by using a Web Portal to purchase services or manage an account.

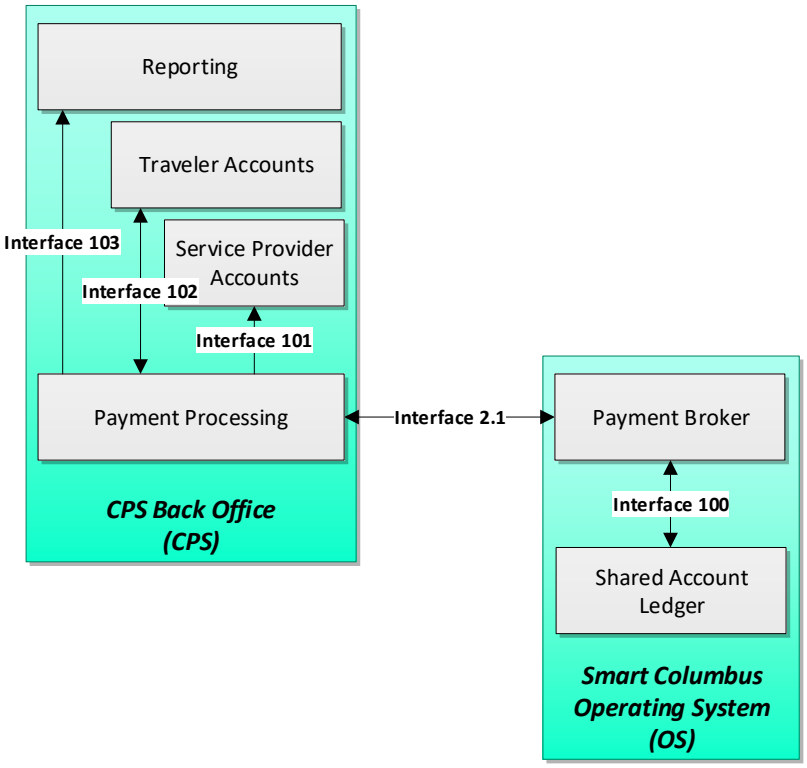
To pay for non-transit trips, the CPS shall generate mobile tickets and activation codes that are accepted at Provider payment equipment. The CPS and COTA shall share an account registry that allows for seamless mobile payments at fareboxes and access to existing transit payment media. Traveler accounts shall credit Provider accounts in the CPS for services rendered. To facilitate payment, the CPS shall coordinate with financial institutions that serve as clearinghouses for Providers to provide payment reconciliation.

Figure 2: Common Payment System Context Diagram shows a context diagram for the CPS. **Figure 3: Internal Interfaces – Payment Processing** shows data flow for Traveler and Provider Accounts in the CPS back office. **Figure 4: Internal Interfaces – Interactive Voice Response Processing** shows data flow for IVR Processing in the CPS back office.



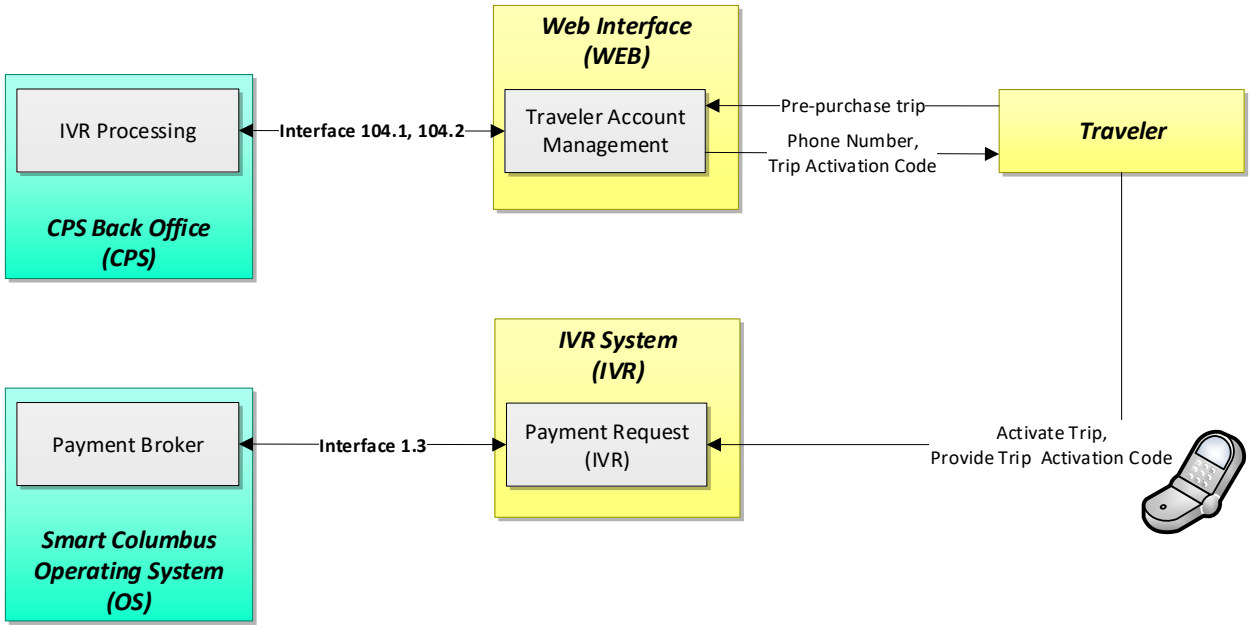
Source: City of Columbus

Figure 2: Common Payment System Context Diagram



Source: City of Columbus

Figure 3: Internal Interfaces – Payment Processing



Source: City of Columbus

Figure 4: Internal Interfaces – Interactive Voice Response Processing

Table 3: System Functional Groups provides functional groups resulting from the proposed system diagram deconstructed into its major components/functionality.

Table 3: System Functional Groups

Ref	FG	High-Level Functionality
CPS	CPS Back Office	The CPS Back Office will process payments between Traveler and Service Provider accounts, reconcile payments with Service Provides, provide interfaces for Travelers and Service Providers to manage accounts, and generate mobile tickets for use by Travelers on their personal information devices. The CPS Back Office needs to be compliant with Payment Card Industry (PCI) Data Security Standards (DSS), ensuring the security and confidentiality of Personally Identifiable Information (PII). The CPS back office will also provide for IVR processing and shall provide back-office functions to create and administer a rewards and incentives program.
COTA	COTA Back Office	COTA's Central Fare Management System (CFMS) will be integrated with the CPS through the Shared Account Ledger. The CFMS is responsible for COTA fare calculation and processing COTA fare payments.
FBOX	COTA Farebox	COTA bus fareboxes provide validation of mobile tickets and accept cash payments. COTA bus fareboxes have a contactless radio-frequency identification (RFID) reader compliant with the ISO 14443 Type A and B standards for smart cards, mobile devices enabled for Near Field Communication (NFC), and credit/debit contactless payments. FBOXs have an optical reader than can be used to process a quick response (QR) code generated with the encrypted shared-account ID.
POS/TVM	Point of Sale Terminal/TVM	POS terminals and TVMs may allow Travelers to load cash or credit onto CPS accounts.
EPMCS	EPM Central System	Back-office system for the EPM application. The EPM Central System will be integrated with the CPS through the Shared Account Ledger. The EPM application will be integrated with the CPS via landing pages to pay for parking.
MPCS	Mobility Provider Central Systems	Mobility Provider back-office systems. Mobility Provider Central Systems will be integrated with the CPS through the Shared Account Ledger. The MMTPA will provide access to mobility provider services and payment options through the CPS.
MPE	Mobility Provider Payment Equipment	Field equipment (such as readers) for mobility and parking Providers.
PID	Personal Information Device	The CPS will provide standard interfaces or “landing pages” designed to integrate mobile payment and ticketing into apps or websites. CPS landing pages will also allow Travelers to interact with the CPS back office for account management.

Ref	FG	High-Level Functionality
PAYD	Payment Device	Devices (such as smart cards, smartphones, bar codes) that support the electronic transfer of funds from the Traveler to the Service Provider.
FIN	Financial Centers	Service Provider Financial Institutions.
WEB	Web Interface	Account management portal for Travelers and Service Providers. Service Providers will utilize their web portal to manage contact and billing information, and to access reports and view individual transactions.
IVR	IVR System	Travelers without access to smartphones will be able to pre-purchase trips using a third-party IVR system. The CPS back office will include a process to generate a unique trip activation code and phone number to call to activate the trip.
HUBS	Smart Mobility Hubs	Kiosks will allow Travelers without smartphones (Title VI requirement) via the touch screen to generate and pay for a trip plan, allowing for a transportation service to pick them up and drop them off at a chosen location.
OS	Smart Columbus Operating System	The OS will contain a Payment Broker to facilitate payment requests through a Shared Account Ledger. The Shared Account Ledger will contain anonymous accounts and balances that are linked to Service Provider accounts or to Traveler accounts in the CPS. The Payment Broker will accept CPS payment requests (from MMTPA, EPM, and a third-party IVR system) and interact with the CPS back office to process payments.
CITY/ COTA	City of Columbus/COTA Users	The City of Columbus/COTA Users will have access to anonymized CPS data stored in the OS. APIs will be provided to allow access by authenticated City of Columbus/COTA Users. Information pertaining to payment and system performance, such as how frequently the CPS is used to pay for trips or parking, will be transmitted to the OS for analysis and common data sharing with other applications in near-real time. City of Columbus Users will have the ability to configure reports using the existing data in the OS.
THRD	Third-Party Users	Third-Party Users will have restricted access to anonymized CPS data stored in the OS. APIs will be provided to allow access by authenticated Users.

Source: City of Columbus

Table 4: Functional Group Subcomponent Definitions provides definitions resulting from the proposed system diagram deconstructed into its major components/functionality.

Table 4: Functional Group Subcomponent Definitions

Ref	Subcomponent	High-Level Functionality
CPS	Administration	The CPS provides administrative access for authorized City/COTA Users. Administration includes access to records of all account information and transaction history.
	PCI Compliance	The CPS is responsible for the processing, storage, and transmission of cardholder data electronically, as well as taking inputs from MMTPA and other Smart Columbus apps to route payment requests to the appropriate banks or processors for payment. The process will ensure sensitive PCI data will be secure and encrypted.
	Notifications and Alerts	Account balance and related payments updates to the Traveler.
	Payment Device Information	Information such as a bar code or QR code to support the electronic transfer of funds from the Traveler to the Service Provider.
	IVR Processing	Back-Office functions related to trip initiation via IVR system.
	Reporting	Reporting and financial auditing services of the CPS.
	Guest Accounts	Temporary accounts that are used to process a one-time payment transaction for Travelers who do not desire to create a CPS account. Payment information is not stored.
	Service Provider Accounts	Provider accounts are created for each Service Provider to receive payments. Provider accounts will store contact and billing information and provide the ability to view reports and individual transactions.
	Traveler Accounts	Each Traveler creates a Traveler account to pay for services. Traveler accounts maintain a balance and can be funded from automatic withdrawals from credit or debit cards on file. Traveler accounts store personal and payment information, auto-fill and alerts settings, and they can allow Users to query and view individual transactions. Traveler accounts may be tied to employee benefits programs to allow workers' pre-tax dollars to pay for transportation and parking services.
	Incentives and Rewards	Back-Office functions related to the creation and administration of a rewards and incentives program.
	Payment Processing	Payment Processing provides the Back-Office functions that support requests for transit and non-transit payment, requests for funds availability (from Traveler accounts), and updates to payment history. It also supports secure communications with the financial infrastructure and distributed payment infrastructure for payment reconciliation with FINs.

Ref	Subcomponent	High-Level Functionality
OS	Payment Broker	The payment broker is required to facilitate payment processing through the shared account ledger. The payment broker interacts with the shared account ledger to validate available funds in a Traveler account and to complete a payment transaction. It is deployed as a microservice in the OS. The payment broker accepts payment requests from the MMTPA and EPM application and interacts with the CPS Payment Processor.
	Shared Account Ledger	The shared account ledger in the OS contains anonymous accounts and balances that are linked to User accounts belonging to Service Providers or to Traveler accounts in the CPS. An API will facilitate two-way updates between the Service Providers and the shared account ledger.
	Anonymous Trip and Payment Data	Anonymous trip and payment data are used for analytics and performance measurement by City/COTA Users, and the data is also available via APIs to third-party Users.
	Analytics	Analytics are reports on trip and payment data to quantify performance.
	User Feedback	User feedback on the CPS is stored in the OS.
	Public APIs	The OS publishes Public APIs to allow access to anonymous trip and payment data.
PID	Payment Method	QR code, bar code, or activation code generated by the CPS and transmitted to the PID.
	Payment Request (MMTPA, EPM)	MMTPA and EPM integration with CPS to request payment.
	EPM Request for Payment	EPM integration with CPS.
	Traveler Account Management	Standard CPS interfaces designed to integrate the CPS payment platform directly into mobile apps or websites. CPS landing pages will allow for one-click payment processing as well as access to CPS account management.
WEB	Payment Request (MMTPA, EPM)	Web portal integration with MMTPA and EPM to request payment.
	Traveler Account Management	Standard CPS interfaces designed to integrate the CPS payment platform directly into mobile apps or websites. CPS landing pages will allow for one-click payment processing as well as access to CPS account management.
	Service Provider Account Management	Standard CPS interfaces designed to integrate the CPS payment platform directly into mobile apps or websites. CPS landing pages will allow Service Provider to manage contact and billing information and provide the ability to view reports and individual transactions.
IVR	Payment Request (IVR)	IVR integration with MMTPA/CPS.
HUBS	Payment Request (MMTPA)	Kiosk integration with MMTPA/CPS.

Ref	Subcomponent	High-Level Functionality
	Traveler Account Management	Standard CPS interfaces designed to integrate the CPS payment platform directly into mobile apps or websites. CPS landing pages will allow for one-click payment processing.
PAYD	Reloadable Smart Card	Reloadable prepaid debit cards not tied to checking accounts, used to fund Traveler accounts.
MPE	Payment Reader	Payment management equipment such as key personal identification number code readers.
MPCS	Mobility Provider Central Management System	Provider Back-Office systems used to validate payment.
EPMCS	Parking Central Management System	The EPMCS is the Back-Office system for the EPM project. Parking facilities interact with the EPMCS for parking information and reservation confirmations.
POS/TVM	Terminal Payment Management	Payment management process allowing Travelers to swipe, scan or enter prepaid card number (contained in magnetic strip, barcode or QR code) to access account and reload value by entering cash into the POS terminal or allowing vendors to accept cash to issue card or add value.
FBOX	Transit Vehicle Onboard Fare Management	After positive validation at a farebox, a Traveler redeems their mobile ticket in the CFMS and deducted from the Traveler account. Alternatively, it may be possible to bypass the farebox operating system and use COTA's onboard network to process the transaction in the CPS.
	Payment Reader	Onboard NFC/smart card, magnetic strip card, and optical reader for QR codes. Alternatively, may include a new Bluetooth device connected to COTA's onboard network.
COTA	Central Fare Management System (CFMS)	CPS Back-Office system that includes the following components and subsystems: account-based fare management, reporting, mobile ticketing application, fareboxes (accepting cash, smartcards, e-tickets, read-only magnetic-strip cards), and TVMs and POS terminals.

Source: City of Columbus

Table 5: Expected Interfaces summarizes the interfaces, facilities, communications and messages the system uses. The reader should reference these figures and table throughout this section to better understand the system concept.

Table 5: Expected Interfaces

Interface ID	Reference	Interface Type	Source Element	Destination Element	Data Flow	Communications Media
CPS-IX2817-V01	Interface 1.1	External	PID (Payment Request)	OS (Payment Broker)	PID shall send payment request information (amount, request type, trip ID, Traveler, Provider) and funds availability request to OS.	Secure IPSEC point to point over internet
CPS-IX2818-V01	Interface 1.2	External	WEB (Payment Request)	OS (Payment Broker)	WEB shall send payment request information (amount, request type, trip ID, Traveler, Provider) and funds availability request to OS.	Secure IPSEC point to point over internet
CPS-IX2819-V01	Interface 1.3	External	IVR (Payment Request)	OS (Payment Broker)	IVR shall send payment request information (amount, request type, activation code) and funds availability request to OS.	Secure IPSEC point to point over internet
CPS-IX2820-V01	Interface 1.4	External	HUBS (Payment Request)	OS (Payment Broker)	HUBS shall send payment request information (amount, request type, trip ID, Traveler, Provider) and funds availability request to OS.	Secure IPSEC point to point over internet
CPS-IX2821-V01	Interface 1.5	External	OS (Payment Broker)	PID (Payment Request)	OS shall send payment authorization response and funds availability to PID.	Secure IPSEC point to point over internet
CPS-IX2822-V01	Interface 1.6	External	OS (Payment Broker)	WEB (Payment Request)	OS shall send payment authorization response and funds availability to WEB.	Secure IPSEC point to point over internet
CPS-IX2823-V01	Interface 1.7	External	OS (Payment Broker)	IVR (Payment Request)	OS shall send payment authorization response, funds availability to IVR.	Secure IPSEC point to point over internet
CPS-IX2824-V01	Interface 1.8	External	OS (Payment Broker)	HUBS (Payment Request)	OS shall send payment authorization response and funds availability response to HUBS.	Secure IPSEC point to point over internet

Interface ID	Reference	Interface Type	Source Element	Destination Element	Data Flow	Communications Media
CPS-IX2825-V01	Interface 2.1	External	OS (Payment Broker)	CPS (Payment Processing)	OS shall send transaction information (request ID, amount, request type, Traveler, Provider) to CPS to credit Service Provider accounts and debit Traveler accounts.	Secure IPSEC point to point over internet
CPS-IX2826-V01	Interface 2.2	External	CPS (Payment Processing)	OS (Payment Broker)	CPS shall send payment authorization response and funds availability to OS.	Secure IPSEC point to point over internet
CPS-IX2827-V01	Interface 2.3	External	CPS (IVR Processing)	OS (Payment Broker)	CPS shall send activation code and phone number to OS.	Secure IPSEC point to point over internet
CPS-IX2828-V01	Interface 3.1	External	PID (Traveler Account Management)	CPS (Traveler Accounts)	PID shall send security credentials, Traveler account information, additions, deletions, modifications, and payment methods to CPS.	Secure IPSEC point to point over internet
CPS-IX2829-V01	Interface 3.2	External	WEB (Traveler Account Management)	CPS (Traveler Accounts)	WEB shall send security credentials, Traveler account information, additions, deletions, modifications, and payment methods to CPS.	Secure IPSEC point to point over internet
CPS-IX2830-V01	Interface 3.3	External	WEB (Provider Account Management)	CPS (Provider Accounts)	WEB shall send security credentials, service Provider account information, modifications to service rates and options, report request parameters, and communications requests to CPS.	Secure IPSEC point to point over internet
CPS-IX2831-V01	Interface 3.4	External	HUBS (Traveler Account Management)	CPS (Traveler Accounts)	HUBS shall send security credentials, Traveler account information, additions, deletions, modifications, and payment methods to CPS.	Secure IPSEC point to point over internet

Interface ID	Reference	Interface Type	Source Element	Destination Element	Data Flow	Communications Media
CPS-IX2832-V01	Interface 3.5	External	CPS (Traveler Accounts)	PID (Traveler Account Management)	CPS will verify changes and provide account information.	Secure IPSEC point to point over internet
CPS-IX2833-V01	Interface 3.6	External	CPS (Traveler Accounts)	WEB (Traveler Account Management)	CPS will verify changes and provide account information. If telephone activation is requested CPS will generate an IVR phone number, activation code associated with a trip ID, Traveler, and service Provider.	Secure IPSEC point to point over internet
CPS-IX2834-V01	Interface 3.7	External	CPS (Provider Accounts)	WEB (Provider Account Management)	CPS will provide verification of account settings and reports on Service Provider accounts for parameters selected.	Secure IPSEC point to point over internet
CPS-IX2835-V01	Interface 3.8	External	CPS (Traveler Accounts)	HUBS (Traveler Account Management)	CPS will verify changes and provide account information. If telephone activation is requested CPS will generate an IVR phone number, activation code associated with a trip ID, Traveler, and Service Provider.	Secure IPSEC point to point over internet
CPS-IX2836-V01	Interface 4	External	CPS (Payment Info)	PID (Payment Method)	CPS shall send secure authorization code to be displayed by QR code, bar code, or activation code on PID.	Secure IPSEC point to point over internet
CPS-IX2837-V01	Interface 5	External	PID (Payment Method)	MPE (Payment Reader)	PID shall send QR code, bar code, or activation code to MPE.	Encrypted (RFID, NFC, QR code, Bluetooth Low Energy (BLE) or Cellular
CPS-IX2838-V01	Interface 6	External	PID (Payment Method)	FBOX (Payment Reader)	PID shall send QR code, bar code, or activation code to FBOX using existing hardware or direct network connection.	Encrypted (RFID, NFC, QR code, BLE or Cellular

Interface ID	Reference	Interface Type	Source Element	Destination Element	Data Flow	Communications Media
CPS-IX2839-V01	Interface 7.1	External	COTA (Management System)	OS (Shared Account Ledger)	COTA shall update and provide User account information to the OS.	Secure IPSEC point to point over internet
CPS-IX2840-V01	Interface 7.2	External	MPCS (Management System)	OS (Shared Account Ledger)	MPCS shall update and provide User account information to the OS.	Secure IPSEC point to point over internet
CPS-IX2841-V01	Interface 7.3	External	EPMCS (Management System)	OS (Shared Account Ledger)	EPMCS shall update and provide User account information to the OS.	Secure IPSEC point to point over internet
CPS-IX2842-V01	Interface 7.4	External	OS (Shared Account Ledger)	COTA (Management System)	OS shall provide updates to User accounts to COTA.	Secure IPSEC point to point over internet
CPS-IX2843-V01	Interface 7.5	External	OS (Shared Account Ledger)	MPCS (Management System)	OS shall provide updates to User accounts to MPCS.	Secure IPSEC point to point over internet
CPS-IX2844-V01	Interface 7.6	External	OS (Shared Account Ledger)	EPMCS (Management System)	OS shall provide updates to User accounts to EPMCS.	Secure IPSEC point to point over internet
CPS-IX2845-V01	Interface 8.1	External	CPS (Payment Processing)	FIN (Payment Processing)	CPS shall send requests for payment authorization to FIN.	Secure IPSEC point to point over internet
CPS-IX2846-V01	Interface 8.2	External	FIN (Payment Processing)	CPS (Payment Processing)	FIN shall send payment authorization response to CPS.	Secure IPSEC point to point over internet
CPS-IX2856-V01	Interface 100	Internal	OS (Payment Broker)	OS (Shared Account Ledger)	OS shall add User to Shared Account Ledger.	Internal Secure Network
CPS-IX2857-V01	Interface 101	Internal	CPS (Payment Processing)	CPS (Service Provider Accounts)	CPS shall provide an internal interface to credit Service Providers.	Internal Secure Network

Interface ID	Reference	Interface Type	Source Element	Destination Element	Data Flow	Communications Media
CPS-IX2858-V01	Interface 102	Internal	CPS (Payment Processing)	CPS (Traveler Accounts)	CPS shall provide an internal interface to deduct funds from Traveler accounts.	Internal Secure Network
CPS-IX2859-V01	Interface 103	Internal	CPS (Payment Processing)	CPS (Reports)	CPS shall provide an internal interface to update payment history.	Internal Secure Network
CPS-IX3194-V01	Interface 104.1	Internal	WEB (Traveler Account Management)	CPS (IVR Processing)	WEB shall provide request type, amount, trip ID, Traveler, and Provider to CPS.	Internal Secure Network
CPS-IX3195-V01	Interface 104.2	Internal	CPS (IVR Processing)	WEB (Traveler Account Management)	CPS shall provide phone number and activation code to WEB.	Internal Secure Network

Source: City of Columbus

2.2. SYSTEM MODES AND STATES

Table 6: CPS System Modes of Operation defines the modes of operations for the CPS. The CPS will include alert processes to make sure the problems are identified quickly, and the cause of the alert can be easily analyzed. Watchdog processes, used to detect and report failure or anomalies, will reside on separate servers from the process being analyzed.

Table 6: CPS System Modes of Operation

Mode	Definition
Operational (Regular)	Normal operating condition, the system is operating as designed and all processes are running as intended. The system is intended to function during all hours of the day. Watchdog processes are running but alerts are not activated when CPS data are within expected parameters.
Degraded Conditions	Represents a situation where primary functionality is lost due to nonfunctioning process or equipment, but an alternative (though less precise) means of accomplishing the function exists. This could be from back-up servers or processes.
Failure Conditions	Represents a situation in which the application is not operating as designed, and processes are not performing as intended. This could be from diminished communications between one or more external systems, diminished data quality or the inability to process data in a timely manner. Failure Conditions include situations that require temporary shutdown of the system. Watchdog processes will provide alerts for Failure Conditions.
Diminished Communications	• **Loss of Communication with COTA:** Loss of communications between CPS and COTA Back Offices. • **Loss of Communication with Service Provider(s):** Loss of communications between CPS Back Office and Mobility and Parking Provider systems. • **Loss of Communications with OS:** Loss of communications between the CPS Back Office and the OS preventing transfer of data. Heartbeats will monitor the connection.
Deficient Data Quality	• **Inaccurate Data:** Inaccurate real-time vehicle location, cost and availability from Service Providers. The application depends on the accuracy of this information to effectively plan routes, make connections, switch modes, and determine if services are running late. Inaccurate service data will greatly reduce the system's effectiveness. Actual trip data will be compared to estimates to determine data quality from each source. • **Inability to Process Data in a Timely Manner:** The amount of data requested to be processed in the CPS Back Office is greater than its processing capability, resulting in delays and/or unacceptable performance.

Mode	Definition
System Health Monitoring	• **API Monitoring:** Diagnostic health monitoring processes to ensure proper communication with Service Providers. Failure messages from these processes will alert required personal. • **Process Monitoring:** Diagnostic health monitoring processes to determine that Back-Office processes are running as intended.
Maintenance	Situation in which equipment and/or systems are being repaired or preventative maintenance is being performed.
Offline	Situation where internet connection is lost, and the application is unable to retrieve real-time updates or operate as intended.

Source: City of Columbus

2.3. MAJOR SYSTEM CHARACTERISTICS

2.3.1. System Capabilities

In an account-based system, fare calculation and payment are completely handled in the Back Office. Users only need to fund and manage a single account to pay for all services. Users can fund their CPS accounts using a variety of methods, such as credit card, debit card, and cash. Also, the account can be tied to subsidization programs, such as paratransit, employee benefits and pre-tax dollars, or can be tied to loyalty programs or incentives with local merchants for qualifying multimodal trips. The CPS will be integrated with COTA's Back Office via a shared account to prevent Users from having to sign up and register in both systems. It will be capable of handling one-to-one and one-to-many payments across different modes of transportation. For example, a Traveler using the CPS to pay for a multimodal trip will pay once for the total trip (that is, all trip segments) and have the funds split from their CPS account for each Service Provider for each segment of the total trip. With a shared account, COTA's smart card can be integrated with the CPS to create a single card system for Central Ohio. Travelers will be able to purchase COTA smart cards at TVMs or reload their CPS accounts using cash or credit at vendor locations. In the case of unbanked Users or Users who, for one reason or another, prefer to pay with cash, it will be possible to fund CPS accounts using reloadable prepaid debit cards not tied to traditional checking accounts. And for Users without smartphone technology, the system will use IVR to request pre-purchased trip pickups over a (touch-tone) phone.

2.3.2. System Conditions

The CPS is generally expected to perform under most conditions, securely and timely delivering payment services for multimodal trips and parking options, allowing for the stated objectives of the project to be met. Situations that may result in degraded or no performance include:

- **Loss of communications:** Localized communications will be employed to ensure that loss of communications will not adversely affect the interaction between third-party applications and the CPS, albeit there may be conditions in which data collected from the CPS will not be forwarded to the OS.

2.4. USER CHARACTERISTICS

This section defines the stakeholders, User classes, and their roles and responsibilities for the CPS. Stakeholders refers to an individual or organization affected by the activities, inputs and outputs of the system being developed. They may have a direct or indirect interest in the system and their level of

participation may vary. This includes public agencies, private organizations or the traveling public (end Users) with a vested interest, or a "stake" in one or more aspect of the CPS. Users are classified based on their perception of the system and the needs identified. Note that some key personnel may have multiple roles based on the User needs and functions.

2.4.1. Service Providers

Service Providers are companies that provide transportation and parking services to Travelers. Transportation service Providers include public transit, car-sharing, bike-sharing, TNCs (or ride-sourcing), taxis/ limos, car/vanpooling, and paratransit. Parking Providers include gated and ungated parking facilities.

2.4.2. City of Columbus

The City is responsible for developing the requirements for the CPS and for deciding the policies and rules necessary to meet the goals and objectives of the overall Smart Columbus program. The City is also responsible for establishing equal partnership with COTA and for ensuring the CPS meets the goals and objectives of COTA's Fare System upgrade and seamlessly integrates with any additional third-party applications identified during the design phase of the project. It is anticipated the City will hand-over ownership of the CPS to a non-governmental organization.

The City includes governmental staff with access to performance and usage information through integration with the OS. These Users will have access to reports and performance measurement data to make informed decisions regarding future improvements to the CPS system and to support broader transportation policy decisions.

2.4.3. Central Ohio Transit Authority

COTA has recently completed a redesign of its fare collection system by replacing all the fareboxes on its fleet of about 367 coaches and installing "validators" on about 80 coaches that will permit cashless transactions and integrate with an account-based mobile ticketing solution. COTA is also planning to upgrade and/or replace their current TVMs and Point of Sale (POS) terminals to allow multiple forms of payments and payment media such as smart cards, online payments, standard magnetic cards and cash. The CPS and COTA Back Offices will share a common ledger of Traveler account information.

- **Fareboxes:** Travelers who have purchased a COTA trip segment(s) will have access to an optical QR code (mobile e-ticket) on the MMTPA which can be activated at FBOXs. Activating an e-ticket will cause the ticket to expire from the Travelers account. If the Traveler's mobile device is NFC-enabled, and compliant with ISO 18092/ISO 21481, the device will broadcast the same unique serial number that is encoded in the QR code. A description of COTA's farebox technology is provided in the MMTPA/CPS ConOps.
- **TVMs:** COTA TVMs will allow cash to be loaded onto an existing COTA smart card to facilitate Travelers who may be unbanked or prefer to use cash. The number of TVMs that allow conversion of cash to credit will be limited. Title VI requirements will be met by allowing unbanked passengers to use cash to pre-purchase trips from TVMs or enter prepaid debit card or smart card information instead of credit or debit cards.

2.4.4. Travelers

Travelers are end Users of the CPS (residents and visitors of Columbus) who interact with the system to plan and pay for multimodal trips and parking services.

2.4.5. Third-Party Users

Third-party Users are members of the public, including researchers, evaluators, and entrepreneurs, who will have limited access to data that is generated by the system for research, evaluation and development purposes. Third-party Users will pull data from the OS (no bidirectional connection).

2.4.6. External Vendor (Offeror)

An external vendor shall be responsible for delivering the CPS and meeting the requirements set forth in this document. A nongovernmental organization (NGO), with support from COTA, will retain an external vendor to administer and maintain the CPS. The external vendor will be responsible to meet the functional, performance, operating and security requirements of the CPS.

2.4.7. Regional Systems

It is envisioned that regional systems such as the Ohio Department of Transportation (ODOT) will be able to utilize the CPS for centralized payments in exchange for transportation-related services. ODOT is the administrative department of the Ohio state government responsible for developing and maintaining all state and federal roadways in Ohio with exception of the Ohio Turnpike.

2.5. OTHER SMART COLUMBUS PROJECTS

Other Smart Columbus projects that will use the CPS include the MMTPA, EPM, OS and HUBS. The OS will share the data utilized and generated by the CPS with other authorized Smart Columbus projects.

- **MMTPA:** The MMTPA is a native mobile app deployed to both iOS and Android devices. The MMTPA is supported by a Back-Office infrastructure provided by the OS, which collects, stores and aggregates the data from multiple Mobility Providers via APIs to calculate routes and provide trip planning services to Travelers. The OS also provides deep integration with the CPS for handling payment requests on behalf of Travelers and Mobility Providers.
- **EPMCS:** The EPMCS will be created using parking availability information from existing garages, surface lots, and parking meters in Downtown and the Short North. The EPMCS will also house and share location and restriction information on the City's loading zones citywide. Data from probe vehicle sensors that report available parking will augment real-time data, allowing the system to calculate the probability of open parking meters with some degree of accuracy. EPMCS data and the City's existing parking database, along with any available real-time parking information will be provided to the OS. The CPS will be developed to handle payments to parking Providers for garages and surface lot parking.
- **OS**: Mobility Providers will provide travel data to the OS to be used for trip optimization. Travelers will pay for trips using their CPS account, and Mobility Providers will be paid for services from the CPS. Using this model, Travelers will be able to maintain a single account across all Smart Columbus applications and access shared features such as trip planning and common payment across various channels. Anonymized payment data generated by the CPS will reside in a "big data" environment within the OS that is comprised of data storage and data retrieval systems.
- **HUBS**: Traveler interactive kiosks will be installed on free standing pylons at HUBS facilities. Kiosks will display real-time transit-related information and provide an embedded touch screen display to serve as a direct interface between Travelers and the MMTPA/CPS. Kiosks will allow Travelers without smartphones (Title VI requirement) via the touch screen to generate and pay for a trip plan, allowing for a mobility Provider to pick them up and drop them off at a chosen location. The kiosk will provide Travelers with a phone number and access code (sent to a non-smartphone or via email) to use at the time of travel. Use of the phone number provided from a

non-smartphone or landline will provide the capability to connect to an IVR system that will allow Travelers to initiate a trip through the MMTPA/CPS.

2.6. ASSUMPTIONS AND DEPENDENCIES

Table 7: Assumptions and Dependencies lists the known assumptions and dependencies that represent a risk to the CPS project and can affect the ability to meet the desired functionality, maintain the project schedule or meet performance goals.

Table 7: Assumptions and Dependencies

Assumption	Corresponding Risk	Dependency	Degree
Columbus has selected an MMTPA vendor and is entering the agile development stage of the project. A CPS vendor will be selected in the first quarter of 2019 and will be responsible for integrating the CPS with the MMTPA. It is assumed that the agile development process for the MMTPA will progress according to schedule to allow for integration of both projects starting at Release 3 of the MMTPA product roadmap.	If integration is not possible, the CPS will not meet all requirements. If integration is delayed, the combined MMTPA/CPS project will also be delayed.	MMTPA agile development schedule	Critical
Service Providers will buy-in to the system and are willing to participate. Service Providers view the CPS as an opportunity to grow business.	If integration is not possible, the CPS will not meet all requirements.	External factors	Med
The City will procure an EPM application solution that can integrate with the CPS.	If integration is not possible, the CPS will not meet all requirements.	EPM procurement	Low

Source: City of Columbus

2.7. SYSTEM CONSTRAINTS

Table 8: System Constraints defines the system constraints in the CPS.

Table 8: System Constraints

Constraint ID	Reference	Constraint
CPS-CN2813-V01	Constraint 1	COTA's fare system vendor is not under contract to support integrating COTA’s Back Office with the CPS.
CPS-CN2814-V01	Constraint 2	Service Providers must be willing to integrate with the OS through open, nonproprietary internet standards, and to accept the CPS as a payment method.

Constraint ID	Reference	Constraint
CPS-CN2815-V01	Constraint 3	Service Providers (especially TNCs) are reluctant to share trip data or allow cost comparison with potential competitor services. Not all Service Providers share APIs with third-party developers or support open standards and data exchange. Currently, TNCs will provide trip data (origin-destination information) only to public agencies that subsidize part of the trip. To address this constraint, the City and COTA plan to adopt a phased approach with Service Providers who are early adopters. Subsequent releases for the system can include additional Service Providers.

Source: City of Columbus

2.8. OPERATIONAL SCENARIOS

Chapter 6 of the ConOps for the MMTPA/CPS for the Smart Columbus Demonstration Program captures and documents the operational scenarios.

Chapter 3. System Requirements

This section of the document lists the identified requirements for the CPS project. The requirements are organized by requirement type. Each requirement type has a requirement identifier (ReqID) (see **Appendix A. Document Terminology and Conventions**) along with its description, a reference number for traceability to User needs, User scenarios and/or policies and constraints. **Table 9: List of Requirement Types** describes the classifications of requirement types in this document. Each requirement also has a verification method (see **Table 10: Methods of Verification** for method definitions). This section also contains programmatic/contractual requirements, in addition to system requirements, to help the Offeror understand the entire system.

Table 9: List of Requirement Types

Type	Description
Functional (FN)	FN Requirements specify actionable and qualitative behaviors (e.g. functions, tasks) of the system of interest.
Performance (PR)	PRs specify quantifiable characteristics of operations that define the extent, or how well and under what conditions a function or task is to be performed (e.g. rates, velocities).
Interface (IF)	IF Requirements define how the system will interact, communicate, or exchange data with external systems (External IF) and how core system elements interact with other parts of the system (Internal IF).
Data (DR)	DRs define the data collected, transformed and stored from various sources as well as identifies new data that is expected to be generated.
Security (SR)	SRs specify what is necessary to protect the integrity and operability of the system, its microservices, connections and data. This includes physical security as well as cyber prevention, detection, identification, response, recovery and auditing requirements.
Non-Functional (NF)	NF Requirements define the characteristics of the overall operation of the system, including the following: • **Physical (PY) Requirements** specify the construction, durability, adaptability and environmental characteristics of the system • **Availability and Recovery (AR) Requirements** define the times of day, days of year, and overall percentage the system can be used, when it will not be available for use, and recovery point and time objectives • **Maintainability (MT) Requirements** specify the level of effort required to locate and correct an error during operation • **Storage and Transport (ST) Requirements** specify the physical location and environment for the system, including designated storage facility, installation site, repair facility, requirements for transporting equipment, etc. • **Disposal (DP) Requirements** specify the items related to the disposal of project/system components, due to either failure replacements, removal, end-of-life upgrade, or retirement

Type	Description
Enabling (EN)	EN Requirements specify details concerning the management of information as well as the production of the system and its life cycle sustainment, including the following: • **Acceptance Testing (AT) Requirements** specify the requirements for testing the system. • **Information Management (IM) Requirements** specify the acquisition, management, and ownership of information from one or more sources, the custodianship and the distribution of that information to those who need it. • **Life-Cycle (LC) Sustainability Requirements** define what items the project or system will review, measure, and analyze as part of its commitment to quality during the life cycle of the system including development, integration, verification, validation and training.
Policy and Regulation (RG)	RG Requirements specify relevant and applicable organizational policies or regulations that affect the development, operation or performance of the system (e.g., Information Technology (IT) and labor policies, reports to regulatory agencies, health or safety criteria, etc.). This section also includes new policy and regulation imposed to realize the system.

Source: City of Columbus

The requirements also maintain a verification method, which details the plan for verifying the requirement based on its stated definition. For each requirement is assigned one of the verification methods listed in **Table 10: Methods of Verification** using the requirements defined in the previous section.

Table 10: Methods of Verification

Type	Description
Inspection	Verification through a visual, auditory or tactile comparison.
Demonstration	Verification that exercises the system software or hardware as it is designed to be used, without external influence, to verify the results are specified by the requirement.
Test	Verification using controlled and predefined inputs and other external elements (e.g. data, triggers, etc.) that influence or induce the system to produce the output specified by the requirement.
Analyze	Verification through indirect and logical conclusion using mathematical analysis, models, calculations, testing equipment and derived outputs based on validated data sets.

Source: City of Columbus

3.1. FUNCTIONAL REQUIREMENTS

This section provides the high-level functional requirements (FN) for the CPS system, or what the system will do. The requirements in **Table 11: Functional Requirements** are organized by functional groups related to user needs identified in the MMTPA/CPS ConOps.

Table 11: Functional Requirements

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2464-V01	CPS Back Office	Payment Processing	The CPS shall perform payment reconciliation with Service Providers for services paid for by Travelers using the CPS.	MMTPA/CPS-UN006-v02	Demonstration
CPS-FN2465-V01	CPS Back Office	Payment Processing	Payment reconciliation between the CPS and Service Providers shall occur at intervals (daily, weekly, or monthly) based on contracted terms with Service Providers.	MMTPA/CPS-UN006-v02	Demonstration
CPS-FN2466-V01	CPS Back Office	Traveler Accounts	The CPS shall provide secure User account management for electronic payments.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2468-V01	OS	Payment Broker	The CPS shall provide an open source payment broker to facilitate payment processing through the shared account ledger.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2469-V01	OS	Payment Broker	The payment broker shall not maintain PCI data. The CPS Back Office will maintain PCI data information in a secure environment.	MMTPA/CPS-UN022-v02 CPS-CN2816-V01	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2470-V01	OS	Payment Broker	The payment broker shall be deployed as a microservice in the OS.	MMTPA/CPS-UN006-v02 CPS-CN2815-V01	Demonstration
CPS-FN2471-V01	OS	Payment Broker	The payment broker shall accept payment requests from the MMTPA and EPM application on the PID.	MMTPA/CPS-UN006-v02 CPS-CN2815-V01	Demonstration
CPS-FN2472-V01	CPS Back Office	Payment Processing	The CPS shall be capable of processing payment requests for multiple trip segments and multiple service Providers at one time through a "click once" payment functionality in the MMTPA.	MMTPA/CPS-UN025-v02	Demonstration
CPS-FN2473-V01	CPS Back Office	Traveler Accounts	Traveler accounts shall maintain a balance (stored cash value) so that transactions can be implemented using "click once" functionality (CPS-FN2472-V01) without having to re-enter payment information.	MMTPA/CPS-UN025-v02	Demonstration
CPS-FN2474-V01	CPS Back Office	Traveler Accounts	The CPS shall have the ability to make automatic withdrawals from a Traveler's payment method on file to replenish a CPS account when the account balance falls below a dollar amount threshold that is set by the Traveler.	MMTPA/CPS-UN022-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2475-V01	CPS Web Portal	Account Management	Travelers shall be able to configure the dollar amount threshold at which the CPS will trigger an automatic withdrawal from a payment method on file to replenish the Traveler's CPS account.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2476-V01	CPS Back Office	Notifications and Alerts	The CPS shall trigger a push notification to the Traveler's mobile device when account balance falls below set dollar amount threshold.	MMTPA/CPS-UN027-v02	Demonstration
CPS-FN2477-V01	CPS Web Portal	Account Management	Travelers shall have the ability to configure whether to receive text and email alerts when their CPS account is low or has been replenished.	MMTPA/CPS-UN027-v02	Demonstration
CPS-FN2478-V01	CPS Web Portal	Account Management	Travelers shall be able to make inquiries pertaining to payments and account status to the CPS Offeror.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2479-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with access to rules and policies governing CPS usage.	MMTPA/CPS-UN007-v02	Demonstration
CPS-FN2480-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with access to current billing status, invoices, and payments.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2481-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with mechanisms to review and challenge current billing status, invoices, and payments.	MMTPA/CPS-UN022-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2482-V01	CPS Back Office	Traveler Accounts	The CPS shall process and clear payments from Travelers directly through a conventional financial payment gateway, or blockchain gateway, not through a middleman merchant account.	MMTPA/CPS-UN041-v02	Demonstration
CPS-FN2484-V01	COTA Farebox	Payment Device Reader	An onboard process may be developed to allow COTA fareboxes to read mobile ticket information from the PID. The Offeror shall negotiate any use of the onboard fare management system with Genfare.	MMTPA/CPS-UN021-v02 CPS-CN2815-V01	Demonstration
CPS-FN2487-V01	CPS Back Office	Payment Processing	The CPS shall process requests for payment that are received from the payment broker.	MMTPA/CPS-UN025-v02	Demonstration
CPS-FN2488-V01	CPS Back Office	Payment Processing	The CPS shall allow Travelers to utilize existing COTA period pass products, which permit journeys within the COTA network, subject to time restrictions.	MMTPA/CPS-UN026-v02	Demonstration
CPS-FN2490-V01	CPS Back Office	Payment Processing	The CPS shall allow virtual transfer credits to be used for the purposes of permitting multi-leg transit trips subject to current restrictions in accordance with COTA policies.	MMTPA/CPS-UN026-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2491-V01	CPS Back Office	Payment Processing	When applying virtual transfer credits toward a multi-leg transit trip, the remainder of the cost of the trip (if additional charges are required) shall be taken from the Traveler account (stored cash value).	MMTPA/CPS-UN026-v02	Demonstration
CPS-FN2493-V01	CPS Web Portal	Account Management	Travelers shall be required to register or provide a Username and password to log into the Web Portal.	MMTPA/CPS-UN028-v02	Demonstration
CPS-FN2494-V01	CPS Web Portal	Account Management	Service Providers shall be required to provide a Username and password to log into the Web Portal.	MMTPA/CPS-UN028-v02	Demonstration
CPS-FN2495-V01	CPS Back Office	Administration	The CPS shall allow for management of special programs such as Traveler discounts, benefits, and loyalty programs.	MMTPA/CPS-UN024-v02	Demonstration
CPS-FN2496-V01	CPS Back Office	CPS Payment Processing	The CPS should provide the ability to bundle services of multiple Providers (monthly subscription plans).	MMTPA/CPS-UN035-v02 CPS-CN2815-V01	Demonstration
CPS-FN2499-V01	CPS Back Office	Payment Processing	The CPS shall be capable of handling payments for non-emergency medical transportation (NEMT) trips funded through Medicaid accounts. This capability is considered “future state” and shall not be required in the final release of the CPS for the grant.	MMTPA/CPS-UN035-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2500-V01	OS	Shared Account Ledger	The CPS shall provide an API to share existing Traveler account information with COTA's CFMS and other Service Providers to the shared account ledger.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2503-V01	CPS Back Office	Payment Processing	The CPS shall accept cash, all major US and international credit cards and debit cards (reloadable cards that are not tied to a personal checking account).	MMTPA/CPS-UN023-v02	Demonstration
CPS-FN2504-V01	CPS Back Office	Payment Processing	The CPS shall accept use of electronic wallets (Apple Pay, Android Pay, and Google Pay).	MMTPA/CPS-UN023-v02	Demonstration
CPS-FN2505-V01	CPS Back Office	Administration	The CPS shall provide administrative accounts secured by Username and password for authorized individuals at the City and COTA.	MMTPA/CPS-UN034-v02 CPS-FN2506-V01	Demonstration
CPS-FN2506-V01	CPS Back Office	Administration	Administrative accounts shall include fine-grained permission levels (e.g., View Only, Limited Access, and Full Control).	MMTPA/CPS-UN034-v02 CPS-FN2505-V01 CPS-FN2528-V01 CPS-FN2529-V01 CPS-FN2569-V01	Demonstration
CPS-FN2507-V01	CPS Back Office	Administration	Each User of the system shall be classified into exactly one account type.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2509-V01	CPS Back Office	Traveler Accounts	Traveler accounts in the CPS Back Office shall be created and administered by the Traveler.	MMTPA/CPS-UN022-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2510-V01	CPS Back Office	Provider Accounts	The CPS shall include secure PCI compliant Service Provider accounts.	MMTPA/CPS-UN022-v02 CPS-CN2815-V01	Demonstration
CPS-FN2511-V01	CPS Web Portal	Account Management	Service Provider accounts shall be administered by the Service Providers.	MMTPA/CPS-UN040-v02 CPS-CN2815-V01	Demonstration
CPS-FN2512-V01	CPS Back Office	Provider Accounts	Service Provider accounts shall be created by authorized individuals at the City and COTA, pending review and approval procedures.	MMTPA/CPS-UN040-v02	Demonstration
CPS-FN2513-V01	CPS Web Portal	Account Management	Service Provider accounts shall have administrative parameters for setting rates for base cost per trip, distance, travel time, and surge pricing (if applicable).	MMTPA/CPS-UN040-v02	Demonstration
CPS-FN2514-V01	CPS Web Portal	Account Management	Service Providers shall have an API to add their existing Traveler accounts to the shared account ledger.	MMTPA/CPS-UN040-v02	Demonstration
CPS-FN2515-V01	CPS Back Office	Guest Accounts	The CPS should include the option for a Traveler to create a guest account to pay for services.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2516-V01	CPS Back Office	Guest Accounts	Guest accounts should be temporary accounts to facilitate one-time payment transactions.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2517-V01	CPS Back Office	Guest Accounts	Guest accounts should not store credit card information, including Card Verification Value (CCV) numbers, in the CPS.	MMTPA/CPS-UN022-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2518-V01	CPS Back Office	Traveler Accounts	Travelers shall be required to register at least one valid method of payment, as defined in CPS-FN2503-V01 and CPS-FN2504-V01, to create a Traveler account.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2520-V01	CPS Web Portal	Account Management	Creating a Traveler account shall require submission of contact information.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2521-V01	CPS Web Portal	Account Management	Contact information shall include first and last name.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2522-V01	CPS Web Portal	Account Management	Contact information shall include an email address.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2523-V01	CPS Web Portal	Account Management	Creating a Traveler account shall require submission of three authenticating security questions and answers.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2524-V01	CPS Web Portal	Account Management	Contact information may include date of birth.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2525-V01	CPS Web Portal	Account Management	Contact information may include a valid driver's license number.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2526-V01	CPS Web Portal	Account Management	Contact information shall include a telephone number.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2527-V01	CPS Web Portal	Account Management	Contact information shall be recorded and treated independently of any personal information related to payments.	MMTPA/CPS-UN022-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2528-V01	CPS Back Office	Administration	The CPS shall permit administrative Users with limited access to transfer the balance (stored cash value) of one registered CPS account to another registered CPS account.	MMTPA/CPS-UN034-v02 MMTPA/CPS-UN042-v02 CPS-FN2506-V01	Demonstration
CPS-FN2529-V01	CPS Back Office	Administration	The CPS shall permit administrative Users to close any account type (e.g. due to prolonged inactivity or abuse of policies).	MMTPA/CPS-UN034-v02 CPS-FN2506-V01	Demonstration
CPS-FN2530-V01	CPS Web Portal	Account Management	The CPS shall enable Travelers to enable, disable, and configure auto-reloading by associating a payment medium (e.g., credit card or online payment service, etc.) to a Traveler account.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2531-V01	CPS Web Portal	Account Management	Auto-reloading shall be configurable to a specific payment medium (e.g., credit card, online payment service, etc.).	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2532-V01	CPS Web Portal	Account Management	Auto-reloading configuration shall include minimum account balance at which point auto-reloading shall be triggered.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2533-V01	CPS Back Office	Payment Processing	When validating a stored cash value transaction from a Traveler account, the system shall not permit the stored cash value balance to enter overdraft (i.e., fall below $0.00).	MMTPA/CPS-UN022-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2534-V01	CPS Back Office	Traveler Accounts	The CPS shall permit more than one COTA smart card to be associated with a single Traveler account to allow funds to be transferred between the accounts.	MMTPA/CPS-UN026-v02	Demonstration
CPS-FN2536-V01	CPS Back Office	Traveler Accounts	The CPS shall associate any COTA issued fare media (including Limited Use Media (LUM) cards) with a registered Traveler account.	MMTPA/CPS-UN026-v02	Demonstration
CPS-FN2537-V01	CPS Back Office	Traveler Accounts	The CPS shall permit multiple fare media to be associated with a single Traveler account.	MMTPA/CPS-UN026-v02	Demonstration
CPS-FN2538-V01	CPS Back Office	Traveler Accounts	The CPS shall permit payment media to be disassociated from an account without closing the account.	MMTPA/CPS-UN026-v02	Demonstration
CPS-FN2539-V01	CPS Web Portal	Account Management	Travelers shall have the ability to close their accounts.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2540-V01	CPS Web Portal	Account Management	Travelers shall identify a payment method to transfer an existing balance, if applicable, when closing an account.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2542-V01	CPS Back Office	Traveler Accounts	The CPS shall be capable of allowing partner organizations (e.g. Regional Systems) to supply their own payment media.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2544-V01	CPS Back Office	Traveler Accounts	Payment media shall include all major U.S. and international credit and debit cards.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02	Demonstration
CPS-FN2545-V01	CPS Back Office	Traveler Accounts	The CPS shall provide international post code and zip code verification for fraud protection.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02	Demonstration
CPS-FN2546-V01	CPS Back Office	Traveler Accounts	Payment media may include PayPal electronic payment services.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02	Demonstration
CPS-FN2547-V01	CPS Back Office	Traveler Accounts	Payment media shall include reloadable pre-paid debit cards (i.e., not tied to a personal checking account) to facilitate unbanked Travelers.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02	Demonstration
CPS-FN2548-V01	CPS Back Office	Traveler Accounts	The CPS shall provide a mechanism for external agencies (e.g., paratransit, employers, colleges or universities, or guardians) to subsidize the cost of transportation for a Traveler.	MMTPA/CPS-UN024-v02	Demonstration
CPS-FN2549-V01	CPS Back Office	Traveler Accounts	The CPS shall provide a mechanism for external agencies (e.g., employers, colleges or universities, or guardians) to subsidize the cost of parking for a Traveler through an authorized validation code or through reoccurring backend Provider.	MMTPA/CPS-UN024-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2550-V01	CPS Web Portal	Account Management	The Web Portal shall allow Traveler accounts to be tied to an employee benefits program using pre-tax dollars to pay for transportation services.	MMTPA/CPS-UN024-v02	Demonstration
CPS-FN2551-V01	CPS Web Portal	Account Management	The Web Portal shall allow Traveler accounts to be tied to an employee benefits program using pre-tax dollars to pay for parking.	MMTPA/CPS-UN024-v02	Demonstration
CPS-FN2553-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers the option to use either an existing COTA fare product or stored value in CPS account to pay for COTA services.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2554-V01	CPS Back Office	Payment Processing	The CPS shall support SPX/Genfare QR codes for payment transactions or provide a viable alternative to satisfy requirements.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2555-V01	CPS Back Office	Payment Processing	The CPS shall support use of electronic wallets for payment transactions.	MMTPA/CPS-UN020-v02	Demonstration
CPS-FN2556-V01	CPS Back Office	Payment Processing	The CPS shall be capable of holding funds in reserve for a period of time as a credit guarantee for services where cost is not fixed (such as fares based on surge pricing, distance or duration) or when an event has yet to occur (such as when payment is required at the end of the trip).	MMTPA/CPS-UN042-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2557-V01	CPS Back Office	Payment Processing	In the event that the service for which the funds are being held is not realized, the hold on the funds shall be removed and credit restored to the Traveler account as necessary.	MMTPA/CPS-UN042-v02	Demonstration
CPS-FN2559-V01	CPS Back Office	Payment Processing	The CPS shall provide the ability for Service Providers to set their fare product structures in the Service Provider Web Portal.	MMTPA/CPS-UN026-v02 CPS-CN2813-V01	Demonstration
CPS-FN2560-V01	CPS Back Office	Payment Processing	The CPS shall be capable of integration with COTA's smart card.	MMTPA/CPS-UN026-v02 CPS-CN2813-V01	Demonstration
CPS-FN2561-V01	CPS Back Office	Payment Processing	The CPS shall provide a mechanism for Travelers who are eligible for COTA's fare subsidy programs to receive those benefits.	MMTPA/CPS-UN026-v02 CPS-CN2813-V01	Demonstration
CPS-FN2566-V01	CPS Back Office	Administration	The CPS Back Office shall retain a record of all account information and transaction history, including data associated with closed accounts, for a minimum of three years.	MMTPA/CPS-UN029-v02	Demonstration
CPS-FN2567-V01	CPS Back Office	Administration	The CPS Back Office shall maintain a transaction log that records all Users that access reports, the reports accessed, edits and changes to the database and the system logon and logoff times.	MMTPA/CPS-UN029-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2568-V01	CPS Back Office	Administration	The transaction log shall maintain information for a minimum of one year.	MMTPA/CPS-UN029-v02	Demonstration
CPS-FN2569-V01	CPS Back Office	Administration	The transaction log shall not be editable to even the highest class of administrative User (full control).	MMTPA/CPS-UN034-v02 CPS-FN2506-V01	Demonstration
CPS-FN2570-V01	CPS Back Office	Reporting	The CPS shall have the ability to generate financial audit reports (CSV and PDF).	MMTPA/CPS-UN038-v02	Demonstration
CPS-FN2571-V01	CPS Back Office	Reporting	Financial audit reports shall include fraudulent account activity where the Traveler has informed administrative Users of unrecognized account transactions.	MMTPA/CPS-UN038-v02	Demonstration
CPS-FN2572-V01	CPS Back Office	Reporting	Financial audit reports shall include financial reconciliation and pay settlement.	MMTPA/CPS-UN038-v02	Demonstration
CPS-FN2573-V01	CPS Back Office	Reporting	Financial audit reports shall include insufficient funds associated with a Traveler account.	MMTPA/CPS-UN038-v02	Demonstration
CPS-FN2574-V01	CPS Back Office	Reporting	Financial audit reports shall include pay transactions by location and trip.	MMTPA/CPS-UN038-v02	Demonstration
CPS-FN2575-V01	CPS Back Office	Reporting	Financial audit reports shall include unused and remaining value associated with a Traveler account.	MMTPA/CPS-UN038-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2576-V01	CPS Back Office	Reporting	Financial audit reports shall include faults and errors.	MMTPA/CPS-UN038-v02	Demonstration
CPS-FN2577-V01	CPS Back Office	Reporting	Financial audit reports shall include incomplete transactions.	MMTPA/CPS-UN038-v02	Demonstration
CPS-FN2578-V01	CPS Back Office	Reporting	Financial audit reports shall include reports of transactions that could not be completed due to missing data.	MMTPA/CPS-UN038-v02	Demonstration
CPS-FN2579-V01	CPS Back Office	Administration	The CPS shall allow authorized individuals to view and export account activity data (CSV and PDF) pertaining to CPS usage associated with Traveler accounts.	MMTPA/CPS-UN033-v02	Demonstration
CPS-FN2580-V01	CPS Back Office	Administration	Account activity data shall include account creation and profile information.	MMTPA/CPS-UN033-v02	Demonstration
CPS-FN2581-V01	CPS Back Office	Administration	Account activity data shall include history of all payment transactions pending and closed.	MMTPA/CPS-UN033-v02	Demonstration
CPS-FN2582-V01	CPS Back Office	Administration	Account activity data shall include balances for both Travelers and Service Providers.	MMTPA/CPS-UN033-v02	Demonstration
CPS-FN2583-V01	CPS Back Office	Administration	Account activity data shall include status of all auto-reload subscriptions associated with each Traveler account.	MMTPA/CPS-UN033-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2591-V01	CPS Back Office	Traveler Accounts	Integration with the MMTPA shall provide a seamless User experience for the Traveler by not requiring a separate logon to the MMTPA.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2592-V01	CPS Back Office	Traveler Accounts	Integration with the EPMCS shall provide the Traveler with a seamless User experience because a separate log-on to the EPM application.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2593-V01	CPS Back Office	Payment Processing	The CPS shall provide real-time funding authorization for payment transactions via cellular connectivity.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2594-V01	CPS Back Office	Payment Processing	The CPS shall provide the capability for funds to be sourced from stored value in the Traveler account rather than payment media on file.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2595-V01	CPS Back Office	Payment Processing	The CPS shall reserve the authorized dollar amount from the stored value in the Traveler account.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2596-V01	CPS Back Office	Payment Processing	The CPS shall ensure credit card transactions are credited and settled directly to the Traveler account.	MMTPA/CPS-UN022-v02 CPS-CN2815-V01	Demonstration
CPS-FN2597-V01	CPS Back Office	Notifications and Alerts	Service Providers shall be able to create and manage notifications.	MMTPA/CPS-UN040-v02	Demonstration
CPS-FN2598-V01	COTA Farebox	Payment Device Reader	The CPS may use existing COTA fareboxes for COTA transactions.	MMTPA/CPS-UN021-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2599-V01	COTA Farebox	Payment Device Reader	The CPS should not require installation of new fareboxes or fare validators.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2600-V01	COTA Farebox	Payment Device Reader	The CPS may provide an embedded SDK that extends the functionality of existing COTA fareboxes.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2601-V01	COTA Farebox	Payment Device Reader	The CPS may integrate with the contactless optical code scanner (compliant with ISO 15426-2 for mobile devices) of existing COTA fareboxes.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2602-V01	COTA Farebox	Payment Device Reader	The CPS may integrate with the contactless RFID reader (compliant with ISO 14443 Type A and B standard) of existing COTA fareboxes for NFC-enabled mobile devices.	MMTPA/CPS-UN019-v02	Demonstration
CPS-FN2603-V01	COTA Farebox	Payment Device Reader	The CPS may integrate with COTA's existing fareboxes to allow recognition of a mobile app presenting a ticket ID via an optical barcode on the device screen, or (if supported by the device) through NFC.	MMTPA/CPS-UN019-v02	Demonstration
CPS-FN2604-V01	Personal Information Device	Application Payment Device	Activating and subsequent use of an e-ticket shall cause the ticket to expire from the Traveler account.	MMTPA/CPS-UN021-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2605-V01	Personal Information Device	Application Payment Device	If the mobile device of the Traveler is NFC-enabled, and compliant with ISO 18092/ISO 21481, the device shall broadcast the same unique serial number that is encoded in the QR code.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2606-V01	CPS Back Office	Payment Device Information	The CPS should be capable of digitally rendering encrypted optical codes (mobile e-tickets) for optical scanning at Service Provider reader equipment.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2607-V01	CPS Back Office	Payment Device Information	Mobile e-tickets should be machine readable 2D optical code compliant with ISO-15415, encoding the unique serial number.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2608-V01	CPS Back Office	Payment Device Information	Mobile e-tickets should serve to create the identifier used to validate and track the ticket and associated transactions in the system.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2609-V01	CPS Back Office	Payment Device Information	Mobile e-tickets should be human readable text displaying the serial number encoded in the optical code.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2610-V01	CPS Back Office	Payment Device Information	Optical codes should be encrypted to centralized randomization algorithms.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2611-V01	CPS Back Office	Payment Device Information	Mobile e-tickets should include security features verifiable by a human inspector (e.g., moving graphic, changing color, real-time clock).	MMTPA/CPS-UN021-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2612-V01	Personal Information Device	Application Payment Device	The screen displaying the e-ticket shall include a soft key to close the mobile e-ticket.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2613-V01	Personal Information Device	Application Payment Device	Opening the mobile e-ticket page shall set the e-ticket in an active state.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2614-V01	Personal Information Device	Application Payment Device	An active mobile e-ticket shall remain accessible to the Traveler in an active state for presentation and validation following an unexpected shutdown of the app.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2615-V01	Personal Information Device	Application Payment Device	Devices that are enabled for NFC, and compliant with ISO 18092 and ISO 21481, shall broadcast the same unique serial number that is encoded in the optical code while the mobile e-ticket remains active.	MMTPA/CPS-UN019-v02	Demonstration
CPS-FN2616-V01	Personal Information Device	Application Payment Device	Closing the mobile e-ticket page shall set the e-ticket in an inactive state, clearing the notification from the device's notification center, and terminating any NFC transmission (if applicable).	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN2617-V01	Personal Information Device	CPS Landing Pages	The PID shall provide Travelers with account balance, pass expiration and related service alerts via push notifications and alerts.	MMTPA/CPS-UN008-v02	Demonstration
CPS-FN2621-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to replenish their account.	MMTPA/CPS-UN022-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2622-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to manage account information.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2623-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to manage payment options.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2624-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to manage account information.	MMTPA/CPS-UN028-v02	Demonstration
CPS-FN2625-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to purchase fare products.	MMTPA/CPS-UN028-v02	Demonstration
CPS-FN2626-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to replenish their account.	MMTPA/CPS-UN028-v02	Demonstration
CPS-FN2627-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to manage payment options.	MMTPA/CPS-UN028-v02	Demonstration
CPS-FN2628-V01	CPS Web Portal	Account Management	The Web Portal shall enable Service Providers to manage accounts directly, by correctly entering login authentication.	MMTPA/CPS-UN028-v02	Demonstration
CPS-FN2629-V01	CPS Web Portal	Account Management	The Web Portal shall enable Travelers to manage accounts directly, by correctly entering login authentication.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2630-V01	CPS Back Office	Notifications and Alerts	The CPS shall be capable of notifying Travelers via text, email, or push notification of payment confirmation.	MMTPA/CPS-UN008-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2631-V01	CPS Back Office	Traveler Accounts	The CPS shall permit the entry of US and international profile information to accommodate tourists and visitors to Central Ohio.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2632-V01	CPS Web Portal	Account Management	The Web Portal shall provide the capability to configure notifications and alerts.	MMTPA/CPS-UN027-v02	Demonstration
CPS-FN2633-V01	CPS Web Portal	Account Management	The Web Portal shall provide the capability to configure notifications and alerts.	MMTPA/CPS-UN028-v02	Demonstration
CPS-FN2634-V01	CPS Web Portal	Account Management	Information relevant to an existing payment(s) (receipt/proof of payment) shall be accessible to the Traveler within the previous three months.	MMTPA/CPS-UN028-v02	Demonstration
CPS-FN2636-V01	CPS Back Office	IVR Processing	The CPS Back Office shall be capable of processing payment requests to generate an activation code to be used for an IVR-requested trip (reference CPS-FN3137-V01).	MMTPA/CPS-UN016-v02	Demonstration
CPS-FN2637-V01	CPS Back Office	IVR Processing	The CPS Back Office shall include a process to transfer the unique trip code purchased using a third-party IVR system to the Traveler by email and by text message.	MMTPA/CPS-UN016-v02	Demonstration
CPS-FN2638-V01	CPS Back Office	Incentives and Rewards	The CPS shall provide Back-Office functions to create and administer a rewards and incentives program.	MMTPA/CPS-UN011-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN2639-V01	CPS Back Office	Incentives and Rewards	Travelers who earn promotions or rewards or financial incentives for completing multimodal trips using the MMTPA, or through other promotions tied to a Traveler account, shall be able to view and access these rewards or incentives through the Traveler account.	MMTPA/CPS-UN011-v02	Demonstration
CPS-FN2640-V01	CPS Back Office	Incentives and Rewards	For promotions or rewards, a Traveler shall be able to activate the promotion or reward through the Traveler account.	MMTPA/CPS-UN011-v02	Demonstration
CPS-FN2641-V01	OS	Payment Broker	Data posted to the OS from the Payment Broker shall have PII obfuscated so that it may be available to third-party Users.	MMTPA/CPS-UN033-v02 CPS-CN2816-V01	Demonstration
CPS-FN2644-V01	CPS Back Office	Payment Processing	Payment transactions shall be authorized in real time through the CPS.	MMTPA/CPS-UN006-v02	Demonstration
CPS-FN2645-V01	PID	Traveler Account Management	The CPS shall provide landing pages for the PID to allow Travelers to manage account information in the CPS Back Office.	MMTPA/CPS-UN006-v02	Demonstration
CPS-FN2646-V01	PID	Application Payment Device	The PID shall accept payment device updates from the CPS Back Office.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN2730-V01	CPS Back Office	Administration	All virtual fare product interfaces presented on the Traveler's Personal Information Device shall be configurable by authorized City/COTA individuals.	MMTPA/CPS-UN021-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN3132-V01	OS	Payment Broker	The payment broker shall debit Traveler shared accounts when a payment is executed.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN3133-V01	OS	Payment Broker	The payment broker shall credit Service Provider accounts when a payment is executed.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN3134-V01	OS	Shared Account Ledger	The CPS shall provide a shared account ledger in the OS containing anonymous accounts and balances that are linked to User accounts belonging to Service Providers or to Traveler accounts in the CPS. The API with the Service Providers will provide two-way updates of these accounts within 10 seconds of any transactions.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN3135-V01	OS	Payment Broker	The payment broker shall interact with the shared account ledger to validate available funds to complete a payment transaction.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN3136-V01	OS	Payment Broker	The payment broker shall accept payment requests from the MMTPA and EPM application.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN3137-V01	OS	Payment Broker	The payment broker shall accept payment requests from the IVR System.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN3138-V01	OS	Payment Broker	The payment broker shall accept payment requests from the MMTPA on the HUBS.	MMTPA/CPS-UN022-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN3139-V01	CPS Back Office	Pay Processing	The CPS shall be capable of providing mobile proof of payment (ticket, bar code, QR code, or other) as needed for the validation on Service Provider field equipment.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN3140-V01	CPS Back Office	Traveler Accounts	The CPS shall allow the dollar amount threshold used to trigger automatic withdrawals to be adjusted by the Traveler in increments of $10 up to a maximum amount of $100.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN3141-V01	CPS Web Portal	Account Management	Inquiries from Travelers regarding payments or account status shall be answered by the Offeror within one business day.	MMTPA/CPS-UN013-v02	Demonstration
CPS-FN3142-V01	COTA Farebox	Payment Device Reader	The onboard process may be integrated with the existing optical scanner and onboard network of the COTA fareboxes.	MMTPA/CPS-UN019-v02 MMTPA/CPS-UN021-v02	Demonstration
CPS-FN3143-V01	COTA Farebox	Payment Device Reader	The onboard process shall notify the COTA bus driver of successful payment through visual and audio indicators onboard the bus.	MMTPA/CPS-UN019-v02 MMTPA/CPS-UN021-v02	Demonstration
CPS-FN3144-V01	CPS Web Portal	Account Management	The CPS shall provide a secure Web Portal to allow Service Providers to manage accounts in the CPS Back Office.	MMTPA/CPS-UN028-v02 MMTPA/CPS-UN040-v02	Demonstration
CPS-FN3145-V01	CPS Web Portal	Account Management	The CPS shall provide a Web Portal to allow Travelers to create and manage accounts in the CPS Back Office.	MMTPA/CPS-UN028-v02	Demonstration

ReqID	FG	Sub-Component	Description	References	Verification Method
CPS-FN3146-V01	CPS Back Office	Traveler Accounts	The CPS shall include the capability to load cash at COTA TVMs to fund a Traveler account.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN3147-V01	CPS Back Office	Traveler Accounts	The CPS may include the capability for POS reloads of Traveler accounts at third-party retailers.	MMTPA/CPS-UN022-v02	Demonstration
CPS-FN3148-V01	CPS Back Office	Reporting	Financial audit reports shall include Service Provider reconciliation of trips made and paid for.	MMTPA/CPS-UN038-v02	Demonstration
CPS-FN3149-V01	COTA Farebox	Payment Device Reader	The CPS shall provide a means to confirm payment of a mobile device onboard the COTA buses.	MMTPA/CPS-UN021-v02	Demonstration
CPS-FN3150-V01	CPS Back Office	Incentives and Rewards	Service Providers should be able to create, view, and manage discounts and incentives offered through the CPS.	MMTPA/CPS-UN011-v02	Demonstration
CPS-FN3151-V01	Personal Information Device	Application Payment Device	Payment device updates from the CPS Back Office shall consist of virtual fare products in the form of mobile e-tickets, QR codes, bar codes, and other types of activation codes to interact with the Farebox, Mobility Provider Equipment, TVMs, or POS terminals.	MMTPA/CPS-UN021-v02	Demonstration

Source: City of Columbus

3.2. PERFORMANCE REQUIREMENTS

This section provides the performance requirements (PR) for the system of interest (i.e. what the system will do). **Table 12: Performance Requirements** lists the system-related performance requirements.

Table 12: Performance Requirements

ReqID	Description	References	Verification Method
CPS-PR2718-V01	The CPS Offeror shall be able to measure data input/output latency on their servers by time-stamping request and response times and provide these statistics accurately for assessing performance against requirement CPS-PR2717-V01.	MMTPA/CPS-UN028-v02 MMTPA/CPS-UN022-v02	Analyze
CPS-PR3152-V01	The system shall be able to update shared accounts with a response time of roughly 10 seconds or less.	MMTPA/CPS-UN022-v02 CPS-IX2818-V01 CPS-IX2819-V01 CPS-IX2820-V01 CPS-IX2821-V01 CPS-IX2822-V01 CPS-IX2823-V01 CPS-IX2824-V01	Analyze
CPS-PR3153-V01	The payment broker shall be able to validate funds with a response time of roughly 1 second or less.	MMTPA/CPS-UN022-v02 CPS-IX2839-V01 CPS-IX2840-V01 CPS-IX2841-V01 CPS-IX2842-V01 CPS-IX2843-V01 CPS-IX2844-V01	Analyze

Source: City of Columbus

3.3. INTERFACE REQUIREMENTS

The CPS interfaces allow dynamic and configurable functionality between internal components of the Smart Columbus SoS and external systems that provide data or some other stated functionality, as per the user needs. **Table 13: Interface Requirements** lists the system-related interface requirements.

Table 13: Interface Requirements

ReqID	Description	References	Verification Method
CPS-IF2724-V01	All User interfaces with which Travelers and Providers shall interact shall be protected by Username and password, such that no unauthorized individual shall gain access to any of the system features.	CPS-CN2815-V01	Inspection
CPS-IF2725-V01	All User interfaces shall be available in English and Spanish language.	MMTPA/CPS-UN032-v02	Inspection
CPS-IF2726-V01	All User interfaces shall include dynamic user prompts in the form of text and graphic aids.	MMTPA/CPS-UN012-v02	Inspection
CPS-IF2727-V01	All User interfaces shall adhere to Web Content Accessibility Guidelines (WCAG) 2.1 for accessibility.	MMTPA/CPS-UN012-v02	Inspection
CPS-IF2728-V01	All User interfaces shall be consistent with Smart City/Smart Columbus branding.	MMTPA/CPS-UN012-v02	Inspection
CPS-IF3159-V01	The CPS shall provide an interface to send payment request information (amount, request type, trip ID, Traveler, Provider) and request for funds availability from the Traveler's personal information device to OS.	MMTPA/CPS-UN006-v02 CPS-IX2817-V01	Inspection
CPS-IF3160-V01	The CPS shall provide an interface to send payment request information (amount, request type, trip ID, Traveler, Provider) and funds availability request to from the Traveler's Web Portal to OS.	MMTPA/CPS-UN006-v02 CPS-IX2818-V01	Inspection
CPS-IF3161-V01	The CPS shall provide an interface to allow a third-party IVR system to send requests for payment (amount, request type, activation code) and requests for funds availability to the payment broker in the OS.	MMTPA/CPS-UN016-v02 CPS-IX2819-V01	Inspection

ReqID	Description	References	Verification Method
CPS-IF3162-V01	The CPS shall provide an interface to allow kiosks at HUBSs to send payment request information (amount, request type, trip ID, Traveler, Provider) and requests for funds availability to the payment broker in the OS.	MMTPA/CPS-UN006-v02 CPS-IX2820-V01	Inspection
CPS-IF3163-V01	The CPS shall provide an interface to send payment authorization and funds availability from the OS to the Traveler's personal information device.	MMTPA/CPS-UN006-v02 MMTPA/CPS-UN027-v02 CPS-IX2821-V01	Inspection
CPS-IF3164-V01	The CPS shall provide an interface to send payment authorization and funds availability from the OS to the Traveler's Web Portal.	MMTPA/CPS-UN006-v02 MMTPA/CPS-UN027-v02 CPS-IX2822-V01	Inspection
CPS-IF3165-V01	The CPS shall provide an interface to send payment authorization and funds availability from the OS to a third-party IVR system.	MMTPA/CPS-UN006-v02 MMTPA/CPS-UN027-v02 CPS-IX2823-V01	Inspection
CPS-IF3166-V01	The CPS shall provide an interface to send payment authorization and funds availability from the OS to kiosks at HUBSs.	MMTPA/CPS-UN006-v02 MMTPA/CPS-UN027-v02 CPS-IX2824-V01	Inspection
CPS-IF3167-V01	The CPS shall provide an interface to send transaction information (request ID, amount, request type, Traveler, Provider) from the OS to CPS to be used in payment processing.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN040-v02 CPS-IX2825-V01	Inspection
CPS-IF3168-V01	The CPS shall provide an interface to send payment authorization and funds availability from the CPS to OS.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN040-v02 CPS-IX2826-V01	Inspection
CPS-IF3169-V01	The CPS shall provide an interface to send activation code and phone number (IVR Processing) to CPS landing pages.	MMTPA/CPS-UN016-v02 CPS-IX2827-V01 CPS-IX3194-V01 CPS-IX3195-V01	Inspection
CPS-IF3170-V01	The CPS shall provide an interface to send security credentials, Traveler account information, additions, deletions, modifications, and payment methods from the Traveler's personal information device to CPS.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02 CPS-IX2828-V01	Inspection

ReqID	Description	References	Verification Method
CPS-IF3171-V01	The CPS shall provide an interface to send security credentials, Traveler account information, additions, deletions, modifications, and payment methods from the Traveler's Web Portal to CPS.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02 CPS-IX2829-V01	Inspection
CPS-IF3172-V01	The CPS shall provide an interface to send security credentials, service Provider account information, modifications to service rates and options, report request parameters, and communications requests from the Service Provider's Web Portal to CPS.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN040-v02 CPS-IX2830-V01	Inspection
CPS-IF3173-V01	The CPS shall provide an interface to allow kiosks at HUBSs to send Traveler account information and verification of changes to the CPS.	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02 CPS-IX2831-V01	Inspection
CPS-IF3174-V01	The CPS shall send Traveler account information and verification of account changes to the Traveler's personal information device.	MMTPA/CPS-UN027-v02 CPS-IX2832-V01	Inspection
CPS-IF3175-V01	The CPS shall provide an interface to send Traveler account information and verification of account changes to the Traveler's CPS Web Portal.	MMTPA/CPS-UN016-v02 MMTPA/CPS-UN027-v02 CPS-IX2833-V01	Inspection
CPS-IF3176-V01	The CPS shall provide an interface to send report information and verification of Service Provider account changes to the Service Provider's CPS Web Portal.	MMTPA/CPS-UN022-v02 CPS-IX2834-V01	Inspection
CPS-IF3177-V01	The CPS shall send Traveler account information and verification of account changes to kiosks at the HUBSs.	MMTPA/CPS-UN022-v02 CPS-IX2835-V01	Inspection
CPS-IF3178-V01	The CPS shall provide an interface to send payment methods to be displayed by QR code, bar code, or activation code on the Traveler's personal information device.	MMTPA/CPS-UN021-v02 CPS-IX2836-V01	Inspection

ReqID	Description	References	Verification Method
CPS-IF3179-V01	The CPS shall provide an interface to send QR code, bar code, or activation code from the Traveler's personal information device to Mobility Provider equipment to authorize transaction.	MMTPA/CPS-UN021-v02 CPS-IX2837-V01	Inspection
CPS-IF3180-V01	The CPS shall provide an interface to send QR code, bar code, or activation code from the Traveler's personal information device to the farebox using existing hardware or direct network connection.	MMTPA/CPS-UN021-v02 CPS-IX2838-V01	Inspection
CPS-IF3181-V01	The CPS shall provide an interface to allow COTA to send User account information to the shared account ledger in the OS.	MMTPA/CPS-UN022-v02 CPS-IX2839-V01	Inspection
CPS-IF3182-V01	The CPS shall provide an interface to allow Mobility Provider Central Systems to send User account information to the shared account ledger in the OS.	MMTPA/CPS-UN022-v02 CPS-IX2840-V01	Inspection
CPS-IF3183-V01	The CPS shall provide an interface to allow EPMCS to send User account information to the shared account ledger in the OS.	MMTPA/CPS-UN022-v02 CPS-IX2841-V01	Inspection
CPS-IF3184-V01	The CPS shall provide an interface to send shared account updates from the OS to COTA.	MMTPA/CPS-UN022-v02 CPS-IX2842-V01	Inspection
CPS-IF3185-V01	The CPS shall provide an interface to send shared account updates from the OS to Mobility Provider Central Systems.	MMTPA/CPS-UN022-v02 CPS-IX2843-V01	Inspection
CPS-IF3186-V01	The CPS shall provide an interface to send shared account updates from the OS to EPMCS.	MMTPA/CPS-UN022-v02 CPS-IX2844-V01	Inspection
CPS-IF3187-V01	The CPS shall provide an interface to send requests for payment authorization to financial institutions of Service Providers.	MMTPA/CPS-UN006-v02 CPS-IX2845-V01	Inspection
CPS-IF3188-V01	The CPS shall provide an interface for financial institutions to send payment authorization response to CPS.	MMTPA/CPS-UN006-v02 CPS-IX2846-V01	Inspection
CPS-IF3189-V01	The CPS shall provide an internal interface to add Users from external systems to the shared account ledger in the OS.	MMTPA/CPS-UN022-v02 CPS-IX2856-V01	Inspection

ReqID	Description	References	Verification Method
CPS-IF3190-V01	The CPS shall provide an internal interface to credit the Service Provider's account in exchange for services.	MMTPA/CPS-UN022-v02 CPS-IX2857-V01	Inspection
CPS-IF3191-V01	The CPS shall provide an internal interface to deduct funds from the Traveler's account in exchange for services.	MMTPA/CPS-UN022-v02 CPS-IX2858-V01	Inspection
CPS-IF3192-V01	The CPS shall provide an internal interface to update payment history for both Travers and Service Providers.	MMTPA/CPS-UN033-v02 CPS-IX2859-V01	Inspection

Source: City of Columbus

3.4. DATA REQUIREMENTS

The data requirements (DR) for the system of interest define the data collected, transformed and stored from various sources and identifies new data that is expected to be generated. **Table 14: Data Requirements** lists the system-related data requirements.

Table 14: Data Requirements

ReqID	Description	References	Verification Method
CPS-DR2647-V01	The CPS shall provide anonymous payment data to the OS for storage in accordance with OS practices.	MMTPA/CPS-UN033-v02 CPS-CN2816-V01	Demonstration
CPS-DR2715-V01	Payment data shall be linked to trip data (origin, destination, start time, end time, mode, transfer, transfer time, transfer location, disembarked location, embarked location) using a common identifier.	MMTPA/CPS-UN033-v02 CPS-CN2816-V01	Demonstration
CPS-DR2716-V01	User feedback shall be stored in the OS.	MMTPA/CPS-UN013-v02 CPS-CN2816-V01	Demonstration
CPS-DR2764-V01	The PID shall collect payment data from CPS Landing Pages.	MMTPA/CPS-UN007-v02	Demonstration
CPS-DR2765-V01	The PID shall not store the collected payment data.	MMTPA/CPS-UN007-v02	Demonstration
CPS-DR2766-V01	The WEB shall collect payment data from CPS Landing Pages.	MMTPA/CPS-UN028-v02	Demonstration
CPS-DR2767-V01	The WEB shall not store the collected payment data.	MMTPA/CPS-UN028-v02	Demonstration

ReqID	Description	References	Verification Method
CPS-DR2768-V01	The IVR shall collect payment data from the Traveler.	MMTPA/CPS-UN016-v02	Demonstration
CPS-DR2769-V01	The IVR shall not store the collected payment data.	MMTPA/CPS-UN016-v02	Demonstration
CPS-DR2770-V01	The HUBS shall collect payment data from CPS Landing Pages.	MMTPA/CPS-UN016-v02	Demonstration
CPS-DR2771-V01	The HUBS shall not store the collected payment data.	MMTPA/CPS-UN016-v02	Demonstration
CPS-DR2772-V01	The CPS Back Office shall store payment data in a PCI compliant environment.	MMTPA/CPS-UN029-v02	Demonstration
CPS-DR2773-V01	The CPS Back Office shall manage Traveler account data.	MMTPA/CPS-UN022-v02	Demonstration
CPS-DR2774-V01	The CPS Back Office shall manage Provider account data.	MMTPA/CPS-UN040-v02	Demonstration
CPS-DR2775-V01	The storage time of anonymous payment data in the OS shall be configurable up to a maximum of 10 years by the City/COTA.	MMTPA/CPS-UN033-v02	Demonstration
CPS-DR2776-V01	The CPS shall generate QR code, bar code, NFC, BLE or activation code, as appropriate.	MMTPA/CPS-UN021-v02	Demonstration
CPS-DR2777-V01	The CPS shall reconcile Provider account data on a daily, weekly, or monthly basis.	MMTPA/CPS-UN021-v02	Demonstration

Source: City of Columbus

3.5. SECURITY REQUIREMENTS

The security requirements (SR) for the system of interest specify what is necessary to protect the integrity and operability of the system, its microservices, connections, and data. This includes physical security as well as cyber prevention, detection, identification, response and recovery requirements. **Table 15: Security Requirements** lists the system-related security requirements.

Table 15: Security Requirements

ReqID	Description	References	Verification Method
CPS-SR2508-V01	The CPS shall include secure PCI compliant Traveler accounts.	MMTPA/CPS-UN022-v02	Demonstration

ReqID	Description	References	Verification Method
CPS-SR2558-V01	The CPS shall be fully compliant with PCI standards, including ensuring that all customer credit card payments completed using the system shall not allow any access to or storage of credit card numbers on any City or COTA-operated computers.	MMTPA/CPS-UN029-v02	Demonstration
CPS-SR2584-V01	The CPS shall only be accessible by authorized individuals, controlled using login and password protection.	MMTPA/CPS-UN022-v02	Test
CPS-SR2585-V01	Travelers shall have the ability to reset a lost password.	MMTPA/CPS-UN022-v02	Test
CPS-SR2586-V01	Service Providers shall have the ability to reset a lost password.	MMTPA/CPS-UN040-v02	Test
CPS-SR2587-V01	Traveler account passwords shall have a minimum of 12 characters with a mix of upper- and lower-case, alphanumeric and special characters.	MMTPA/CPS-UN022-v02	Test
CPS-SR2588-V01	Service Provider account passwords shall have a minimum of 12 characters with a mix of upper- and lower-case, alphanumeric and special characters.	MMTPA/CPS-UN040-v02	Test
CPS-SR2589-V01	Travelers who have not accessed an account in 90 days or more shall be required to reset password upon next login.	MMTPA/CPS-UN022-v02	Test
CPS-SR2590-V01	Service Providers who have not accessed an account in 90 days of more shall be required to reset password upon next login.	MMTPA/CPS-UN040-v02	Test
CPS-SR2648-V01	All systems, subsystems and devices shall only allow access to authorized User classes.	MMTPA/CPS-UN031-v02	Test
CPS-SR2649-V01	All security breach detections shall be confidential, and accessible only to Users of the appropriate class.	MMTPA/CPS-UN031-v02	Test

ReqID	Description	References	Verification Method
CPS-SR2650-V01	Security provisions for communications networks shall be described.	MMTPA/CPS-UN031-v02	Test
CPS-SR2651-V01	For all data transactions, the system security shall include authentication features to verify that all claimed source, recipient or User identities are correct and valid.	MMTPA/CPS-UN031-v02	Test
CPS-SR2652-V01	All APIs should use security keys.	MMTPA/CPS-UN031-v02	Test
CPS-SR2653-V01	All accounts shall be monitored for traffic volume to detect denial of service (DoS) attacks.	MMTPA/CPS-UN031-v02	Test
CPS-SR2654-V01	The CPS shall be architected and fortified to defend against DoS attacks.	MMTPA/CPS-UN031-v02	Test
CPS-SR2655-V01	All data transactions shall include non-repudiation features to verify message content, and resolve claims that data was not correctly originated or received by a certain User.	MMTPA/CPS-UN031-v02	Test
CPS-SR2656-V01	The CPS security shall provide features to maintain data integrity, including error checking, error monitoring, error handling and encryption.	MMTPA/CPS-UN031-v02	Test
CPS-SR2657-V01	The CPS shall include verification features to confirm that there have been no losses of data at any point in the data transfers.	MMTPA/CPS-UN031-v02	Test
CPS-SR2658-V01	The CPS shall include verification features to confirm that there have been no unauthorized changes to, or destruction of, data.	MMTPA/CPS-UN031-v02	Test
CPS-SR2659-V01	The CPS shall include features to automatically detect, correct and prevent the propagation of invalid or erroneous data throughout the system.	MMTPA/CPS-UN031-v02	Test
CPS-SR2719-V01	The Offeror shall perform security testing to verify the system security at least once per year.	MMTPA/CPS-UN031-v02	Test

ReqID	Description	References	Verification Method
CPS-SR2720-V01	Security testing shall include penetration and vulnerability testing.	MMTPA/CPS-UN031-v02	Test
CPS-SR2721-V01	The CPS shall provide secure communications, including certificates management.	MMTPA/CPS-UN031-v02	Test
CPS-SR2722-V01	The Offeror shall perform external threat assessment for the Web Portal and landing pages.	MMTPA/CPS-UN031-v02	Test
CPS-SR2723-V01	Communication between external systems and the CPS shall operate in an encrypted, end-to-end connection.	MMTPA/CPS-UN031-v02	Test
CPS-SR2778-V01	The CPS shall comply with PCI Data Security Standards (DSS) Version 3.2.	MMTPA/CPS-UN029-v02	Test
CPS-SR2779-V01	The CPS shall safeguard cardholder data by implementing and maintaining a firewall.	MMTPA/CPS-UN029-v02	Test
CPS-SR2780-V01	The CPS shall create custom passwords and other unique security measures rather than using the default setting from the Offeror-supplied systems.	MMTPA/CPS-UN029-v02	Test
CPS-SR2781-V01	The CPS shall safeguard stored cardholder data.	MMTPA/CPS-UN029-v02	Test
CPS-SR2782-V01	The CPS shall encrypt cardholder data that is transmitted across open, public networks.	MMTPA/CPS-UN029-v02	Test
CPS-SR2783-V01	The CPS Offeror shall implement and update anti-virus software on a weekly basis.	MMTPA/CPS-UN029-v02	Test
CPS-SR2784-V01	Security patches and updates shall be installed within 24 hours after being made available for installation by the Offeror.	MMTPA/CPS-UN029-v02	Test
CPS-SR2785-V01	The CPS shall create and sustain secure systems and applications.	MMTPA/CPS-UN029-v02	Test
CPS-SR2786-V01	The CPS shall keep cardholder access limited by need-to-know.	MMTPA/CPS-UN029-v02	Test

ReqID	Description	References	Verification Method
CPS-SR2787-V01	The CPS shall require unique identifiers for Users with digital access to cardholder data.	MMTPA/CPS-UN029-v02	Test
CPS-SR2788-V01	The CPS shall restrict physical access to cardholder data.	MMTPA/CPS-UN029-v02	Test
CPS-SR2789-V01	The CPS shall require network resources and cardholder data access to be logged and reported.	MMTPA/CPS-UN029-v02	Test
CPS-SR2790-V01	The CPS shall run daily security system and process tests.	MMTPA/CPS-UN029-v02	Test
CPS-SR2791-V01	The CPS shall address information security by creating a policy.	MMTPA/CPS-UN029-v02	Test

Source: City of Columbus

3.6. NON-FUNCTIONAL REQUIREMENTS

The non-functional requirements (NF) for the system of interest specifies define the characteristics of the overall operation of the system such as availability, maintainability, reliability, safety, environmental, human factors, and ergonomics.

3.6.1. Physical Requirements

The physical requirements (PY) specify the physical characteristics of the system, such as material, shape and size, as well as necessary hardware components. **Table 16: Physical Requirements** lists the physical requirements for the system.

Table 16: Physical Requirements

ReqID	Description	References	Verification Method
CPS-PY2660-V01	The CPS shall be capable of mobile device payments by presenting a reservation ID via an encrypted optical code on the device screen, or (if supported by the device) through NFC.	MMTPA/CPS-UN021-v02	Test

Source: City of Columbus

3.6.2. Availability and Recoverability Requirements

The availability and recovery requirements (AR) define the times of day, days of year, and overall percentage the system can be used and when it will not be available for use. It also specifies the recovery time objective of the system, which describes the time frame permitted for a system to become operational, the recovery point objective, which specifies up to what point in time shall the data be

restored, as well as how the system is expected to restore services (e.g. failover, backups, etc.) in an event of a failure. The ability to recover quickly from a system failure or disaster depends on a blend of technologies and having a predefined plan for recovering the data on new hardware, when appropriate. **Table 17: Availability and Recovery Requirements** shows the availability and recovery requirements for the system.

Table 17: Availability and Recovery Requirements

ReqID	Description	References	Verification Method
CPS-AR2710-V01	The system shall provide 99.99% operational availability over a given year.	MMTPA/CPS-UN034-v02	Analyze
CPS-AR2711-V01	The functioning of system features at performance levels as defined in CPS-PR248-v01 shall be used to measure system availability.	MMTPA/CPS-UN034-v02	Analyze
CPS-AR2712-V01	The functioning of system features in compliance with planned maintenance requirements as defined in CPS-MT343-v01 shall be used to measure system availability.	MMTPA/CPS-UN034-v02	Analyze
CPS-AR2713-V01	The City shall retain the ability to determine and modify which system features are to be included or excluded from the system scope to which availability requirements are applied.	MMTPA/CPS-UN034-v02	Analyze
CPS-AR2714-V01	Reduced availability associated with planned maintenance but falling outside the start and/or end times and dates agreed between the City and the Offeror, shall be considered as impacting system availability.	MMTPA/CPS-UN034-v02	Analyze

Source: City of Columbus

3.6.3. Maintainability Requirements

The maintainability requirements (MT) for the system specify the level of effort required to locate and correct an error during operation, establishing a quantitative requirement for planned and unplanned support (e.g. mean and maximum times to repair or resolve issues, number of people and skill levels required, support equipment necessary, maintenance staff hours, time and frequency of preventative maintenance, etc.). **Table 18: Maintainability Requirements** shows the maintainability requirements for the system.

Table 18: Maintainability Requirements

ReqID	Description	References	Verification Method
CPS-MT2948-V01	The Offeror shall be responsible for maintenance of the CPS Back Office and related functions.	MMTPA/CPS-UN034-v02	Demonstration
CPS-MT2949-V01	The Offeror shall be responsible for maintenance of the CPS Landing Pages providing integration with MMTPA and EPM.	MMTPA/CPS-UN034-v02	Demonstration
CPS-MT2950-V01	The Offeror shall be responsible for maintenance of the interfaces between the CPS and external systems identified in the CPS System Requirements document.	MMTPA/CPS-UN034-v02	Demonstration

Source: City of Columbus

3.6.4. Disposal Requirements

The disposal requirements (DP) specify the items related to the disposal of project/system components, due to either failure replacements, removal, end-of-life, upgrade, or retirement. **Table 19: Disposal Requirements** shows the disposal requirements for the system.

Table 19: Disposal Requirements

ReqID	Description	References	Verification Method
CPS-DP2682-V01	The CPS shall remain operational after the completion of the deployment period unless otherwise directed by the City.	MMTPA/CPS-UN034-v02	Analyze

Source: City of Columbus

3.7. ENABLING REQUIREMENTS

The enabling requirements specify details concerning the management of information as well as the production of the system and its lifecycle sustainment, including development, integration, verification, validation, and training.

3.8. ACCEPTANCE TESTING REQUIREMENTS

The acceptance testing requirements (AT) pertain to the requirements for testing the system. **Table 20: Acceptance Testing** shows the acceptance testing requirements for the system.

Table 20: Acceptance Testing

ReqID	Description	References	Verification Method
CPS-AT2921-V01	The Offeror shall undertake testing to demonstrate that all contract requirements have been provided.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2922-V01	All testing shall be conducted according to the approved Acceptance Test Procedures (ATP).	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2923-V01	Testing shall be completed for each release to verify that the requirements have been addressed.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2924-V01	At a minimum, testing shall include (as applicable): verification of necessary functions, communications and operational interfaces.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2925-V01	Testing shall be completed on the system to confirm that the system meets the required functionality.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2926-V01	Testing may be witnessed by City/COTA representatives (City/COTA staff and/or designated support consultants).	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2927-V01	The Offeror shall submit an ATP document for approval prior to undertaking testing.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2928-V01	The ATP shall address how each testable requirement will be demonstrated, including the method for performing the test.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2929-V01	The ATP shall address the results that will constitute success for each test.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2930-V01	The ATP shall address the responsibilities of both the Offeror and City/COTA representatives during each test.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2931-V01	The ATP shall include the test stage(s) at which each requirement will be demonstrated.	MMTPA/CPS-UN034-v02	Demonstration

ReqID	Description	References	Verification Method
CPS-AT2932-V01	A cross-reference shall link each requirement with the ATP test(s) being conducted to demonstrate the requirement.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2933-V01	Dry-run tests shall be conducted by the Offeror prior to the formal start of any testing involving the City/COTA representatives to ensure that successful completion of the formal witnessed tests can be reasonably anticipated.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2934-V01	The Offeror shall notify the City/COTA and receive authorization from the City to proceed with testing.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2935-V01	The Offeror shall allow the City/COTA to witness any tests at each test stage.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2936-V01	Test Results Documentation (TRD) shall be provided upon completion of testing.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2937-V01	Any proposed time for testing shall be approved by the City/COTA.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2938-V01	The TRD shall document version number of each software system component being tested.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2939-V01	The TRD shall document details of the dataset used.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2940-V01	The TRD shall document the result of each ATP procedure.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2941-V01	The TRD shall document which contract requirements have been demonstrated.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2942-V01	The TRD shall document list of failures and open issues identified during testing along with action plan to resolve them.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2943-V01	The TRD shall be approved by the City/COTA before a test stage can be considered complete.	MMTPA/CPS-UN034-v02	Demonstration

ReqID	Description	References	Verification Method
CPS-AT2944-V01	All deficiencies shall be rectified and retested as part of completing each testing stage.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2945-V01	SA shall not be granted until all test stages for that deployment phase are complete and all requirements formally demonstrated through Acceptance Testing.	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2946-V01	A requirement classified as having been demonstrated during a certain Acceptance Testing stage should be subsequently redefined as having been not demonstrated if compliance issues emerge prior to System Acceptance (SA).	MMTPA/CPS-UN034-v02	Demonstration
CPS-AT2947-V01	Any residual deficiencies shall be rectified, together with any outstanding training and documentation having been provided, before City/COTA will grant acceptance.	MMTPA/CPS-UN034-v02	Demonstration

Source: City of Columbus

3.8.1. Information Management Requirements

The information management requirements (IM) specify the acquisition, management, and ownership of information from one or more sources, the custodianship and the distribution of that information to those who need it, and its ultimate disposition through archiving or deletion. **Table 21: Information Management Requirements** shows the information management requirements for the system.

Table 21: Information Management Requirements

ReqID	Description	References	Verification Method
CPS-IM2661-V01	The CPS Back Office shall be hosted external to the City of Columbus.	MMTPA/CPS-UN034-v02	Inspection
CPS-IM2732-V01	The Offeror shall provide overall system schematic and architecture.	MMTPA/CPS-UN034-v02	Inspection
CPS-IM2735-V01	The Offeror shall provide a PCI Compliance Plan demonstrating adherence to PCI DSS 3.2.	MMTPA/CPS-UN034-v02	Inspection

ReqID	Description	References	Verification Method
CPS-IM2736-V01	The Offeror shall provide a System Security Plan, describing security features including fail-over procedure, firewall, data encryption/privacy, management of all encryption keys; and communication.	MMTPA/CPS-UN034-v02	Inspection
CPS-IM2737-V01	The Offeror shall provide a Data Backup and Recovery Plan.	MMTPA/CPS-UN034-v02	Inspection
CPS-IM2738-V01	The System Security Plan shall include documentation for an Annual PCI Compliance audit.	MMTPA/CPS-UN034-v02	Inspection
CPS-IM2739-V01	The Offeror shall demonstrate traceability that all User needs and system requirements have been satisfied.	MMTPA/CPS-UN034-v02	Inspection

Source: City of Columbus

3.8.2. Life-Cycle Sustainability Requirements

The life cycle sustainability requirements (LC) define what items the project or system will review, measure and analyze as part of its commitment to quality during the life cycle of the system. The capacity to change or enhance the product and life cycle processes can be designed into the system architecture to enable the cost-effective sustainment of the system throughout its life cycle. This design attribute should be established early in the system's development to provide a basis for planning each incremental development effort. **Table 22: Life-Cycle Sustainability Requirements** shows the life cycle sustainability requirements for the system.

Table 22: Life-Cycle Sustainability Requirements

ReqID	Description	References	Verification Method
CPS-LC2662-V01	The Offeror shall provide system performance reports on a monthly and on an ad-hoc basis.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2663-V01	Performance reports shall include system availability.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2664-V01	Performance reports shall include system usage, including transactions, payment broker authorizations (failed and approved), PIDs hits and PIDs unique accesses.	MMTPA/CPS-UN034-v02	Demonstration

ReqID	Description	References	Verification Method
CPS-LC2665-V01	Performance reports shall include average and percentile response times.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2666-V01	Performance reports shall include security breaches.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2667-V01	Performance reports shall include attempted security breaches.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2668-V01	Performance reports shall include critical issues observed during the month along with information regarding issue causes and resolutions.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2669-V01	The Offeror shall provide a Quality Assurance/Quality Control (QA/QC) Plan for approval before award of the contract.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2670-V01	The QA/QC Plan shall define principles and processes the Offeror shall follow while developing the system.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2671-V01	The QA/QC Plan shall identify the risk management process the Offeror shall follow, which shall define the risks and critical elements of the system development process, along with the contingency plans to address these.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2672-V01	The QA/QC Plan shall identify the system development, testing, and QA/QC standards the Offeror shall follow while developing the system.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2673-V01	The QA/QC Plan shall identify the error/defect collection and analysis process to ensure that any introduced errors shall be tracked, identified, and eliminated.	MMTPA/CPS-UN034-v02	Demonstration
CPS-LC2674-V01	The QA/QC Plan shall identify the change management practices the Offeror shall follow while developing the system, to ensure that any system development changes and associated reasons are documented.	MMTPA/CPS-UN034-v02	Demonstration

ReqID	Description	References	Verification Method
CPS-LC2675-V01	The QA/QC Plan shall identify the security management process the Offeror shall follow to ensure that the system development follows secure processes and technology and the system achieves the desired security level.	MMTPA/CPS-UN034-v02	Demonstration

Source: City of Columbus

3.8.3. Policy and Regulation Requirements

The policy and regulation requirements (RG) for the system of interest specifies relevant and applicable organizational policies and regulations that affect the development, operation or performance of the system (e.g. IT and labor policies, reports to regulatory agencies, health or safety criteria, etc.). This section also includes new policy and regulation imposed to realize the system. **Table 23: Policy and Regulation Requirements** shows the policy and regulation requirements for the system.

Table 23: Policy and Regulation Requirements

ReqID	Description	References	Verification Method
CPS-RG2676-V01	APIs should follow best practices to achieve the business needs and purposes for which they are designed.	MMTPA/CPS-UN035-v02 CPS-CN2814-V01	Inspection
CPS-RG2677-V01	APIs should be well documented and follow an established coding standard.	MMTPA/CPS-UN035-v02 CPS-CN2814-V01	Inspection
CPS-RG2678-V01	APIs should use a semantic model that is close to the thing it describes (e.g., classes like "payment" and "Traveler").	MMTPA/CPS-UN035-v02 CPS-CN2814-V01	Inspection
CPS-RG2679-V01	The CPS should follow open architecture with well-defined and documented interfaces that are public as opposed to proprietary.	MMTPA/CPS-UN035-v02	Inspection
CPS-RG2680-V01	The CPS shall be responsible for PCI compliance.	MMTPA/CPS-UN036-v02	Inspection

ReqID	Description	References	Verification Method
CPS-RG2681-V01	The CPS shall be responsible for all applicable card transaction security rules and regulations including PCI and DSS compliance, all laws, and any other governing authority requirements as may apply.	MMTPA/CPS-UN036-v02	Inspection
CPS-RG3154-V01	The Offeror shall package applications into a Docker Image to ensure version control, portability, isolation and security.	MMTPA/CPS-UN035-v02	Inspection
CPS-RG3155-V01	The Offeror shall validate the interoperability of their application with other Microservices and the OS core in a sandbox environment.	MMTPA/CPS-UN035-v02	Inspection
CPS-RG3156-V01	The Offeror shall inform the OS architectural team when promotion from the sandbox environment to production is ready, to follow production deployment procedures.	MMTPA/CPS-UN035-v02	Inspection
CPS-RG3157-V01	The Offeror shall provide the ability to monitor the microservice health and performance of externally built applications deployed to the OS Microservice environment to ensure health of the Microservices environment.	MMTPA/CPS-UN035-v02	Inspection

ReqID	Description	References	Verification Method
CPS-RG3158-V01	The Offeror shall provide application production support for failure analysis and remediation commensurate to the contracted SLA to ensure proper operation of the Microservice environment.	MMTPA/CPS-UN035-v02	Inspection

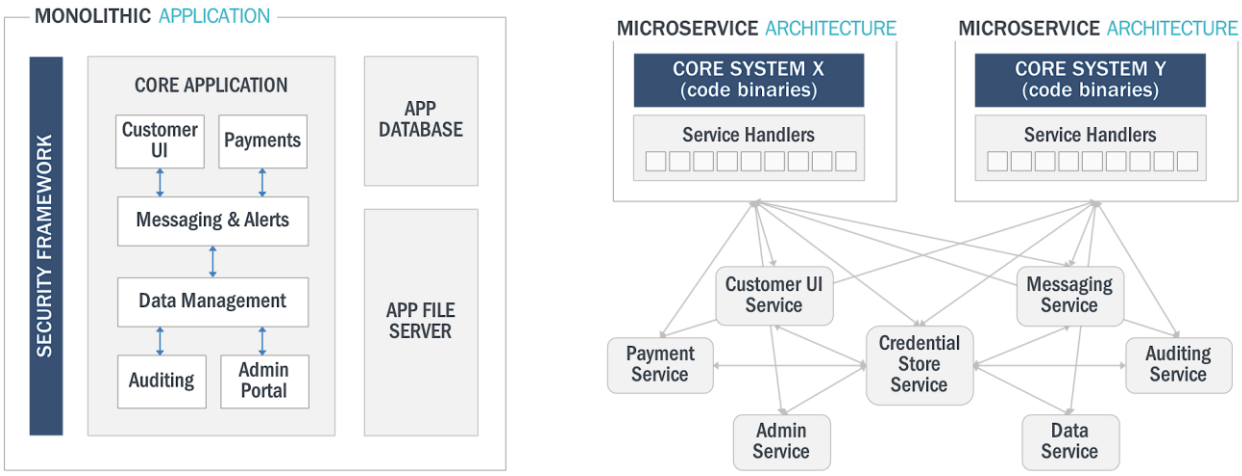
Source: City of Columbus

Chapter 4. Engineering Principles

This section describes engineering principles that guide composition of the CPS.

4.1. REFERENCE ARCHITECTURE

Historically, software systems have been developed as a single, monolithic unit constructed from a blend of hand-built custom technologies. The more features added, the more complicated the system becomes to work with contributing to high-risk, high-maintenance dependencies and a software structure that resembles spaghetti code, making software very difficult and costly to manage over time. The architecture of the Smart Columbus program breaks apart this model by designing a set of small, discrete, independent and standardized processes (i.e., FGs) that produce a service and can be plugged in for a cleaner, more efficient build. **Figure 5: Monolithic Versus Microservice Reference Architecture** provides an illustration of the reference architecture for monolithic verses services by FG.



Source: City of Columbus

Figure 5: Monolithic Versus Microservice Reference Architecture

As **Figure 5** depicts, system features in a monolithic application are hard-wired into the application and cannot be used otherwise. In theory, the entire system would need to be cloned. On the other hand, a modular design allows services to operate independently, making plug-and-play features easy and quick to configure, deploy and scale.

The CPS is mindfully designed to leverage this model to create an SoS targeted for performance, agility and scalability in a manageable way. Each API establishes a set of rules and principles for how the prepackaged FG microservice will integrate. The communications bus will be built over hardware infrastructure and governed by software, which will enable FG microservices to communicate securely while operating independently.

Appendix A. Document Terminology and Conventions

A.1 REQUIREMENT NUMBERING CONVENTION

Each requirement contains a unique ID for traceability and configuration management. Requirements for all projects in the Smart Columbus program will follow the same convention. This identifier contains six elements partitioned into four octets, each representing an identifiable attribute of the requirement. The convention is as follows:

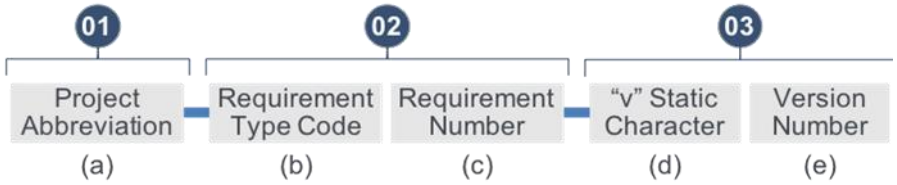


Table 24: Requirements Numbering Convention

	Description	Data Type, Casing	Number of Characters/Digits
Project Abbreviation	The designated Smart Columbus project acronym (e.g. CPS, EPM, etc.)	String, Upper Case	
Requirement Type Code	FN: Functional PR: Performance IF: Interface DR: Data SR: Security RG: Policy and Regulation PY: Physical AR: Availability and Recovery MT: Maintainability ST: Storage and Transport DP: Disposal IM: Information Management LC: Life Cycle Sustainability AT: Acceptance Testing	String, Upper Case	2
Requirement Number	An integer incrementing by one, indicating the number of requirements established.	Integer	3
"v" Static Character	Static letter "v" represents the requirement version.	Character	1
Version Number	An integer incrementing by 1, indicating the number of revisions made to the requirement.	Integer	2

Source: City of Columbus

An example of a Functional Requirement would be “CPS-FN001-v01” in which the following applies:

- The **Project Abbreviation** is “CPS”
- “FN001” is the **Requirement Type Code** coupled with the **3-Digit Requirement Number**
- “v01” is the **“v” Static Character** coupled with the **2-Digit Version Number**

A.2 REQUIREMENTS TABLE HEADINGS

The columns in the requirements tables throughout this document have the following definitions:

- **Req. ID:** a unique identifier providing a reference to a specific requirement.
- **Description:** Statement of the business function or conditions the system must meet.
- **Reference:** Additional requirement(s), documents, standards, etc. relating to the function or condition the system must meet.
- **Verification Method:** Approach to confirming requirement is satisfied.

A.3 CONFORMANCE

Requirements listed in this document use the following terminology:

- SHALL: indicates the definition is an absolute requirement of the specification.
- SHALL NOT: Indicates the definition is an absolute prohibition of the specification.
- SHOULD (RECOMMENDED): Indicates there may exist valid reasons or circumstances to omit a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT (NOT RECOMMENDED): Indicates there may exist valid reasons or circumstances when a particular function of condition is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any function or condition described with this label.
- MAY (OPTIONAL): Indicates an item is truly optional. Some vendors may choose to include or implement Optional Requirements to add value or enhance their overall product while other vendors may omit the same Optional Requirement to reduce cost, increase time to market, etc. An implementation which does not include an Optional Requirement SHALL be interoperable with implementations which does include the Optional Requirement, though perhaps with reduced functionality. In the same vein an implementation which does include an Optional Requirement SHALL be interoperable with an implementation which does not include the Optional Requirement (with the exception for the feature the option provides).

Appendix B. Requirements by System Functional Groups

Table 25: Requirements Organized by Functional Groups organizes requirements defined in **Chapter 3. System Requirements** into its functional groups. This organization is intended for ease of use and quick reference during system design.

Table 25: Requirements Organized by Functional Groups

Functional Group	ReqID	Description
CPS Back Office	CPS-FN2464-V01	The CPS shall perform payment reconciliation with Service Providers for services paid for by Travelers using the CPS.
CPS Back Office	CPS-FN2465-V01	Payment reconciliation between the CPS and Service Providers shall occur at intervals (daily, weekly, or monthly) based on contracted terms with Service Providers.
CPS Back Office	CPS-FN2466-V01	The CPS shall provide secure User account management for electronic payments.
OS	CPS-FN2468-V01	The CPS shall provide an open source payment broker to facilitate payment processing through the shared account ledger.
OS	CPS-FN2469-V01	The payment broker shall not maintain PCI data. The CPS Back Office will maintain PCI data information in a secure environment.
OS	CPS-FN2470-V01	The payment broker shall be deployed as a microservice in the OS.
OS	CPS-FN2471-V01	The payment broker shall accept payment requests from the MMTPA and EPM application on the PID.
CPS Back Office	CPS-FN2472-V01	The CPS shall be capable of processing payment requests for multiple trip segments and multiple service Providers at one time through a "click once" payment functionality in the MMTPA.
CPS Back Office	CPS-FN2473-V01	Traveler accounts shall maintain a balance (stored cash value) so that transactions can be implemented using "click once" functionality (CPS-FN2472-V01) without having to re-enter payment information.
CPS Back Office	CPS-FN2474-V01	The CPS shall have the ability to make automatic withdrawals from a Traveler's payment method on file to replenish a CPS account when the account balance falls below a dollar amount threshold that is set by the Traveler.

Functional Group	ReqID	Description
CPS Web Portal	CPS-FN2475-V01	Travelers shall be able to configure the dollar amount threshold at which the CPS will trigger an automatic withdrawal from a payment method on file to replenish the Traveler's CPS account.
CPS Back Office	CPS-FN2476-V01	The CPS shall trigger a push notification to the Traveler's mobile device when account balance falls below set dollar amount threshold.
CPS Web Portal	CPS-FN2477-V01	Travelers shall have the ability to configure whether to receive text and email alerts when their CPS account is low or has been replenished.
CPS Web Portal	CPS-FN2478-V01	Travelers shall be able to make inquiries pertaining to payments and account status to the CPS Offeror.
CPS Web Portal	CPS-FN2479-V01	The Web Portal shall provide Travelers with access to rules and policies governing CPS usage.
CPS Web Portal	CPS-FN2480-V01	The Web Portal shall provide Travelers with access to current billing status, invoices, and payments.
CPS Web Portal	CPS-FN2481-V01	The Web Portal shall provide Travelers with mechanisms to review and challenge current billing status, invoices, and payments.
CPS Back Office	CPS-FN2482-V01	The CPS shall process and clear payments from Travelers directly through a conventional financial payment gateway, or blockchain gateway, not through a middleman merchant account.
COTA Farebox	CPS-FN2484-V01	An onboard process may be developed to allow COTA fareboxes to read mobile ticket information from the PID. The Offeror shall negotiate any use of the onboard fare management system with Genfare.
CPS Back Office	CPS-FN2487-V01	The CPS shall process requests for payment that are received from the payment broker.
CPS Back Office	CPS-FN2488-V01	The CPS shall allow Travelers to utilize existing COTA period pass products, which permit journeys within the COTA network, subject to time restrictions.
CPS Back Office	CPS-FN2490-V01	The CPS shall allow virtual transfer credits to be used for the purposes of permitting multi-leg transit trips subject to current restrictions in accordance with COTA policies.
CPS Back Office	CPS-FN2491-V01	When applying virtual transfer credits toward a multi-leg transit trip, the remainder of the cost of the trip (if additional charges are required) shall be taken from the Traveler account (stored cash value).
CPS Web Portal	CPS-FN2493-V01	Travelers shall be required to register or provide a Username and password to log into the Web Portal.
CPS Web Portal	CPS-FN2494-V01	Service Providers shall be required to provide a Username and password to log into the Web Portal.

Functional Group	ReqID	Description
CPS Back Office	CPS-FN2495-V01	The CPS shall allow for management of special programs such as Traveler discounts, benefits, and loyalty programs.
CPS Back Office	CPS-FN2496-V01	The CPS should provide the ability to bundle services of multiple Providers (monthly subscription plans).
CPS Back Office	CPS-FN2499-V01	The CPS shall be capable of handling payments for non-emergency medical transportation (NEMT) trips funded through Medicaid accounts. This capability is considered "future state" and shall not be required in the final release of the CPS for the grant.
OS	CPS-FN2500-V01	The CPS shall provide an API to share existing Traveler account information with COTA's CFMS and other Service Providers to the shared account ledger.
CPS Back Office	CPS-FN2503-V01	The CPS shall accept cash, all major US and international credit cards and debit cards (reloadable cards that are not tied to a personal checking account).
CPS Back Office	CPS-FN2504-V01	The CPS shall accept use of electronic wallets (Apple Pay, Android Pay, and Google Pay).
CPS Back Office	CPS-FN2505-V01	The CPS shall provide administrative accounts secured by Username and password for authorized individuals at the City and COTA.
CPS Back Office	CPS-FN2506-V01	Administrative accounts shall include fine-grained permission levels (e.g., View Only, Limited Access, and Full Control).
CPS Back Office	CPS-FN2507-V01	Each User of the system shall be classified into exactly one account type.
CPS Back Office	CPS-SR2508-V01	The CPS shall include secure PCI compliant Traveler accounts.
CPS Back Office	CPS-FN2509-V01	Traveler accounts in the CPS Back Office shall be created and administered by the Traveler.
CPS Back Office	CPS-FN2510-V01	The CPS shall include secure PCI compliant Service Provider accounts.
CPS Web Portal	CPS-FN2511-V01	Service Providers shall administer Service Provider accounts.
CPS Back Office	CPS-FN2512-V01	Service Provider accounts shall be created by authorized individuals at the City and COTA, pending review and approval procedures.
CPS Web Portal	CPS-FN2513-V01	Service Provider accounts shall have administrative parameters for setting rates for base cost per trip, distance, travel time, and surge pricing (if applicable).
CPS Web Portal	CPS-FN2514-V01	Service Providers shall have an API to add their existing Traveler accounts to the shared account ledger.
CPS Back Office	CPS-FN2515-V01	The CPS should include the option for a Traveler to create a guest account to pay for services.
CPS Back Office	CPS-FN2516-V01	Guest accounts should be temporary accounts to facilitate one-time payment transactions.

Functional Group	ReqID	Description
CPS Back Office	CPS-FN2517-V01	Guest accounts should not store credit card information, including CCV numbers, in the CPS.
CPS Back Office	CPS-FN2518-V01	Travelers shall be required to register at least one valid method of payment, as defined in CPS-FN2503-V01 and CPS-FN2504-V01, to create a Traveler account.
CPS Web Portal	CPS-FN2520-V01	Creating a Traveler account shall require submission of contact information.
CPS Web Portal	CPS-FN2521-V01	Contact information shall include first and last name.
CPS Web Portal	CPS-FN2522-V01	Contact information shall include an email address.
CPS Web Portal	CPS-FN2523-V01	Creating a Traveler account shall require submission of three authenticating security questions and answers.
CPS Web Portal	CPS-FN2524-V01	Contact information may include date of birth.
CPS Web Portal	CPS-FN2525-V01	Contact information may include a valid driver's license number.
CPS Web Portal	CPS-FN2526-V01	Contact information shall include a telephone number.
CPS Web Portal	CPS-FN2527-V01	Contact information shall be recorded and treated independently of any personal information related to payments.
CPS Back Office	CPS-FN2528-V01	The CPS shall permit administrative Users with limited access to transfer the balance (stored cash value) of one registered CPS account to another registered CPS account.
CPS Back Office	CPS-FN2529-V01	The CPS shall permit administrative Users to close any account type (e.g. due to prolonged inactivity or abuse of policies).
CPS Web Portal	CPS-FN2530-V01	The CPS shall enable Travelers to enable, disable, and configure auto-reloading by associating a payment medium (e.g., credit card or online payment service, etc.) to a Traveler account.
CPS Web Portal	CPS-FN2531-V01	Auto-reloading shall be configurable to a specific payment medium (e.g., credit card, online payment service, etc.).
CPS Web Portal	CPS-FN2532-V01	Auto-reloading configuration shall include minimum account balance at which point auto-reloading shall be triggered.
CPS Back Office	CPS-FN2533-V01	When validating a stored cash value transaction from a Traveler account, the system shall not permit the stored cash value balance to enter overdraft (i.e., fall below $0.00).
CPS Back Office	CPS-FN2534-V01	The CPS shall permit more than one COTA smart card to be associated with a single Traveler account to allow funds to be transferred between the accounts.
CPS Back Office	CPS-FN2536-V01	The CPS shall associate any COTA issued fare media (including LUM cards) with a registered Traveler account.
CPS Back Office	CPS-FN2537-V01	The CPS shall permit multiple fare media to be associated with a single Traveler account.

Functional Group	ReqID	Description
CPS Back Office	CPS-FN2538-V01	The CPS shall permit payment media to be disassociated from an account without closing the account.
CPS Web Portal	CPS-FN2539-V01	Travelers shall have the ability to close their accounts.
CPS Web Portal	CPS-FN2540-V01	Travelers shall identify a payment method to transfer an existing balance, if applicable, when closing an account.
CPS Back Office	CPS-FN2542-V01	The CPS shall be capable of allowing partner organizations (e.g. Regional Systems) to supply their own payment media.
CPS Back Office	CPS-FN2544-V01	Payment media shall include all major U.S. and international credit and debit cards.
CPS Back Office	CPS-FN2545-V01	The CPS shall provide international post code and zip code verification for fraud protection.
CPS Back Office	CPS-FN2546-V01	Payment media may include PayPal electronic payment services.
CPS Back Office	CPS-FN2547-V01	Payment media shall include reloadable pre-paid debit cards (i.e., not tied to a personal checking account) to facilitate unbanked Travelers.
CPS Back Office	CPS-FN2548-V01	The CPS shall provide a mechanism for external agencies (e.g., paratransit, employers, colleges or universities, or guardians) to subsidize the cost of transportation for a Traveler.
CPS Back Office	CPS-FN2549-V01	The CPS shall provide a mechanism for external agencies (e.g., employers, colleges or universities, or guardians) to subsidize the cost of parking for a Traveler through an authorized validation code or through reoccurring backend Provider.
CPS Web Portal	CPS-FN2550-V01	The Web Portal shall allow Traveler accounts to be tied to an employee benefits program using pre-tax dollars to pay for transportation services.
CPS Web Portal	CPS-FN2551-V01	The Web Portal shall allow Traveler accounts to be tied to an employee benefits program using pre-tax dollars to pay for parking.
CPS Web Portal	CPS-FN2553-V01	The Web Portal shall provide Travelers the option to use either an existing COTA fare product or stored value in CPS account to pay for COTA services.
CPS Back Office	CPS-FN2554-V01	The CPS shall support SPX/Genfare QR codes for payment transactions or provide a viable alternative to satisfy requirements.
CPS Back Office	CPS-FN2555-V01	The CPS shall support use of electronic wallets for payment transactions.
CPS Back Office	CPS-FN2556-V01	The CPS shall be capable of holding funds in reserve for a period of time as a credit guarantee for services where cost is not fixed (such as fares based on surge pricing, distance or duration) or when an event has yet to occur (such as when payment is required at the end of the trip).

Functional Group	ReqID	Description
CPS Back Office	CPS-FN2557-V01	In the event that the service for which the funds are being held is not realized, the hold on the funds shall be removed and credit restored to the Traveler account as necessary.
CPS Back Office	CPS-SR2558-V01	The CPS shall be fully compliant with PCI standards, including ensuring that all customer credit card payments completed using the system shall not allow any access to or storage of credit card numbers on any City or COTA-operated computers.
CPS Back Office	CPS-FN2559-V01	The CPS shall provide the ability for Service Providers to set their fare product structures in the Service Provider Web Portal.
CPS Back Office	CPS-FN2560-V01	The CPS shall be capable of integration with COTA's smart card.
CPS Back Office	CPS-FN2561-V01	The CPS shall provide a mechanism for Travelers who are eligible for COTA's fare subsidy programs to receive those benefits.
CPS Back Office	CPS-FN2566-V01	The CPS Back Office shall retain a record of all account information and transaction history, including data associated with closed accounts, for a minimum of three years.
CPS Back Office	CPS-FN2567-V01	The CPS Back Office shall maintain a transaction log that records all Users that access reports, the reports accessed, edits and changes to the database and the system logon and logoff times.
CPS Back Office	CPS-FN2568-V01	The transaction log shall maintain information for a minimum of one year.
CPS Back Office	CPS-FN2569-V01	The transaction log shall not be editable to even the highest class of administrative User (full control).
CPS Back Office	CPS-FN2570-V01	The CPS shall have the ability to generate financial audit reports (CSV and PDF).
CPS Back Office	CPS-FN2571-V01	Financial audit reports shall include fraudulent account activity where the Traveler has informed administrative Users of unrecognized account transactions.
CPS Back Office	CPS-FN2572-V01	Financial audit reports shall include financial reconciliation and pay settlement.
CPS Back Office	CPS-FN2573-V01	Financial audit reports shall include insufficient funds associated with a Traveler account.
CPS Back Office	CPS-FN2574-V01	Financial audit reports shall include pay transactions by location and trip.
CPS Back Office	CPS-FN2575-V01	Financial audit reports shall include unused and remaining value associated with a Traveler account.
CPS Back Office	CPS-FN2576-V01	Financial audit reports shall include faults and errors.
CPS Back Office	CPS-FN2577-V01	Financial audit reports shall include incomplete transactions.

Functional Group	ReqID	Description
CPS Back Office	CPS-FN2578-V01	Financial audit reports shall include reports of transactions that could not be completed due to missing data.
CPS Back Office	CPS-FN2579-V01	The CPS shall allow authorized individuals to view and export account activity data (CSV and PDF) pertaining to CPS usage associated with Traveler accounts.
CPS Back Office	CPS-FN2580-V01	Account activity data shall include account creation and profile information.
CPS Back Office	CPS-FN2581-V01	Account activity data shall include history of all payment transactions pending and closed.
CPS Back Office	CPS-FN2582-V01	Account activity data shall include balances for both Travelers and Service Providers.
CPS Back Office	CPS-FN2583-V01	Account activity data shall include status of all auto-reload subscriptions associated with each Traveler account.
CPS Back Office	CPS-SR2584-V01	The CPS shall only be accessible by authorized individuals, controlled using login and password protection.
CPS Back Office	CPS-SR2585-V01	Travelers shall have the ability to reset a lost password.
CPS Back Office	CPS-SR2586-V01	Service Providers shall have the ability to reset a lost password.
CPS Back Office	CPS-SR2587-V01	Traveler account passwords shall have a minimum of 12 characters with a mix of upper- and lower-case, alphanumeric and special characters.
CPS Back Office	CPS-SR2588-V01	Service Provider account passwords shall have a minimum of 12 characters with a mix of upper- and lower-case, alphanumeric and special characters.
CPS Back Office	CPS-SR2589-V01	Travelers who have not accessed an account in 90 days or more shall be required to reset password upon next login.
CPS Back Office	CPS-SR2590-V01	Service Providers who have not accessed an account in 90 days of more shall be required to reset password upon next login.
CPS Back Office	CPS-FN2591-V01	Integration with the MMTPA shall provide a seamless User experience for the Traveler by not requiring a separate logon to the MMTPA.
CPS Back Office	CPS-FN2592-V01	Integration with the EPM shall provide a seamless User experience for the Traveler by not requiring a separate logon to the EPM application.
CPS Back Office	CPS-FN2593-V01	The CPS shall provide real-time funding authorization for payment transactions via cellular connectivity.
CPS Back Office	CPS-FN2594-V01	The CPS shall provide the capability for funds to be sourced from stored value in the Traveler account rather than payment media on file.
CPS Back Office	CPS-FN2595-V01	The CPS shall reserve the authorized dollar amount from the stored value in the Traveler account.

Functional Group	ReqID	Description
CPS Back Office	CPS-FN2596-V01	The CPS shall ensure credit card transactions are credited and settled directly to the Traveler account.
CPS Back Office	CPS-FN2597-V01	Service Providers shall be able to create and manage notifications.
COTA Farebox	CPS-FN2598-V01	The CPS may use existing COTA fareboxes for COTA transactions.
COTA Farebox	CPS-FN2599-V01	The CPS should not require installation of new fareboxes or fare validators.
COTA Farebox	CPS-FN2600-V01	The CPS may provide an embedded SDK that extends the functionality of existing COTA fareboxes.
COTA Farebox	CPS-FN2601-V01	The CPS may integrate with the contactless optical code scanner (compliant with ISO 15426-2 for mobile devices) of existing COTA fareboxes.
COTA Farebox	CPS-FN2602-V01	The CPS may integrate with the contactless RFID reader (compliant with ISO 14443 Type A and B standard) of existing COTA fareboxes for NFC-enabled mobile devices.
COTA Farebox	CPS-FN2603-V01	The CPS may integrate with COTA's existing fareboxes to allow recognition of a mobile app presenting a ticket ID via an optical barcode on the device screen, or (if supported by the device) through NFC.
Personal Information Device	CPS-FN2604-V01	Activating and subsequent use of an e-ticket shall cause the ticket to expire from the Traveler account.
Personal Information Device	CPS-FN2605-V01	If the mobile device of the Traveler is NFC-enabled, and compliant with ISO 18092/ISO 21481, the device shall broadcast the same unique serial number that is encoded in the QR code.
CPS Back Office	CPS-FN2606-V01	The CPS should be capable of digitally rendering encrypted optical codes (mobile e-tickets) for optical scanning at Service Provider reader equipment.
CPS Back Office	CPS-FN2607-V01	Mobile e-tickets should be machine readable 2D optical code compliant with ISO-15415, encoding the unique serial number.
CPS Back Office	CPS-FN2608-V01	Mobile e-tickets should serve to create the identifier used to validate and track the ticket and associated transactions in the system.
CPS Back Office	CPS-FN2609-V01	Mobile e-tickets should be human readable text displaying the serial number encoded in the optical code.
CPS Back Office	CPS-FN2610-V01	Optical codes should be encrypted to centralized randomization algorithms.
CPS Back Office	CPS-FN2611-V01	Mobile e-tickets should include security features verifiable by a human inspector (e.g., moving graphic, changing color, real-time clock).

Functional Group	ReqID	Description
Personal Information Device	CPS-FN2612-V01	The screen displaying the e-ticket shall include a soft key to close the mobile e-ticket.
Personal Information Device	CPS-FN2613-V01	Opening the mobile e-ticket page shall set the e-ticket in an active state.
Personal Information Device	CPS-FN2614-V01	An active mobile e-ticket shall remain accessible to the Traveler in an active state for presentation and validation following an unexpected shutdown of the app.
Personal Information Device	CPS-FN2615-V01	Devices that are enabled for Near-Field Communication (NFC), and compliant with ISO 18092 and ISO 21481, shall broadcast the same unique serial number that is encoded in the optical code while the mobile e-ticket remains active.
Personal Information Device	CPS-FN2616-V01	Closing the mobile e-ticket page shall set the e-ticket in an inactive state, clearing the notification from the device's notification center, and terminating any NFC transmission (if applicable).
Personal Information Device	CPS-FN2617-V01	The PID shall provide Travelers with account balance, pass expiration and related service alerts via push notifications and alerts.
CPS Web Portal	CPS-FN2621-V01	The Web Portal shall provide Travelers with the ability to replenish their account.
CPS Web Portal	CPS-FN2622-V01	The Web Portal shall provide Travelers with the ability to manage account information.
CPS Web Portal	CPS-FN2623-V01	The Web Portal shall provide Travelers with the ability to manage payment options.
CPS Web Portal	CPS-FN2624-V01	The Web Portal shall provide Travelers with the ability to manage account information.
CPS Web Portal	CPS-FN2625-V01	The Web Portal shall provide Travelers with the ability to purchase fare products.
CPS Web Portal	CPS-FN2626-V01	The Web Portal shall provide Travelers with the ability to replenish their account.
CPS Web Portal	CPS-FN2627-V01	The Web Portal shall provide Travelers with the ability to manage payment options.
CPS Web Portal	CPS-FN2628-V01	The Web Portal shall enable Service Providers to manage accounts directly, by correctly entering login authentication.
CPS Web Portal	CPS-FN2629-V01	The Web Portal shall enable Travelers to manage accounts directly, by correctly entering login authentication.
CPS Back Office	CPS-FN2630-V01	The CPS shall be capable of notifying Travelers via text, email, or push notification of payment confirmation.
CPS Back Office	CPS-FN2631-V01	The CPS shall permit the entry of US and international profile information to accommodate tourists and visitors to Central Ohio.

Functional Group	ReqID	Description
CPS Web Portal	CPS-FN2632-V01	The Web Portal shall provide the capability to configure notifications and alerts.
CPS Web Portal	CPS-FN2633-V01	The Web Portal shall provide the capability to configure notifications and alerts.
CPS Web Portal	CPS-FN2634-V01	Information relevant to an existing payment(s) (receipt/proof of payment) shall be accessible to the Traveler within the previous three months.
CPS Back Office	CPS-FN2636-V01	The CPS Back Office shall be capable of processing payment requests to generate an activation code to be used for an IVR-requested trip (reference CPS-FN3137-V01).
CPS Back Office	CPS-FN2637-V01	The CPS Back Office shall include a process to transfer the unique trip code purchased using a third-party IVR system to the Traveler by email and by text message.
CPS Back Office	CPS-FN2638-V01	The CPS shall provide Back-Office functions to create and administer a rewards and incentives program.
CPS Back Office	CPS-FN2639-V01	Travelers who earn promotions or rewards or financial incentives for completing multimodal trips using the MMTPA, or through other promotions tied to a Traveler account, shall be able to view and access these rewards or incentives through the Traveler account.
CPS Back Office	CPS-FN2640-V01	For promotions or rewards, a Traveler shall be able to activate the promotion or reward through the Traveler account.
OS	CPS-FN2641-V01	Data posted to the OS from the Payment Broker shall have PII obfuscated so that it may be available to third-party Users.
CPS Back Office	CPS-FN2644-V01	Payment transactions shall be authorized in real time through the CPS.
PID	CPS-FN2645-V01	The CPS shall provide landing pages for the PID to allow Travelers to manage account information in the CPS Back Office.
PID	CPS-FN2646-V01	The PID shall accept payment device updates from the CPS Back Office.
OS	CPS-DR2647-V01	The CPS shall provide anonymous payment data to the OS for storage in accordance with OS practices.
CPS Back Office	CPS-SR2648-V01	All systems, subsystems and devices shall only allow access to authorized User classes.
CPS Back Office	CPS-SR2649-V01	All security breach detections shall be confidential, and accessible only to Users of the appropriate class.
CPS Back Office	CPS-SR2650-V01	Security provisions for communications networks shall be described.
CPS Back Office	CPS-SR2651-V01	For all data transactions, the system security shall include authentication features to verify that all claimed source, recipient or User identities are correct and valid.

Functional Group	ReqID	Description
CPS Back Office	CPS-SR2652-V01	All APIs should use security keys.
CPS Back Office	CPS-SR2653-V01	All accounts shall be monitored for traffic volume to detect denial of service (DoS) attacks.
CPS Back Office	CPS-SR2654-V01	The CPS shall be architected and fortified to defend against DoS attacks.
CPS Back Office	CPS-SR2655-V01	All data transactions shall include non-repudiation features to verify message content, and resolve claims that data was not correctly originated or received by a certain User.
CPS Back Office	CPS-SR2656-V01	The CPS security shall provide features to maintain data integrity, including error checking, error monitoring, error handling and encryption.
CPS Back Office	CPS-SR2657-V01	The CPS shall include verification features to confirm that there have been no losses of data at any point in the data transfers.
CPS Back Office	CPS-SR2658-V01	The CPS shall include verification features to confirm that there have been no unauthorized changes to, or destruction of, data.
CPS Back Office	CPS-SR2659-V01	The CPS shall include features to automatically detect, correct and prevent the propagation of invalid or erroneous data throughout the system.
CPS Back Office	CPS-PY2660-V01	The CPS shall be capable of mobile device payments by presenting a reservation ID via an encrypted optical code on the device screen, or (if supported by the device) through NFC.
CPS Back Office	CPS-IM2661-V01	The CPS Back Office shall be hosted external to the City of Columbus.
CPS Back Office	CPS-LC2662-V01	The Offeror shall provide system performance reports on a monthly and on an ad-hoc basis.
CPS Back Office	CPS-LC2663-V01	Performance reports shall include system availability.
CPS Back Office	CPS-LC2664-V01	Performance reports shall include system usage, including transactions, payment broker authorizations (failed and approved), PIDs hits and PIDs unique accesses.
CPS Back Office	CPS-LC2665-V01	Performance reports shall include average and percentile response times.
CPS Back Office	CPS-LC2666-V01	Performance reports shall include security breaches.
CPS Back Office	CPS-LC2667-V01	Performance reports shall include attempted security breaches.
CPS Back Office	CPS-LC2668-V01	Performance reports shall include critical issues observed during the month along with information regarding issue causes and resolutions.
CPS Back Office	CPS-LC2669-V01	The Offeror shall provide a Quality Assurance/Quality Control (QA/QC) Plan for approval before award of the contract.

Functional Group	ReqID	Description
CPS Back Office	CPS-LC2670-V01	The QA/QC Plan shall define principles and processes the Offeror shall follow while developing the system.
CPS Back Office	CPS-LC2671-V01	The QA/QC Plan shall identify the risk management process the Offeror shall follow, which shall define the risks and critical elements of the system development process, along with the contingency plans to address these.
CPS Back Office	CPS-LC2672-V01	The QA/QC Plan shall identify the system development, testing, and QA/QC standards the Offeror shall follow while developing the system.
CPS Back Office	CPS-LC2673-V01	The QA/QC Plan shall identify the error/defect collection and analysis process to ensure that any introduced errors shall be tracked, identified, and eliminated.
CPS Back Office	CPS-LC2674-V01	The QA/QC Plan shall identify the change management practices the Offeror shall follow while developing the system, to ensure that any system development changes and associated reasons are documented.
CPS Back Office	CPS-LC2675-V01	The QA/QC Plan shall identify the security management process the Offeror shall follow to ensure that the system development follows secure processes and technology and the system achieves the desired security level.
CPS Back Office	CPS-RG2676-V01	APIs should follow best practices to achieve the business needs and purposes for which they are designed.
CPS Back Office	CPS-RG2677-V01	APIs should be well documented and follow an established coding standard.
CPS Back Office	CPS-RG2678-V01	APIs should use a semantic model that is close to the thing it describes (e.g., classes like "payment" and "Traveler").
CPS Back Office	CPS-RG2679-V01	The CPS should follow open architecture with well-defined and documented interfaces that are public as opposed to proprietary.
CPS Back Office	CPS-RG2680-V01	The CPS shall be responsible for PCI compliance.
CPS Back Office	CPS-RG2681-V01	The CPS shall be responsible for all applicable card transaction security rules and regulations including PCI and DSS compliance, all laws, and any other governing authority requirements as may apply.
CPS Back Office	CPS-DP2682-V01	The CPS shall remain operational after the completion of the deployment period unless otherwise directed by the City.
CPS Back Office	CPS-AR2710-V01	The system shall provide 99.99% operational availability over a given year.
CPS Back Office	CPS-AR2711-V01	The functioning of system features at performance levels as defined in CPS-PR248-v01 shall be used to measure system availability.
CPS Back Office	CPS-AR2712-V01	The functioning of system features in compliance with planned maintenance requirements as defined in CPS-MT343-v01 shall be used to measure system availability.

Functional Group	ReqID	Description
CPS Back Office	CPS-AR2713-V01	The City shall retain the ability to determine and modify which system features are to be included or excluded from the system scope to which availability requirements are applied.
CPS Back Office	CPS-AR2714-V01	Reduced availability associated with planned maintenance but falling outside the start and/or end times and dates agreed between the City and the Offeror, shall be considered as impacting system availability.
OS	CPS-DR2715-V01	Payment data shall be linked to trip data (origin, destination, start time, end time, mode, transfer, transfer time, transfer location, disembarked location, embarked location) using a common identifier.
OS	CPS-DR2716-V01	User feedback shall be stored in the OS.
CPS Back Office	CPS-PR2718-V01	The CPS Offeror shall be able to measure data input/output latency on their servers by time-stamping request and response times and provide these statistics accurately for assessing performance against requirement CPS-PR2717-V01.
CPS Back Office	CPS-SR2719-V01	The Offeror shall perform security testing to verify the system security at least once per year.
CPS Back Office	CPS-SR2720-V01	Security testing shall include penetration and vulnerability testing.
CPS Back Office	CPS-SR2721-V01	The CPS shall provide secure communications, including certificates management.
CPS Back Office	CPS-SR2722-V01	The Offeror shall perform external threat assessment for the Web Portal and landing pages.
CPS Back Office	CPS-SR2723-V01	Communication between external systems and the CPS shall operate in an encrypted, end-to-end connection.
CPS Back Office	CPS-IF2724-V01	All User interfaces with which Travelers and Providers shall interact shall be protected by Username and password, such that no unauthorized individual shall gain access to any of the system features.
CPS Back Office	CPS-IF2725-V01	All User interfaces shall be available in English and Spanish language.
CPS Back Office	CPS-IF2726-V01	All User interfaces shall include dynamic User prompts in the form of text and graphic aids.
CPS Back Office	CPS-IF2727-V01	All User interfaces shall adhere to Web Content Accessibility Guidelines (WCAG) 2.1 for accessibility.
CPS Back Office	CPS-IF2728-V01	All User interfaces shall be consistent with Smart City/Smart Columbus branding.
CPS Back Office	CPS-FN2730-V01	All virtual fare product interfaces presented on the Traveler's Personal Information Device shall be configurable by authorized City/COTA individuals.
CPS Back Office	CPS-IM2732-V01	The Offeror shall provide overall system schematic and architecture.

Functional Group	ReqID	Description
CPS Back Office	CPS-IM2735-V01	The Offeror shall provide a PCI Compliance Plan demonstrating adherence to PCI DSS 3.2.
CPS Back Office	CPS-IM2736-V01	The Offeror shall provide a System Security Plan, describing security features including fail-over procedure, firewall, data encryption/privacy, management of all encryption keys; and communication.
CPS Back Office	CPS-IM2737-V01	The Offeror shall provide a Data Backup and Recovery Plan.
CPS Back Office	CPS-IM2738-V01	The System Security Plan shall include documentation for an Annual PCI Compliance audit.
CPS Back Office	CPS-IM2739-V01	The Offeror shall demonstrate traceability that all User needs and system requirements have been satisfied.
Personal Information Device	CPS-DR2764-V01	The PID shall collect payment data from CPS Landing Pages.
Personal Information Device	CPS-DR2765-V01	The PID shall not store the collected payment data.
CPS Web Portal	CPS-DR2766-V01	The WEB shall collect payment data from CPS Landing Pages.
CPS Web Portal	CPS-DR2767-V01	The WEB shall not store the collected payment data.
IVR System	CPS-DR2768-V01	The IVR shall collect payment data from the Traveler.
IVR System	CPS-DR2769-V01	The IVR shall not store the collected payment data.
HUBS	CPS-DR2770-V01	The HUBS shall collect payment data from CPS Landing Pages.
HUBS	CPS-DR2771-V01	The HUBS shall not store the collected payment data.
CPS Back Office	CPS-DR2772-V01	The CPS Back Office shall store payment data in a PCI compliant environment.
CPS Back Office	CPS-DR2773-V01	The CPS Back Office shall manage Traveler account data.
CPS Back Office	CPS-DR2774-V01	The CPS Back Office shall manage Provider account data.
OS	CPS-DR2775-V01	The storage time of anonymous payment data in the OS shall be configurable up to a maximum of 10 years by the City/COTA.
CPS Back Office	CPS-DR2776-V01	The CPS shall generate QR code, bar code, NFC, BLE or activation code, as appropriate.
CPS Back Office	CPS-DR2777-V01	The CPS shall reconcile Provider account data on a daily, weekly, or monthly basis.
CPS Back Office	CPS-SR2778-V01	The CPS shall comply with PCI Data Security Standards (DSS) Version 3.2.
CPS Back Office	CPS-SR2779-V01	The CPS shall safeguard cardholder data by implementing and maintaining a firewall.

Functional Group	ReqID	Description
CPS Back Office	CPS-SR2780-V01	The CPS shall create custom passwords and other unique security measures rather than using the default setting from the Offeror-supplied systems.
CPS Back Office	CPS-SR2781-V01	The CPS shall safeguard stored cardholder data.
CPS Back Office	CPS-SR2782-V01	The CPS shall encrypt cardholder data that is transmitted across open, public networks.
CPS Back Office	CPS-SR2783-V01	The CPS Offeror shall implement and update anti-virus software on a weekly basis.
CPS Back Office	CPS-SR2784-V01	Security patches and updates shall be installed within 24 hours after being made available for installation by the Offeror.
CPS Back Office	CPS-SR2785-V01	The CPS shall create and sustain secure systems and applications.
CPS Back Office	CPS-SR2786-V01	The CPS shall keep cardholder access limited by need-to-know.
CPS Back Office	CPS-SR2787-V01	The CPS shall require unique identifiers for Users with digital access to cardholder data.
CPS Back Office	CPS-SR2788-V01	The CPS shall restrict physical access to cardholder data.
CPS Back Office	CPS-SR2789-V01	The CPS shall require network resources and cardholder data access to be logged and reported.
CPS Back Office	CPS-SR2790-V01	The CPS shall run daily security system and process tests.
CPS Back Office	CPS-SR2791-V01	The CPS shall address information security by creating a policy.
CPS Back Office	CPS-AT2921-V01	The Offeror shall undertake testing to demonstrate that all contract requirements have been provided.
CPS Back Office	CPS-AT2922-V01	All testing shall be conducted according to the approved Acceptance Test Procedures (ATP).
CPS Back Office	CPS-AT2923-V01	Testing shall be completed for each release to verify that the requirements have been addressed.
CPS Back Office	CPS-AT2924-V01	At a minimum, testing shall include (as applicable): verification of necessary functions, communications and operational interfaces.
CPS Back Office	CPS-AT2925-V01	Testing shall be completed on the system to confirm that the system meets the required functionality.
CPS Back Office	CPS-AT2926-V01	Testing may be witnessed by City/COTA representatives (City/COTA staff and/or designated support consultants).
CPS Back Office	CPS-AT2927-V01	The Offeror shall submit an ATP document for approval prior to undertaking testing.
CPS Back Office	CPS-AT2928-V01	The ATP shall address how each testable requirement will be demonstrated, including the method for performing the test.

Functional Group	ReqID	Description
CPS Back Office	CPS-AT2929-V01	The ATP shall address the results that will constitute success for each test.
CPS Back Office	CPS-AT2930-V01	The ATP shall address the responsibilities of both the Offeror and City/COTA representatives during each test.
CPS Back Office	CPS-AT2931-V01	The ATP shall include the test stage(s) at which each requirement will be demonstrated.
CPS Back Office	CPS-AT2932-V01	A cross-reference shall link each requirement with the ATP test(s) being conducted to demonstrate the requirement.
CPS Back Office	CPS-AT2933-V01	Dry-run tests shall be conducted by the Offeror prior to the formal start of any testing involving the City/COTA representatives to ensure that successful completion of the formal witnessed tests can be reasonably anticipated.
CPS Back Office	CPS-AT2934-V01	The Offeror shall notify the City/COTA and receive authorization from the City to proceed with testing.
CPS Back Office	CPS-AT2935-V01	The Offeror shall allow the City/COTA to witness any tests at each test stage.
CPS Back Office	CPS-AT2936-V01	Test Results Documentation (TRD) shall be provided upon completion of testing.
CPS Back Office	CPS-AT2937-V01	Any proposed time for testing shall be approved by the City/COTA.
CPS Back Office	CPS-AT2938-V01	The TRD shall document version number of each software system component being tested.
CPS Back Office	CPS-AT2939-V01	The TRD shall document details of the dataset used.
CPS Back Office	CPS-AT2940-V01	The TRD shall document the result of each ATP procedure.
CPS Back Office	CPS-AT2941-V01	The TRD shall document which contract requirements have been demonstrated.
CPS Back Office	CPS-AT2942-V01	The TRD shall document list of failures and open issues identified during testing along with action plan to resolve them.
CPS Back Office	CPS-AT2943-V01	The TRD shall be approved by the City/COTA before a test stage can be considered complete.
CPS Back Office	CPS-AT2944-V01	All deficiencies shall be rectified and retested as part of completing each testing stage.
CPS Back Office	CPS-AT2945-V01	SA shall not be granted until all test stages for that deployment phase are complete and all requirements formally demonstrated through Acceptance Testing.
CPS Back Office	CPS-AT2946-V01	A requirement classified as having been demonstrated during a certain Acceptance Testing stage should be subsequently redefined as having been not demonstrated if compliance issues emerge prior to System Acceptance (SA).

Functional Group	ReqID	Description
CPS Back Office	CPS-AT2947-V01	Any residual deficiencies shall be rectified, together with any outstanding training and documentation having been provided, before City/COTA will grant acceptance.
CPS Back Office	CPS-MT2948-V01	The Offeror shall be responsible for maintenance of the CPS Back Office and related functions.
CPS Back Office	CPS-MT2949-V01	The Offeror shall be responsible for maintenance of the CPS Landing Pages providing integration with MMTPA and EPM.
CPS Back Office	CPS-MT2950-V01	The Offeror shall be responsible for maintenance of the interfaces between the CPS and external systems identified in the CPS System Requirements document.
OS	CPS-FN3132-V01	The payment broker shall debit Traveler shared accounts when a payment is executed.
OS	CPS-FN3133-V01	The payment broker shall credit Service Provider accounts when a payment is executed.
OS	CPS-FN3134-V01	The CPS shall provide a shared account ledger in the OS containing anonymous accounts and balances that are linked to User accounts belonging to Service Providers or to Traveler accounts in the CPS. The API with the Service Providers will provide two-way updates of these accounts within 10 seconds of any transactions.
OS	CPS-FN3135-V01	The payment broker shall interact with the shared account ledger to validate available funds to complete a payment transaction.
OS	CPS-FN3136-V01	The payment broker shall accept payment requests from the MMTPA and EPM application.
OS	CPS-FN3137-V01	The payment broker shall accept payment requests from the IVR System.
OS	CPS-FN3138-V01	The payment broker shall accept payment requests from the MMTPA on the HUBS.
CPS Back Office	CPS-FN3139-V01	The CPS shall be capable of providing mobile proof of payment (ticket, bar code, QR code, or other) as needed for the validation on Service Provider field equipment.
CPS Back Office	CPS-FN3140-V01	The CPS shall allow the dollar amount threshold used to trigger automatic withdrawals to be adjusted by the Traveler in increments of $10 up to a maximum amount of $100.
CPS Web Portal	CPS-FN3141-V01	Inquiries from Travelers regarding payments or account status shall be answered by the Offeror within one business day.
COTA Farebox	CPS-FN3142-V01	The onboard process may be integrated with the existing optical scanner and onboard network of the COTA fareboxes.
COTA Farebox	CPS-FN3143-V01	The onboard process shall notify the COTA bus driver of successful payment through visual and audio indicators onboard the bus.

Functional Group	ReqID	Description
CPS Web Portal	CPS-FN3144-V01	The CPS shall provide a secure Web Portal to allow Service Providers to manage accounts in the CPS Back Office.
CPS Web Portal	CPS-FN3145-V01	The CPS shall provide a Web Portal to allow Travelers to create and manage accounts in the CPS Back Office.
CPS Back Office	CPS-FN3146-V01	The CPS shall include the capability to load cash at COTA TVMs to fund a Traveler account.
CPS Back Office	CPS-FN3147-V01	The CPS may include the capability for POS reloads of Traveler accounts at third-party retailers.
CPS Back Office	CPS-FN3148-V01	Financial audit reports shall include Service Provider reconciliation of trips made and paid for.
COTA Farebox	CPS-FN3149-V01	The CPS shall provide a means to confirm payment of a mobile device onboard the COTA buses.
CPS Back Office	CPS-FN3150-V01	Service Providers should be able to create, view, and manage discounts and incentives offered through the CPS.
PID	CPS-FN3151-V01	Payment device updates from the CPS Back Office shall consist of virtual fare products in the form of mobile e-tickets, QR codes, bar codes, and other types of activation codes to interact with the Farebox, Mobility Provider Equipment, TVMs, or POS terminals.
OS	CPS-PR3152-V01	The system shall be able to update shared accounts with a response time of roughly 10 seconds or less.
OS	CPS-PR3153-V01	The payment broker shall be able to validate funds with a response time of roughly 1 second or less.
OS	CPS-RG3154-V01	The Offeror shall package applications into a Docker Image to ensure version control, portability, isolation and security.
OS	CPS-RG3155-V01	The Offeror shall validate the interoperability of their application with other Microservices and the OS core in a sandbox environment.
OS	CPS-RG3156-V01	The Offeror shall inform the OS architectural team when promotion from the sandbox environment to production is ready, to follow production deployment procedures.
OS	CPS-RG3157-V01	The Offeror shall provide the ability to monitor the microservice health and performance of externally built applications deployed to the OS Microservice environment to ensure health of the Microservices environment.
OS	CPS-RG3158-V01	The Offeror shall provide application production support for failure analysis and remediation commensurate to the contracted SLA to ensure proper operation of the Microservice environment.
PID	CPS-IF3159-V01	The CPS shall provide an interface to send payment request information (amount, request type, trip ID, Traveler, Provider) and request for funds availability from the Traveler's personal information device to OS.

Functional Group	ReqID	Description
CPS Web Portal	CPS-IF3160-V01	The CPS shall provide an interface to send payment request information (amount, request type, trip ID, Traveler, Provider) and funds availability request to from the Traveler's Web Portal to OS.
IVR	CPS-IF3161-V01	The CPS shall provide an interface to allow a third-party IVR system to send requests for payment (amount, request type, activation code) and requests for funds availability to the payment broker in the OS.
HUBS	CPS-IF3162-V01	The CPS shall provide an interface to allow kiosks at HUBSs to send payment request information (amount, request type, trip ID, Traveler, Provider) and requests for funds availability to the payment broker in the OS.
OS	CPS-IF3163-V01	The CPS shall provide an interface to send payment authorization and funds availability from the OS to the Traveler's PID.
OS	CPS-IF3164-V01	The CPS shall provide an interface to send payment authorization and funds availability from the OS to the Traveler's Web Portal.
OS	CPS-IF3165-V01	The CPS shall provide an interface to send payment authorization and funds availability from the OS to a third-party IVR system.
OS	CPS-IF3166-V01	The CPS shall provide an interface to send payment authorization and funds availability from the OS to kiosks at HUBSs.
OS	CPS-IF3167-V01	The CPS shall provide an interface to send transaction information (request ID, amount, request type, Traveler, Provider) from the OS to CPS to be used in payment processing.
CPS Back Office	CPS-IF3168-V01	The CPS shall provide an interface to send payment authorization and funds availability from the CPS to OS.
IVR	CPS-IF3169-V01	The CPS shall provide an interface to send activation code and phone number (IVR Processing) to the payment broker in the OS.
PID	CPS-IF3170-V01	The CPS shall provide an interface to send security credentials, Traveler account information, additions, deletions, modifications, and payment methods from the Traveler's PID to CPS.
CPS Web Portal	CPS-IF3171-V01	The CPS shall provide an interface to send security credentials, Traveler account information, additions, deletions, modifications, and payment methods from the Traveler's Web Portal to CPS.
CPS Web Portal	CPS-IF3172-V01	The CPS shall provide an interface to send security credentials, service Provider account information, modifications to service rates and options, report request parameters, and communications requests from the Service Provider's Web Portal to CPS.

Functional Group	ReqID	Description
HUBSs	CPS-IF3173-V01	The CPS shall provide an interface to allow kiosks at HUBSs to send Traveler account information and verification of changes to the CPS.
CPS Back Office	CPS-IF3174-V01	The CPS shall send Traveler account information and verification of account changes to the Traveler's personal information device.
CPS Back Office	CPS-IF3175-V01	The CPS shall provide an interface to send Traveler account information and verification of account changes to the Traveler's CPS Web Portal.
CPS Back Office	CPS-IF3176-V01	The CPS shall provide an interface to send report information and verification of Service Provider account changes to the Service Provider's CPS Web Portal.
CPS Back Office	CPS-IF3177-V01	The CPS shall send Traveler account information and verification of account changes to kiosks at the HUBSs.
CPS Back Office	CPS-IF3178-V01	The CPS shall provide an interface to send payment methods to be displayed by QR code, bar code, or activation code on the Traveler's personal information device.
PID	CPS-IF3179-V01	The CPS shall provide an interface to send QR code, bar code, or activation code from the Traveler's personal information device to Mobility Provider equipment to authorize transaction.
PID	CPS-IF3180-V01	The CPS shall provide an interface to send QR code, bar code, or activation code from the Traveler's personal information device to the farebox using existing hardware or direct network connection.
COTA CFMS	CPS-IF3181-V01	The CPS shall provide an interface to allow COTA to send User account information to the shared account ledger in the OS.
Mobility Provider Central Management System	CPS-IF3182-V01	The CPS shall provide an interface to allow Mobility Provider Central Systems to send User account information to the shared account ledger in the OS.
EPMCS	CPS-IF3183-V01	The CPS shall provide an interface to allow EPMCS System to send User account information to the shared account ledger in the OS.
OS	CPS-IF3184-V01	The CPS shall provide an interface to send shared account updates from the OS to COTA.
OS	CPS-IF3185-V01	The CPS shall provide an interface to send shared account updates from the OS to Mobility Provider Central Systems.
OS	CPS-IF3186-V01	The CPS shall provide an interface to send shared account updates from the OS to EPMCS.
CPS Back Office	CPS-IF3187-V01	The CPS shall provide an interface to send requests for payment authorization to financial institutions of Service Providers.

Functional Group	ReqID	Description
Financial Centers	CPS-IF3188-V01	The CPS shall provide an interface for financial institutions to send payment authorization response to CPS.
OS	CPS-IF3189-V01	The CPS shall provide an internal interface to add Users from external systems to the shared account ledger in the OS.
CPS Back Office	CPS-IF3190-V01	The CPS shall provide an internal interface to credit the Service Provider's account in exchange for services.
CPS Back Office	CPS-IF3191-V01	The CPS shall provide an internal interface to deduct funds from the Traveler's account in exchange for services.
CPS Back Office	CPS-IF3192-V01	The CPS shall provide an internal interface to update payment history for both Travers and Service Providers.

Source: City of Columbus

Appendix C. Mapped User Needs

Table 26: Mapped User Needs provides a mapping of each User need established in the ConOps with the requirements that were created based off that User defined in **Chapter 3**. This organization is intended for ease of use and quick reference during system design.

Table 26: Mapped User Needs

USER NEED:	MMTPA/CPS-UN006-v02			USER: Traveler
Title:	**CPS Integration**			
Description:	The MMTPA/CPS system needs to provide Travelers with seamless integration with the CPS. Travelers will be able to view, book, and pay for multimodal services without leaving the MMTPA.			
Priority:	Essential			
Related Requirements, Constraints and System Interfaces				
Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Functional	CPS-FN2464-V01	CPS Back-Office	Payment Processing	The CPS shall perform payment reconciliation with Service Providers for services paid for by Travelers using the CPS.
Functional	CPS-FN2470-V01	OS	Payment Broker	The payment broker shall be deployed as a microservice in the OS.
Functional	CPS-FN2471-V01	OS	Payment Broker	The payment broker shall accept payment requests from the MMTPA and EPM application on the PID.
Functional	CPS-FN2465-V01	CPS Back-Office	Payment Processing	Payment reconciliation between the CPS and Service Providers shall occur at intervals (daily, weekly or monthly) based on contracted terms with Service Providers.

Functional	CPS-FN2645-V01	PID	Traveler Account Management	The CPS shall provide landing pages for the PID to allow Travelers to manage account information in the CPS Back Office.
Functional	CPS-FN2644-V01	CPS Back-Office	Payment Processing	Payment transactions shall be authorized in real time through the CPS.
Interface	CPS-IF3159-V01	Personal Information Device	Payment Request	The CPS shall provide an interface to send payment request information (amount, request type, trip ID, Traveler, Provider) and request for funds availability from the Traveler's personal information device to OS.
Interface	CPS-IF3160-V01	CPS Web Portal	Payment Request	The CPS shall provide an interface to send payment request information (amount, request type, trip ID, Traveler, Provider) and funds availability request to from the Traveler's Web Portal to OS.
Interface	CPS-IF3162-V01	HUBSs	Payment Request	The CPS shall provide an interface to allow kiosks at HUBSs to send payment request information (amount, request type, trip ID, Traveler, Provider) and requests for funds availability to the payment broker in the OS.

Interface	CPS-IF3163-V01	OS	Payment Broker	The CPS shall provide an interface to send payment authorization and funds availability from the OS to the Traveler's personal information device.
Interface	CPS-IF3164-V01	OS	Payment Broker	The CPS shall provide an interface to send payment authorization and funds availability from the OS to the Traveler's Web Portal.
Interface	CPS-IF3165-V01	OS	Payment Broker	The CPS shall provide an interface to send payment authorization and funds availability from the OS to a third-party IVR system.
Interface	CPS-IF3166-V01	OS	Payment Broker	The CPS shall provide an interface to send payment authorization and funds availability from the OS to kiosks at HUBSs.
Interface	CPS-IF3187-V01	CPS Back Office	Payment Processing	The CPS shall provide an interface to send requests for payment authorization to financial institutions of Service Providers.
Interface	CPS-IF3188-V01	Financial Centers	Payment Process	The CPS shall provide an interface for financial institutions to send payment authorization response to CPS.

USER NEED:	MMTPA/CPS-UN007-v02	USER: Traveler
Title:	**Access to Instructions and Educational Material**	
Description:	The MMTPA/CPS system needs to provide Travelers with access to limited instructions for use of the application. Instructions will be accessible within the application, such as help with navigation or how to access account information. Travelers will have access educational material outside of the application, such as links to educational material pertaining to each mode of service to understand how the service works. Access to instructions and educational material does not constitute training, either web-based or in-person.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2479-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with access to rules and policies governing CPS usage.
Data	CPS-DR2764-V01	Personal Information Device	CPS Landing Pages	The PID shall collect payment data from CPS Landing Pages.
Data	CPS-DR2765-V01	Personal Information Device	CPS Landing Pages	The PID shall not store the collected payment data.

USER NEED:	MMTPA/CPS-UN008-v02	USER: Traveler
Title:	**Notifications and Alerts**	
Description:	The MMTPA/CPS system needs to notify Travelers of service disruptions, or if a reserved trip is delayed or canceled. Travelers may configure the types of notifications they receive, including frequency, to provide for better User experience. Travelers will receive personalized traffic information including early warning in case of an increasing travel time to a specific location and possible alternative routes and/or modes. An example of this would be a notice based on predictive traffic information or a travel time forecast. Travelers will be notified when reaching an important step during travel such as an upcoming transfer point. Users also need to be informed when a reserved service is no longer available or is altered. Users need to be provided with notifications or prompts, such as departure times or stop notifications. Options for receiving notifications and alerts should include push notifications, email, and text message.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description

Functional	CPS-FN2617-V01	Personal Information Device	CPS Landing Pages	The PID shall provide Travelers with account balance, pass expiration and related service alerts via push notifications and alerts.
Functional	CPS-FN2630-V01	CPS Back-Office	Notifications and Alerts	The CPS shall be capable of notifying Travelers via text, email, or push notification of payment confirmation.

USER NEED:	**MMTPA/CPS-UN011-v02**	**USER: Traveler**
Title:	**Loyalty, Incentives and Rewards**	
Description:	The MMTPA system needs to provide Travelers with access to incentives and rewards for scheduling and completing multimodal trips using the CPS. Incentives and rewards may include discounted transportation, or points toward coupons that may be earned from participating Mobility Providers, local vendors and merchants. Loyalty programs can be monitored through the system. Gamification may also be used to incentivize multimodal trips. Travelers need to be able view progress towards earning an incentive or reward when logged into the MMTPA to monitor progress. Incentives and rewards will be administered through Back-Office functions of the CPS.	
Priority:	Desirable	

Related Requirements, Constraints, and System Interfaces

Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Functional	CPS-FN2640-V01	CPS Back Office	Incentives and Rewards	For promotions or rewards, a Traveler shall be able to activate the promotion or reward through the Traveler account.
Functional	CPS-FN2638-V01	CPS Back Office	Incentives and Rewards	The CPS shall provide Back-Office functions to create and administer a rewards and incentives program.

Functional	CPS-FN2639-V01	CPS Back Office	Incentives and Rewards	Travelers who earn promotions or rewards or financial incentives for completing multimodal trips using the MMTPA, or through other promotions tied to a Traveler account, shall be able to view and access these rewards or incentives through the Traveler account.
Functional	CPS-FN3150-V01	CPS Back Office	Incentives and Rewards	Service Providers should be able to create, view, and manage discounts and incentives offered through the CPS.

USER NEED:	**MMTPA/CPS-UN012-v02**	**USER: Traveler**
Title:	**Graphical User Interface**	
Description:	The MMTPA/CPS system needs to provide Travelers with a Graphical User Interface (GUI). The GUI needs to display maps, text and other graphical information to allow effective use of the application. Travelers also need an interface to make payments, manage account information, and register payment methods. All interfaces need to be simple to use and facilitate use on a mobile device.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Interface	CPS-IF2726-V01	CPS Back Office	CPS Payment Processing	All User interfaces shall include dynamic User prompts in the form of text and graphic aids.
Interface	CPS-IF2728-V01	CPS Back Office	CPS Payment Processing	All User interfaces shall be consistent with Smart City/Smart Columbus branding.

Interface	CPS-IF2727-V01	CPS Back Office	CPS Payment Processing	All User interfaces shall adhere to Web Content Accessibility Guidelines (WCAG) 2.1 for accessibility.

USER NEED:	**MMTPA/CPS-UN013-v02**	**USER: Traveler**
Title:	**User Feedback**	
Description:	The MMTPA/CPS system needs to provide Travelers with the ability to submit feedback on the app. This information will be used by the City and COTA to determine whether the application is working as intended and to make enhancements. The MMTPA/CPS system also needs to provide Travelers with the ability to submit feedback to Mobility Providers through integration with existing feedback systems.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Data	CPS-DR2716-V01	OS	User Feedback	User feedback shall be stored in the OS.
Functional	CPS-FN3141-V01	CPS Web Portal	Account Management	Inquiries from Travelers regarding payments or account status shall be answered by the Offeror within one business day.

USER NEED:	**MMTPA/CPS-UN016-v02**	**USER: Traveler**
Title:	**IVR System**	
Description:	The MMTPA/CPS system needs to allow Travelers without access to smartphones to utilize the system. It is envisioned that an IVR System may be available to Travelers at HUBSs to schedule a trip. Providing access to the system for Users without access to smartphones is needed to meet a Title VI provision to qualify for NTD funding. Other options, such as a Call Center, are believed to be cost prohibitive.	
Priority:	Desirable	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Data	CPS-DR2769-V01	IVR System	IVR System Request for Payment	The IVR shall not store the collected payment data.
Data	CPS-DR2768-V01	IVR System	IVR System Request for Payment	The IVR shall collect payment data from the Traveler.

Data	CPS-DR2770-V01	HUBS	CPS Landing Pages	The HUBS shall collect payment data from CPS Landing Pages.
Data	CPS-DR2771-V01	HUBS	CPS Landing Pages	The HUBS shall not store the collected payment data.
Functional	CPS-FN2636-V01	CPS Back Office	IVR Processing	The CPS Back Office shall be capable of processing payment requests to generate an activation code to be used for an IVR-requested trip (reference CPS-FN3137-V01).
Functional	CPS-FN2637-V01	CPS Back Office	IVR Processing	The CPS Back Office shall include a process to transfer the unique trip code purchased using a third-party IVR system to the Traveler by email and by text message.
Interface	CPS-IF3161-V01	IVR	Payment Request	The CPS shall provide an interface to allow a third-party IVR system to send requests for payment (amount, request type, activation code) and requests for funds availability to the payment broker in the OS.
Interface	CPS-IF3169-V01	IVR System	IVR Processing	The CPS shall provide an interface to send activation code and phone number (IVR Processing) to the payment broker in the OS.

Interface	CPS-IF3175-V01	CPS Back Office	Traveler Accounts	The CPS shall provide an interface to send Traveler account information and verification of account changes to the Traveler's CPS Web Portal.

USER NEED:	**MMTPA/CPS-UN019-v02**			**USER: Traveler**
Title:	**NFC Integration**			
Description:	The MMTPA/CPS system needs to support NFC and Bluetooth mobile payments, as well as SPX/Genfare QR codes.			
Priority:	Essential			
Related Requirements, Constraints, and System Interfaces				
Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Functional	CPS-FN2602-V01	COTA Farebox	Payment Device Reader	The CPS may integrate with the contactless RFID reader (compliant with ISO 14443 Type A and B standard) of existing COTA fareboxes for NFC-enabled mobile devices.
Functional	CPS-FN2603-V01	COTA Farebox	Payment Device Reader	The CPS may integrate with COTA's existing fareboxes to allow recognition of a mobile app presenting a ticket ID via an optical barcode on the device screen, or (if supported by the device) through NFC.

Functional	CPS-FN2615-V01	Personal Information Device	Application Payment Device	Devices that are enabled for NFC, and compliant with ISO 18092 and ISO 21481, shall broadcast the same unique serial number that is encoded in the optical code while the mobile e-ticket remains active.
Functional	CPS-FN3142-V01	COTA Farebox	Payment Device Reader	The onboard process may be integrated with the existing optical scanner and onboard network of the COTA fareboxes.
Functional	CPS-FN3143-V01	COTA Farebox	Payment Device Reader	The onboard process shall notify the COTA bus driver of successful payment through visual and audio indicators onboard the bus.

USER NEED:	**MMTPA/CPS-UN020-v02**			**USER: Traveler**
Title:	**Electronic Pay Wallets**			
Description:	The MMTPA/CPS system should have the capability to support use of electronic wallets (Apple Pay, Android Pay, Google Pay) and the capability to support contactless Europay, MasterCard, Visa cards.			
Priority:	Desirable			
Related Requirements, Constraints, and System Interfaces				
Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Functional	CPS-FN2555-V01	CPS Back Office	Payment Processing	The CPS shall support use of electronic wallets for payment transactions.

USER NEED:	MMTPA/CPS-UN021-v02	USER: Traveler
Title:	**Mobile Ticketing**	
Description:	The MMTPA/CPS system needs to provide Travelers with access to mobile ticketing. The MMTPA needs to be integrated with COTA's mobile ticketing solution in order to generate COTA fare media. COTA's Fare System may also be responsible for generating barcodes that are used to unlock car-share vehicles. Barcodes need to be transmitted to the Traveler in the same manner as COTA fare media.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2484-V01	COTA Farebox	Payment Device Reader	An onboard process may be developed to allow COTA fareboxes to read mobile ticket information from the PID. The Offeror shall negotiate any use of the onboard fare management system with Genfare.
Functional	CPS-FN2554-V01	CPS Back Office	Payment Processing	The CPS shall support SPX/Genfare QR codes for payment transactions or provide a viable alternative to satisfy requirements.
Functional	CPS-FN2599-V01	COTA Farebox	Payment Device Reader	The CPS should not require installation of new fareboxes or fare validators.
Functional	CPS-FN2612-V01	Personal Information Device	Application Payment Device	The screen displaying the e-ticket shall include a soft key to close the mobile e-ticket.
Functional	CPS-FN2608-V01	CPS Back Office	Payment Device Information	Mobile e-tickets should serve to create the identifier used to validate and track the ticket and associated transactions in the system.

Functional	CPS-FN2610-V01	CPS Back Office	Payment Device Information	Optical codes should be encrypted to centralized randomization algorithms.
Functional	CPS-FN2598-V01	COTA Farebox	Payment Device Reader	The CPS may use existing COTA fareboxes for COTA transactions.
Functional	CPS-FN2600-V01	COTA Farebox	Payment Device Reader	The CPS may provide an embedded SDK that extends the functionality of existing COTA fareboxes.
Functional	CPS-FN2611-V01	CPS Back Office	Payment Device Information	Mobile e-tickets should include security features verifiable by a human inspector (e.g., moving graphic, changing color, real-time clock).
Functional	CPS-FN2609-V01	CPS Back Office	Payment Device Information	Mobile e-tickets should be human readable text displaying the serial number encoded in the optical code.
Functional	CPS-FN2613-V01	Personal Information Device	Application Payment Device	Opening the mobile e-ticket page shall set the e-ticket in an active state.
Functional	CPS-FN2601-V01	COTA Farebox	Payment Device Reader	The CPS may integrate with the contactless optical code scanner (compliant with ISO 15426-2 for mobile devices) of existing COTA fareboxes.
Functional	CPS-FN2606-V01	CPS Back Office	Payment Device Information	The CPS should be capable of digitally rendering encrypted optical codes (mobile e-tickets) for optical scanning at Service Provider reader equipment.

Functional	CPS-FN2607-V01	CPS Back Office	Payment Device Information	Mobile e-tickets should be machine readable 2D optical code compliant with ISO-15415, encoding the unique serial number.
Functional	CPS-FN2604-V01	Personal Information Device	Application Payment Device	Activating and subsequent use of an e-ticket shall cause the ticket to expire from the Traveler account.
Functional	CPS-FN2605-V01	Personal Information Device	Application Payment Device	If the mobile device of the Traveler is NFC-enabled, and compliant with ISO 18092/ISO 21481, the device shall broadcast the same unique serial number that is encoded in the QR code.
Functional	CPS-FN2616-V01	Personal Information Device	Application Payment Device	Closing the mobile e-ticket page shall set the e-ticket in an inactive state, clearing the notification from the device's notification center, and terminating any NFC transmission (if applicable).
Functional	CPS-FN2614-V01	Personal Information Device	Application Payment Device	An active mobile e-ticket shall remain accessible to the Traveler in an active state for presentation and validation following an unexpected shutdown of the app.

Physical	CPS-PY2660-V01	CPS Back Office	Payment Device Information	The CPS shall be capable of mobile device payments by presenting a reservation ID via an encrypted optical code on the device screen, or (if supported by the device) through NFC.
Functional	CPS-FN2730-V01	CPS Back Office	Administration	All virtual fare product interfaces presented on the Traveler's Personal Information Device shall be configurable by authorized City/COTA individuals.
Data	CPS-DR2776-V01	CPS Back Office	CPS Landing Pages	The CPS shall generate QR code, bar code, NFC, BLE or activation code, as appropriate.
Data	CPS-DR2777-V01	CPS Back Office	CPS Payment Processing	The CPS shall reconcile Provider account data on a daily, weekly, or monthly basis.
Interface	CPS-IF3178-V01	CPS Back Office	Payment Information	The CPS shall provide an interface to send payment methods to be displayed by QR code, bar code, or activation code on the Traveler's personal information device.
Interface	CPS-IF3179-V01	Personal Information Device	Payment Method	The CPS shall provide an interface to send QR code, bar code, or activation code from the Traveler's personal information device to Mobility Provider equipment to authorize transaction.

Interface	CPS-IF3180-V01	Personal Information Device	Payment Method	The CPS shall provide an interface to send QR code, bar code, or activation code from the Traveler's personal information device to the farebox using existing hardware or direct network connection.
Functional	CPS-FN3139-V01	CPS Back Office	Pay Processing	The CPS shall be capable of providing mobile proof of payment (ticket, bar code, QR code, or other) as needed for the validation on Service Provider field equipment.
Functional	CPS-FN3142-V01	COTA Farebox	Payment Device Reader	The onboard process may be integrated with the existing optical scanner and onboard network of the COTA fareboxes.
Functional	CPS-FN3143-V01	COTA Farebox	Payment Device Reader	The onboard process shall notify the COTA bus driver of successful payment through visual and audio indicators onboard the bus.
Functional	CPS-FN3149-V01	COTA Farebox	Payment Device Reader	The CPS shall provide a means to confirm payment of a mobile device onboard the COTA buses.

Functional	CPS-FN3151-V01	Personal Information Device	Application Payment Device	Payment device updates from the CPS Back Office shall consist of virtual fare products in the form of mobile e-tickets, QR codes, bar codes, and other types of activation codes to interact with the Farebox, Mobility Provider Equipment, TVMs, or POS terminals.

USER NEED:	**MMTPA/CPS-UN022-v02**	**USER: Traveler**
Title:	**CPS Account**	
Description:	The MMTPA/CPS system needs to provide Travelers with the ability to create an account through a one-time setup process that prompts Users for billing information (e.g., cash, credit/debit cards, prepaid debit cards, or other electronic payment). Account information should include the following, at a minimum: first and last name, date of birth, telephone number, email address, mailing address, and authenticating security question and answer. This information will be independent of any personal information related to connection of payment accounts. Once an account is created, the Traveler will be able to log in using an ID and password. Travelers who do not wish to create a CPS account will be able to create a temporary account for issuing a one-time payment. Travelers need to be able to recover lost passwords and have the ability to delete their CPS account if desired. Travelers need to be able to create a guest Account to make payments using the CPS, but payment information is not stored and the account is not permanent. The guest account will be available for Users who do not wish to create a permanent CPS account. Travelers need the CPS to provide the ability to register multiple forms of payment and to specify a default payment method to be used when paying for transportation services or parking services. Users will need to be able to set a preferred payment method. There may be times when a User's preferred payment method cannot be used, for example, if a preferred credit card has expired, in which case, another payment method may be substituted. Also, the availability of certain payment methods may be limited based on a service being used to complete the transaction. For example, there may be restrictions on the types of payment for a service. Mobility Providers will be required to establish merchant accounts in the CPS to receive payment in exchange for services offered through the MMTPA.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Functional	CPS-FN2480-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with access to current billing status, invoices, and payments.

Functional	CPS-FN2478-V01	CPS Web Portal	Account Management	Travelers shall be able to make inquiries pertaining to payments and account status to the CPS Offeror.
Security	CPS-SR2508-V01	CPS Back Office	PCI Compliance	The CPS shall include secure PCI compliant Traveler accounts.
Functional	CPS-FN2510-V01	CPS Back Office	Provider Accounts	The CPS shall include secure PCI compliant Service Provider accounts.
Functional	CPS-FN2475-V01	CPS Web Portal	Account Management	Travelers shall be able to configure the dollar amount threshold at which the CPS will trigger an automatic withdrawal from a payment method on file to replenish the Traveler's CPS account.
Functional	CPS-FN2481-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with mechanisms to review and challenge current billing status, invoices, and payments.
Functional	CPS-FN2474-V01	CPS Back Office	Traveler Accounts	The CPS shall have the ability to make automatic withdrawals from a Traveler's payment method on file to replenish a CPS account when the account balance falls below a dollar amount threshold that is set by the Traveler.

Functional	CPS-FN2500-V01	OS	Shared Account Ledger	The CPS shall provide an API to share existing Traveler account information with COTA's CFMS and other Service Providers to the shared account ledger.
Functional	CPS-FN2515-V01	CPS Back Office	Guest Accounts	The CPS should include the option for a Traveler to create a guest account to pay for services.
Functional	CPS-FN2516-V01	CPS Back Office	Guest Accounts	Guest accounts should be temporary accounts to facilitate one-time payment transactions.
Functional	CPS-FN2517-V01	CPS Back Office	Guest Accounts	Guest accounts should not store credit card information, including CCV numbers, in the CPS.
Functional	CPS-FN2507-V01	CPS Back Office	Administration	Each User of the system shall be classified into exactly one account type.
Functional	CPS-FN2509-V01	CPS Back Office	Traveler Accounts	Traveler accounts in the CPS Back Office shall be created and administered by the Traveler.
Functional	CPS-FN2525-V01	CPS Web Portal	Account Management	Contact information may include a valid driver's license number.
Functional	CPS-FN2518-V01	CPS Back Office	Traveler Accounts	Travelers shall be required to register at least one valid method of payment, as defined in CPS-FN2503-V01 and CPS-FN2504-V01, to create a Traveler account.

Functional	CPS-FN2522-V01	CPS Web Portal	Account Management	Contact information shall include an email address.
Functional	CPS-FN2523-V01	CPS Web Portal	Account Management	Creating a Traveler account shall require submission of three authenticating security questions and answers.
Functional	CPS-FN2520-V01	CPS Web Portal	Account Management	Creating a Traveler account shall require submission of contact information.
Functional	CPS-FN2521-V01	CPS Web Portal	Account Management	Contact information shall include first and last name.
Functional	CPS-FN2530-V01	CPS Web Portal	Account Management	The CPS shall enable Travelers to enable, disable, and configure auto-reloading by associating a payment medium (e.g., credit card or online payment service, etc.) to a Traveler account.
Functional	CPS-FN2546-V01	CPS Back Office	Traveler Accounts	Payment media may include PayPal electronic payment services.
Functional	CPS-FN2544-V01	CPS Back Office	Traveler Accounts	Payment media shall include all major U.S. and international credit and debit cards.
Functional	CPS-FN2553-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers the option to use either an existing COTA fare product or stored value in CPS account to pay for COTA services.
Functional	CPS-FN2531-V01	CPS Web Portal	Account Management	Auto-reloading shall be configurable to a specific payment medium (e.g., credit card, online payment service, etc.).

Functional	CPS-FN2542-V01	CPS Back Office	Traveler Accounts	The CPS shall be capable of allowing partner organizations (e.g. Regional Systems) to supply their own payment media.
Functional	CPS-FN2532-V01	CPS Web Portal	Account Management	Auto-reloading configuration shall include minimum account balance at which point auto-reloading shall be triggered.
Functional	CPS-FN2547-V01	CPS Back Office	Traveler Accounts	Payment media shall include reloadable pre-paid debit cards (i.e., not tied to a personal checking account) to facilitate unbanked Travelers.
Security	CPS-SR2584-V01	CPS Back Office	Traveler Accounts Provider Accounts	The CPS shall only be accessible by authorized individuals, controlled using login and password protection.
Functional	CPS-FN2540-V01	CPS Web Portal	Account Management	Travelers shall identify a payment method to transfer an existing balance, if applicable, when closing an account.
Functional	CPS-FN2524-V01	CPS Web Portal	Account Management	Contact information may include date of birth.
Functional	CPS-FN2526-V01	CPS Web Portal	Account Management	Contact information shall include a telephone number.
Functional	CPS-FN2466-V01	CPS Back Office	Traveler Accounts	The CPS shall provide secure User account management for electronic payments.

Functional	CPS-FN2469-V01	OS	Payment Broker	The payment broker shall not maintain PCI data. The CPS Back Office will maintain PCI data information in a secure environment.
Functional	CPS-FN2594-V01	CPS Back Office	Payment Processing	The CPS shall provide the capability for funds to be sourced from stored value in the Traveler account rather than payment media on file.
Functional	CPS-FN2596-V01	CPS Back Office	Payment Processing	The CPS shall ensure credit card transactions are credited and settled directly to the Traveler account.
Functional	CPS-FN2595-V01	CPS Back Office	Payment Processing	The CPS shall reserve the authorized dollar amount from the stored value in the Traveler account.
Functional	CPS-FN2468-V01	OS	Payment Broker	The CPS shall provide an open source payment broker to facilitate payment processing through the shared account ledger.
Functional	CPS-FN2621-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to replenish their account.
Functional	CPS-FN2545-V01	CPS Back Office	Traveler Accounts	The CPS shall provide international post code and zip code verification for fraud protection.
Functional	CPS-FN2622-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to manage account information.

Functional	CPS-FN2623-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to manage payment options.
Functional	CPS-FN2646-V01	Personal Information Device	Application Payment Device	The PID shall accept payment device updates from the CPS Back Office.
Functional	CPS-FN2629-V01	CPS Web Portal	Account Management	The Web Portal shall enable Travelers to manage accounts directly, by correctly entering login authentication.
Functional	CPS-FN2631-V01	CPS Back Office	Traveler Accounts	The CPS shall permit the entry of US and international profile information to accommodate tourists and visitors to Central Ohio.
Functional	CPS-FN2527-V01	CPS Web Portal	Account Management	Contact information shall be recorded and treated independently of any personal information related to payments.
Functional	CPS-FN2533-V01	CPS Back Office	Payment Processing	When validating a stored cash value transaction from a Traveler account, the system shall not permit the stored cash value balance to enter overdraft (i.e., fall below $0.00).
Functional	CPS-FN2539-V01	CPS Web Portal	Account Management	Travelers shall have the ability to close their accounts.
Security	CPS-SR2587-V01	CPS Back Office	Traveler Accounts	Traveler account passwords shall have a minimum of 12 characters with a mix of upper- and lower-case, alphanumeric and special characters.

Security	CPS-SR2585-V01	CPS Back Office	Traveler Accounts	Travelers shall have the ability to reset a lost password.
Functional	CPS-FN2591-V01	CPS Back Office	Traveler Accounts	Integration with the MMTPA shall provide a seamless User experience for the Traveler by not requiring a separate logon to the MMTPA.
Functional	CPS-FN2592-V01	CPS Back Office	Traveler Accounts	Integration with the EPM shall provide a seamless User experience for the Traveler by not requiring a separate logon to the EPM application.
Security	CPS-SR2589-V01	CPS Back Office	Traveler Accounts	Travelers who have not accessed an account in 90 days or more shall be required to reset password upon next login.
Functional	CPS-FN2593-V01	CPS Back Office	Payment Processing	The CPS shall provide real-time funding authorization for payment transactions via cellular connectivity.
Data	CPS-DR2773-V01	CPS Back Office	PCI Compliance	The CPS Back Office shall manage Traveler account data.
Interface	CPS-IF3167-V01	OS	Payment Broker	The CPS shall provide an interface to send transaction information (request ID, amount, request type, Traveler, Provider) from the OS to CPS to be used in payment processing.

Interface	CPS-IF3168-V01	CPS Back Office	Payment Processing	The CPS shall provide an interface to send payment authorization and funds availability from the CPS to OS.
Interface	CPS-IF3170-V01	PID	Traveler Account Management	The CPS shall provide an interface to send security credentials, Traveler account information, additions, deletions, modifications, and payment methods from the Traveler's personal information device to CPS.
Interface	CPS-IF3171-V01	CPS Web Portal	Traveler Account Management	The CPS shall provide an interface to send security credentials, Traveler account information, additions, deletions, modifications, and payment methods from the Traveler's Web Portal to CPS.
Interface	CPS-IF3172-V01	CPS Web Portal	Provider Account Management	The CPS shall provide an interface to send security credentials, service Provider account information, modifications to service rates and options, report request parameters, and communications requests from the Service Provider's Web Portal to CPS.
Interface	CPS-IF3173-V01	HUBSs	Traveler Account Management	The CPS shall provide an interface to allow kiosks at HUBSs to send Traveler account information and verification of changes to the CPS.

Interface	CPS-IF3176-V01	CPS Back Office	Provider Accounts	The CPS shall provide an interface to send report information and verification of Service Provider account changes to the Service Provider's CPS Web Portal.
Interface	CPS-IF3177-V01	CPS Back Office	Traveler Accounts	The CPS shall send Traveler account information and verification of account changes to kiosks at the HUBSs.
Interface	CPS-IF3181-V01	COTA CFMS	COTA CFMS	The CPS shall provide an interface to allow COTA to send User account information to the shared account ledger in the OS.
Interface	CPS-IF3182-V01	Mobility Provider Central Management System	Provider Central Management System	The CPS shall provide an interface to allow Mobility Provider Central Systems to send User account information to the shared account ledger in the OS.
Interface	CPS-IF3183-V01	EPMCS	Parking Central Management System	The CPS shall provide an interface to allow EPMCS to send User account information to the shared account ledger in the OS.
Interface	CPS-IF3184-V01	OS	Shared Account Ledger	The CPS shall provide an interface to send shared account updates from the OS to COTA.

Interface	CPS-IF3185-V01	OS	Shared Account Ledger	The CPS shall provide an interface to send shared account updates from the OS to Mobility Provider Central Systems.
Interface	CPS-IF3186-V01	OS	Shared Account Ledger	The CPS shall provide an interface to send shared account updates from the OS to EPMCS.
Interface	CPS-IF3189-V01	OS	Payment Broker	The CPS shall provide an internal interface to add Users from external systems to the shared account ledger in the OS.
Interface	CPS-IF3190-V01	CPS Back Office	Payment Processing	The CPS shall provide an internal interface to credit the Service Provider's account in exchange for services.
Interface	CPS-IF3191-V01	CPS Back Office	Payment Processing	The CPS shall provide an internal interface to deduct funds from the Traveler's account in exchange for services.
Functional	CPS-FN3132-V01	OS	Payment Broker	The payment broker shall debit Traveler shared accounts when a payment is executed.
Functional	CPS-FN3133-V01	OS	Payment Broker	The payment broker shall credit Service Provider accounts when a payment is executed.

Functional	CPS-FN3134-V01	OS	Shared Account Ledger	The CPS shall provide a shared account ledger in the OS containing anonymous accounts and balances that are linked to User accounts belonging to Service Providers or to Traveler accounts in the CPS. The API with the Service Providers will provide two-way updates of these accounts within 10 seconds of any transactions.
Functional	CPS-FN3135-V01	OS	Payment Broker	The payment broker shall interact with the shared account ledger to validate available funds to complete a payment transaction.
Functional	CPS-FN3136-V01	OS	Payment Broker	The payment broker shall accept payment requests from the MMTPA and EPM application.
Functional	CPS-FN3137-V01	OS	Payment Broker	The payment broker shall accept payment requests from the IVR System.
Functional	CPS-FN3138-V01	OS	Payment Broker	The payment broker shall accept payment requests from the MMTPA on the HUBS.

Functional	CPS-FN3140-V01	CPS Back Office	Traveler Accounts	The CPS shall allow the dollar amount threshold used to trigger automatic withdrawals to be adjusted by the Traveler in increments of $10 up to a maximum amount of $100.
Functional	CPS-FN3146-V01	CPS Back Office	Traveler Accounts	The CPS shall include the capability to load cash at COTA TVMs to fund a Traveler account.
Functional	CPS-FN3147-V01	CPS Back Office	Traveler Accounts	The CPS may include the capability for POS reloads of Traveler accounts at third-party retailers.
Performance	CPS-PR2718-V01	CPS Back Office	CPS Payment Processing	The CPS Offeror shall be able to measure data input/output latency on their servers by time-stamping request and response times and provide these statistics accurately for assessing performance against requirement CPS-PR2717-V01.
Performance	CPS-PR3152-V01	OS	Shared Accounts Ledger	The system shall be able to update shared accounts with a response time of roughly 10 seconds or less.
Performance	CPS-PR3153-V01	OS	Payment Broker	The payment broker shall be able to validate funds with a response time of roughly 1 second or less.

USER NEED:	MMTPA/CPS-UN023-v02	USER: Traveler
Title:	**Payment Media**	
Description:	The MMTPA/CPS system needs to accept numerous forms of payment. Payment media include cash, all major US credit/debit cards (includes all cards issued from the following US financial institutions: American Express, Discover, MasterCard, and Visa), major international cards, and debit cards (reloadable cards that are not tied to a personal checking account). Travelers who are unbanked will be able to purchase a COTA smart card with cash or use a reloadable prepaid debit card not tied to a financial institution or checking account to fund a CPS account. It is anticipated that smart cards will be available for purchase at retailers throughout Columbus.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2504-V01	CPS Back Office	Payment Processing	The CPS shall accept use of electronic wallets (Apple Pay, Android Pay, and Google Pay).
Functional	CPS-FN2503-V01	CPS Back Office	Payment Processing	The CPS shall accept cash, all major US and international credit cards and debit cards (reloadable cards that are not tied to a personal checking account).
Functional	CPS-FN2546-V01	CPS Back Office	Traveler Accounts	Payment media may include PayPal electronic payment services.
Functional	CPS-FN2544-V01	CPS Back Office	Traveler Accounts	Payment media shall include all major U.S. and international credit and debit cards.
Functional	CPS-FN2542-V01	CPS Back Office	Traveler Accounts	The CPS shall be capable of allowing partner organizations (e.g. Regional Systems) to supply their own payment media.

Functional	CPS-FN2547-V01	CPS Back Office	Traveler Accounts	Payment media shall include reloadable pre-paid debit cards (i.e., not tied to a personal checking account) to facilitate unbanked Travelers.
Functional	CPS-FN2545-V01	CPS Back Office	Traveler Accounts	The CPS shall provide international post code and zip code verification for fraud protection.
Interface	CPS-IF3170-V01	Personal Information Device	Traveler Account Management	The CPS shall provide an interface to send security credentials, Traveler account information, additions, deletions, modifications, and payment methods from the Traveler's personal information device to CPS.
Interface	CPS-IF3171-V01	CPS Web Portal	Traveler Account Management	The CPS shall provide an interface to send security credentials, Traveler account information, additions, deletions, modifications, and payment methods from the Traveler's Web Portal to CPS.
Interface	CPS-IF3173-V01	HUBSs	Traveler Account Management	The CPS shall provide an interface to allow kiosks at HUBS to send Traveler account information and verification of changes to the CPS.

USER NEED:	MMTPA/CPS-UN024-v02			USER: Traveler
Title:	**Subsidization**			
Description:	The MMTPA/CPS system needs to provide the ability for third parties (such as an employer, a college or university, or guardian) to subsidize transportation. For example, a Traveler's account in the CPS may be linked to an employer's account if that employer wishes to subsidize the employee's transportation.			
Priority:	Desirable			

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2495-V01	CPS Back Office	Administration	The CPS shall allow for management of special programs such as Traveler discounts, benefits, and loyalty programs.
Functional	CPS-FN2549-V01	CPS Back Office	Traveler Accounts	The CPS shall provide a mechanism for external agencies (e.g., employers, colleges or universities, or guardians) to subsidize the cost of parking for a Traveler through an authorized validation code or through reoccurring backend Provider.
Functional	CPS-FN2551-V01	CPS Web Portal	Account Management	The Web Portal shall allow Traveler accounts to be tied to an employee benefits program using pre-tax dollars to pay for parking.
Functional	CPS-FN2550-V01	CPS Web Portal	Account Management	The Web Portal shall allow Traveler accounts to be tied to an employee benefits program using pre-tax dollars to pay for transportation services.
Functional	CPS-FN2548-V01	CPS Back Office	Traveler Accounts	

USER NEED:	MMTPA/CPS-UN025-v02	USER: Traveler
Title:	**Pay Once**	
Description:	The MMTPA/CPS system needs to allow Travelers to “click once” to pay for services. For example, an MMTPA User who creates a trip involving multiple trip segments and modes of transportation, and who has a registered CPS account, will only need to pay once for all trip segments. Travelers who do not wish to register a CPS account will be able to make one-time payments. For example, when attempting to pay without a CPS account, Users will have the option to “continue as guest.”	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2473-V01	CPS Back Office	Traveler Accounts	Traveler accounts shall maintain a balance (stored cash value) so that transactions can be implemented using "click once" functionality (CPS-FN2472-V01) without having to re-enter payment information.
Functional	CPS-FN2472-V01	CPS Back Office	Payment Processing	The CPS shall be capable of processing payment requests for multiple trip segments and multiple service Providers at one time through a "click once" payment functionality in the MMTPA.
Functional	CPS-FN2487-V01	CPS Back Office	Payment Processing	The CPS shall process requests for payment that are received from the payment broker.

USER NEED:	MMTPA/CPS-UN026-v02	USER: Traveler
Title:	**Existing Fare Products**	
Description:	The MMTPA/CPS system needs to allow Travelers with existing fare products, such as COTA's C-pass program, to utilize the existing fare product when paying for associated trips. For example, existing C-pass or OSU riders who have unlimited passes to use COTA services and would need to have those passes recognized by the System when using the MMTPA/CPS to pay for travel. It is envisioned that existing fare products for any Mobility Provider will be accounted for in the Traveler's CPS account.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2490-V01	CPS Back Office	Payment Processing	The CPS shall allow virtual transfer credits to be used for the purposes of permitting multi-leg transit trips subject to current restrictions in accordance with COTA policies.
Functional	CPS-FN2488-V01	CPS Back Office	Payment Processing	The CPS shall allow Travelers to utilize existing COTA period pass products, which permit journeys within the COTA network, subject to time restrictions.
Functional	CPS-FN2491-V01	CPS Back Office	Payment Processing	When applying virtual transfer credits toward a multi-leg transit trip, the remainder of the cost of the trip (if additional charges are required) shall be taken from the Traveler account (stored cash value).
Functional	CPS-FN2536-V01	CPS Back Office	Traveler Accounts	The CPS shall associate any COTA issued fare media (including LUM cards) with a registered Traveler account.

Functional	CPS-FN2538-V01	CPS Back Office	Traveler Accounts	The CPS shall permit payment media to be disassociated from an account without closing the account.
Functional	CPS-FN2559-V01	CPS Back Office	Payment Processing	The CPS shall provide the ability for Service Providers to set their fare product structures in the Service Provider Web Portal.
Functional	CPS-FN2537-V01	CPS Back Office	Traveler Accounts	The CPS shall permit multiple fare media to be associated with a single Traveler account.
Functional	CPS-FN2561-V01	CPS Back Office	Payment Processing	The CPS shall provide a mechanism for Travelers who are eligible for COTA's fare subsidy programs to receive those benefits.
Functional	CPS-FN2560-V01	CPS Back Office	Payment Processing	The CPS shall be capable of integration with COTA's smart card.
Functional	CPS-FN2534-V01	CPS Back Office	Traveler Accounts	The CPS shall permit more than one COTA smart card to be associated with a single Traveler account to allow funds to be transferred between the accounts.

USER NEED:	MMTPA/CPS-UN027-v02	USER: Traveler
Title:	**Notification of Payment and Account Status**	
Description:	The MMTPA/CPS system needs to alert Travelers of payment and account status. Travelers need the CPS to alert them in case of insufficient funds so they may address the situation.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2477-V01	CPS Web Portal	Account Management	Travelers shall have the ability to configure whether to receive text and email alerts when their CPS account is low or has been replenished.
Functional	CPS-FN2476-V01	CPS Back Office	Notifications and Alerts	The CPS shall trigger a push notification to the Traveler's mobile device when account balance falls below set dollar amount threshold.
Functional	CPS-FN2632-V01	CPS Web Portal	Account Management	The Web Portal shall provide the capability to configure notifications and alerts.
Interface	CPS-IF3163-V01	OS	Payment Broker	The CPS shall provide an interface to send payment authorization and funds availability from the OS to the Traveler's personal information device.
Interface	CPS-IF3164-V01	OS	Payment Broker	The CPS shall provide an interface to send payment authorization and funds availability from the OS to the Traveler's Web Portal.

Interface	CPS-IF3165-V01	OS	Payment Broker	The CPS shall provide an interface to send payment authorization and funds availability from the OS to a third-party IVR system.
Interface	CPS-IF3166-V01	OS	Payment Broker	The CPS shall provide an interface to send payment authorization and funds availability from the OS to kiosks at HUBSs.
Interface	CPS-IF3174-V01	CPS Back Office	Traveler Accounts	The CPS shall send Traveler account information and verification of account changes to the Traveler's personal information device.
Interface	CPS-IF3175-V01	CPS Back Office	Traveler Accounts	The CPS shall provide an interface to send Traveler account information and verification of account changes to the Traveler's CPS Web Portal.

USER NEED:	**MMTPA/CPS-UN028-v02**			**USER: Traveler**
Title:	**Traveler Web Portal**			
Description:	The MMTPA/CPS system needs to provide Travelers with a Web Portal. Travelers need the ability to manage account settings, payment products, and contact info, as well as the ability to view and export CPS transactions. Travelers should be able to perform the same trip planning functions as in the MMTPA.			
Priority:	Essential			
Related Requirements, Constraints, and System Interfaces				
Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Functional	CPS-FN2494-V01	CPS Web Portal	Account Management	Service Providers shall be required to provide a Username and password to log into the Web Portal.

Functional	CPS-FN2493-V01	CPS Web Portal	Account Management	Travelers shall be required to register or provide a Username and password to log into the Web Portal.
Functional	CPS-FN2624-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to manage account information.
Functional	CPS-FN2634-V01	CPS Web Portal	Account Management	Information relevant to an existing payment(s) (receipt/proof of payment) shall be accessible to the Traveler within the previous three months.
Functional	CPS-FN2627-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to manage payment options.
Functional	CPS-FN2628-V01	CPS Web Portal	Account Management	The Web Portal shall enable Service Providers to manage accounts directly, by correctly entering login authentication.
Functional	CPS-FN2625-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to purchase fare products.
Functional	CPS-FN2626-V01	CPS Web Portal	Account Management	The Web Portal shall provide Travelers with the ability to replenish their account.
Functional	CPS-FN2633-V01	CPS Web Portal	Account Management	The Web Portal shall provide the capability to configure notifications and alerts.

Performance	CPS-PR2718-V01	CPS Back Office	CPS Payment Processing	The CPS Offeror shall be able to measure data input/output latency on their servers by time-stamping request and response times and provide these statistics accurately for assessing performance against requirement CPS-PR2717-V01.
Data	CPS-DR2766-V01	CPS Web Portal	Anonymous Trip and Payment Data	The WEB shall collect payment data from CPS Landing Pages.
Data	CPS-DR2767-V01	CPS Web Portal	CPS Landing Pages	The WEB shall not store the collected payment data.
Functional	CPS-FN3144-V01	CPS Web Portal	Account Management	The CPS shall provide a secure Web Portal to allow Service Providers to manage accounts in the CPS Back Office.
Functional	CPS-FN3145-V01	CPS Web Portal	Account Management	The CPS shall provide a Web Portal to allow Travelers to create and manage accounts in the CPS Back Office.

USER NEED:	MMTPA/CPS-UN029-v02	USER: Traveler
Title:	**Storage of Sensitive Data**	
Description	The MMTPA/CPS system needs to provide Travelers with the ability to store sensitive credit card data for processing payment requests. Travelers need the CPS to comply with the latest PCI data security standards, including all audit and compliance certification activities to ensure personal and financial safety.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2568-V01	CPS Back Office	Administration	The transaction log shall maintain information for a minimum of one year.
Security	CPS-SR2558-V01	CPS Back Office	PCI Compliance	The CPS shall be fully compliant with PCI standards, including ensuring that all customer credit card payments completed using the system shall not allow any access to or storage of credit card numbers on any City or COTA-operated computers.
Functional	CPS-FN2566-V01	CPS Back Office	Administration	The CPS Back Office shall retain a record of all account information and transaction history, including data associated with closed accounts, for a minimum of three years.
Functional	CPS-FN2567-V01	CPS Back Office	Administration	The CPS Back Office shall maintain a transaction log that records all Users that access reports, the reports accessed, edits and changes to the database and the system logon and logoff times.

Data	CPS-DR2772-V01	CPS Back Office	PCI Compliance	The CPS Back Office shall store payment data in a PCI compliant environment.
Security	CPS-SR2782-V01	CPS Back Office	PCI Compliance	The CPS shall encrypt cardholder data that is transmitted across open, public networks.
Security	CPS-SR2785-V01	CPS Back Office	PCI Compliance	The CPS shall create and sustain secure systems and applications.
Security	CPS-SR2786-V01	CPS Back Office	PCI Compliance	The CPS shall keep cardholder access limited by need-to-know.
Security	CPS-SR2783-V01	CPS Back Office	PCI Compliance	The CPS Offeror shall implement and update anti-virus software on a weekly basis.
Security	CPS-SR2784-V01	CPS Back Office	PCI Compliance	Security patches and updates shall be installed within 24 hours after being made available for installation by the Offeror.
Security	CPS-SR2787-V01	CPS Back Office	PCI Compliance	The CPS shall require unique identifiers for Users with digital access to cardholder data.
Security	CPS-SR2780-V01	CPS Back Office	PCI Compliance	The CPS shall create custom passwords and other unique security measures rather than using the default setting from the Offeror-supplied systems.
Security	CPS-SR2781-V01	CPS Back Office	PCI Compliance	The CPS shall safeguard stored cardholder data.

Security	CPS-SR2778-V01	CPS Back Office	PCI Compliance	The CPS shall comply with PCI Data Security Standards (DSS) Version 3.2.
Security	CPS-SR2779-V01	CPS Back Office	PCI Compliance	The CPS shall safeguard cardholder data by implementing and maintaining a firewall.
Security	CPS-SR2789-V01	CPS Back Office	PCI Compliance	The CPS shall require network resources and cardholder data access to be logged and reported.
Security	CPS-SR2790-V01	CPS Back Office	PCI Compliance	The CPS shall run daily security system and process tests.
Security	CPS-SR2788-V01	CPS Back Office	PCI Compliance	The CPS shall restrict physical access to cardholder data.
Security	CPS-SR2791-V01	CPS Back Office	PCI Compliance	The CPS shall address information security by creating a policy.

USER NEED:	**MMTPA/CPS-UN031-v02**	**USER: Traveler**
Title:	**Security and Encryption**	
Description:	The MMTPA/CPS system needs to encrypt communications. This applies to the transport layer.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Security	CPS-SR2654-V01	CPS Back Office	CPS Payment Processing	The CPS shall be architected and fortified to defend against DoS attacks.
Security	CPS-SR2657-V01	CPS Back Office	CPS Payment Processing	The CPS shall include verification features to confirm that there have been no losses of data at any point in the data transfers.

Security	CPS-SR2658-V01	CPS Back Office	CPS Payment Processing	The CPS shall include verification features to confirm that there have been no unauthorized changes to, or destruction of, data.
Security	CPS-SR2655-V01	CPS Back Office	CPS Payment Processing	All data transactions shall include non-repudiation features to verify message content, and resolve claims that data was not correctly originated or received by a certain User.
Security	CPS-SR2656-V01	CPS Back Office	CPS Payment Processing	The CPS security shall provide features to maintain data integrity, including error checking, error monitoring, error handling and encryption.
Security	CPS-SR2648-V01	CPS Back Office	Administration	All systems, subsystems and devices shall only allow access to authorized User classes.
Security	CPS-SR2649-V01	CPS Back Office	Administration	All security breach detections shall be confidential, and accessible only to Users of the appropriate class.
Security	CPS-SR2659-V01	CPS Back Office	CPS Payment Processing	The CPS shall include features to automatically detect, correct and prevent the propagation of invalid or erroneous data throughout the system.
Security	CPS-SR2652-V01	CPS Back Office	CPS Payment Processing	All APIs should use security keys.

Security	CPS-SR2653-V01	CPS Back Office	CPS Payment Processing	All accounts shall be monitored for traffic volume to detect denial of service (DoS) attacks.
Security	CPS-SR2650-V01	CPS Back Office	CPS Payment Processing	Security provisions for communications networks shall be described.
Security	CPS-SR2651-V01	CPS Back Office	CPS Payment Processing	For all data transactions, the system security shall include authentication features to verify that all claimed source, recipient or User identities are correct and valid.
Security	CPS-SR2719-V01	CPS Back Office	CPS Payment Processing	The Offeror shall perform security testing to verify the system security at least once per year.
Security	CPS-SR2722-V01	CPS Back Office	CPS Payment Processing	The Offeror shall perform external threat assessment for the Web Portal and landing pages.
Security	CPS-SR2723-V01	CPS Back Office	CPS Payment Processing	Communication between external systems and the CPS shall operate in an encrypted, end-to-end connection.
Security	CPS-SR2720-V01	CPS Back Office	CPS Payment Processing	Security testing shall include penetration and vulnerability testing.
Security	CPS-SR2721-V01	CPS Back Office	CPS Payment Processing	The CPS shall provide secure communications, including certificates management.

USER NEED:	MMTPA/CPS-UN032-v02	USER: Traveler
Title:	**Support for Multiple Languages**	
Description:	The MMTPA/CPS system needs to provide Travelers with the ability to select English or Spanish (at a minimum) as their preferred language at any point before or during any transaction and present all dynamic text and audible words (if applicable) to the Traveler in their preferred language. Training and educational material should also support the Traveler's preferred language.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Interface	CPS-IF2725-V01	CPS Back Office	CPS Payment Processing	All User interfaces shall be available in English and Spanish language.

USER NEED:	MMTPA/CPS-UN033-v02	USER: City/COTA
Title:	**Access to Trip and Payment Data**	
Description:	The MMTPA/CPS system needs to provide the City and COTA with access to data generated by the MMTPA/CPS system. Trip and payment data consist of the following and pertain only to an executed trip in which payment is made: trip request (time, origin, destination, route), trip start time, mode, transfer (time, location, disembarked, embarked), trip end time, payment initiated, payment amount, payment complete. The trip should reference all trip activity for each mode for multi-leg trips. Trip and payment data will not contain PII that could potentially identify a specific individual.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2583-V01	CPS Back Office	Administration	Account activity data shall include status of all auto-reload subscriptions associated with each Traveler account.
Functional	CPS-FN2579-V01	CPS Back Office	Administration	The CPS shall allow authorized individuals to view and export account activity data (CSV and PDF) pertaining to CPS usage associated with Traveler accounts.

Functional	CPS-FN2581-V01	CPS Back Office	Administration	Account activity data shall include history of all payment transactions pending and closed.
Functional	CPS-FN2641-V01	OS	Payment Broker	Data posted to the OS from the Payment Broker shall have PII obfuscated so that it may be available to third-party Users.
Data	CPS-DR2647-V01	OS	Anonymous Trip and Payment Data	The CPS shall provide anonymous payment data to the OS for storage in accordance with OS practices.
Functional	CPS-FN2582-V01	CPS Back Office	Administration	Account activity data shall include balances for both Travelers and Service Providers.
Functional	CPS-FN2580-V01	CPS Back Office	Administration	Account activity data shall include account creation and profile information.
Data	CPS-DR2715-V01	OS	Payment Broker	Payment data shall be linked to trip data (origin, destination, start time, end time, mode, transfer, transfer time, transfer location, disembarked location, embarked location) using a common identifier.
Data	CPS-DR2775-V01	OS	Anonymous Trip and Payment Data	The storage time of anonymous payment data in the OS shall be configurable up to a maximum of 10 years by the City/COTA.

Interface	CPS-IF3192-V01	CPS Back Office	Payment Processing	The CPS shall provide an internal interface to update payment history for both Travers and Service Providers.

USER NEED:	**MMTPA/CPS-UN034-v02**			**USER: City/COTA**
Title:	**Operations and Maintenance**			
Description:	The MMTPA/CPS system needs to be maintained and operated external to the City.			
Priority:	Essential			
Related Requirements, Constraints, and System Interfaces				
Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Availability and Recovery	CPS-AR2710-V01	CPS Back Office	CPS Payment Processing	The system shall provide 99.99% operational availability over a given year.
Availability and Recovery	CPS-AR2711-V01	CPS Back Office	CPS Payment Processing	The functioning of system features at performance levels as defined in CPS-PR248-v01 shall be used to measure system availability.
Availability and Recovery	CPS-AR2714-V01	CPS Back Office	CPS Payment Processing	Reduced availability associated with planned maintenance but falling outside the start and/or end times and dates agreed between the City and the Offeror, shall be considered as impacting system availability.
Availability and Recovery	CPS-AR2712-V01	CPS Back Office	CPS Payment Processing	The functioning of system features in compliance with planned maintenance requirements as defined in CPS-MT343-v01 shall be used to measure system availability.

Availability and Recovery	CPS-AR2713-V01	CPS Back Office	CPS Payment Processing	The City shall retain the ability to determine and modify which system features are to be included or excluded from the system scope to which availability requirements are applied.
Functional	CPS-FN2506-V01	CPS Back Office	Administration	Administrative accounts shall include fine-grained permission levels (e.g., View Only, Limited Access, and Full Control).
Functional	CPS-FN2528-V01	CPS Back Office	Administration	The CPS shall permit administrative Users with limited access to transfer the balance (stored cash value) of one registered CPS account to another registered CPS account.
Functional	CPS-FN2529-V01	CPS Back Office	Administration	The CPS shall permit administrative Users to close any account type (e.g. due to prolonged inactivity or abuse of policies).
Functional	CPS-FN2505-V01	CPS Back Office	Administration	The CPS shall provide administrative accounts secured by Username and password for authorized individuals at the City and COTA.
Functional	CPS-FN2569-V01	CPS Back Office	Administration	The transaction log shall not be editable to even the highest class of administrative User (full control).

Disposal	CPS-DP2682-V01	CPS Back Office	CPS Payment Processing	The CPS shall remain operational after the completion of the deployment period unless otherwise directed by the City.
Information Management	CPS-IM2661-V01	CPS Back Office	Shared Account Processing	The CPS Back Office shall be hosted external to the City of Columbus.
Life Cycle Sustainment	CPS-LC2662-V01	CPS Back Office	Reporting	The Offeror shall provide system performance reports on a monthly and on an ad-hoc basis.
Life Cycle Sustainment	CPS-LC2665-V01	CPS Back Office	Reporting	Performance reports shall include average and percentile response times.
Life Cycle Sustainment	CPS-LC2666-V01	CPS Back Office	Reporting	Performance reports shall include security breaches.
Life Cycle Sustainment	CPS-LC2663-V01	CPS Back Office	Reporting	Performance reports shall include system availability.
Life Cycle Sustainment	CPS-LC2664-V01	CPS Back Office	Reporting	Performance reports shall include system usage, including transactions, payment broker authorizations (failed and approved), PIDs hits and PIDs unique accesses.
Life Cycle Sustainment	CPS-LC2667-V01	CPS Back Office	Reporting	Performance reports shall include attempted security breaches.

Life Cycle Sustainment	CPS-LC2671-V01	CPS Back Office	Reporting	The QA/QC Plan shall identify the risk management process the Offeror shall follow, which shall define the risks and critical elements of the system development process, along with the contingency plans to address these.
Life Cycle Sustainment	CPS-LC2674-V01	CPS Back Office	Reporting	The QA/QC Plan shall identify the change management practices the Offeror shall follow while developing the system, to ensure that any system development changes and associated reasons are documented.
Life Cycle Sustainment	CPS-LC2675-V01	CPS Back Office	Reporting	The QA/QC Plan shall identify the security management process the Offeror shall follow to ensure that the system development follows secure processes and technology and the system achieves the desired security level.
Life Cycle Sustainment	CPS-LC2672-V01	CPS Back Office	Reporting	The QA/QC Plan shall identify the system development, testing, and QA/QC standards the Offeror shall follow while developing the system.

Life Cycle Sustainment	CPS-LC2673-V01	CPS Back Office	Reporting	The QA/QC Plan shall identify the error/defect collection and analysis process to ensure that any introduced errors shall be tracked, identified, and eliminated.
Life Cycle Sustainment	CPS-LC2669-V01	CPS Back Office	Reporting	The Offeror shall provide a Quality Assurance/Quality Control (QA/QC) Plan for approval before award of the contract.
Life Cycle Sustainment	CPS-LC2670-V01	CPS Back Office	Reporting	The QA/QC Plan shall define principles and processes the Offeror shall follow while developing the system.
Life Cycle Sustainment	CPS-LC2668-V01	CPS Back Office	Reporting	Performance reports shall include critical issues observed during the month along with information regarding issue causes and resolutions.
Information Management	CPS-IM2737-V01	CPS Back Office	CPS Payment Processing	The Offeror shall provide a Data Backup and Recovery Plan.
Information Management	CPS-IM2738-V01	CPS Back Office	CPS Payment Processing	The System Security Plan shall include documentation for an Annual PCI Compliance audit.
Information Management	CPS-IM2739-V01	CPS Back Office	CPS Payment Processing	The Offeror shall demonstrate traceability that all User needs and system requirements have been satisfied.

Information Management	CPS-IM2735-V01	CPS Back Office	CPS Payment Processing	The Offeror shall provide a PCI Compliance Plan demonstrating adherence to PCI DSS 3.2.
Information Management	CPS-IM2736-V01	CPS Back Office	CPS Payment Processing	The Offeror shall provide a System Security Plan, describing security features including fail-over procedure, firewall, data encryption/privacy, management of all encryption keys; and communication.
Information Management	CPS-IM2732-V01	CPS Back Office	CPS Payment Processing	The Offeror shall provide overall system schematic and architecture.
Acceptance Testing	CPS-AT2921-V01	CPS Back Office	CPS Payment Processing	The Offeror shall undertake testing to demonstrate that all contract requirements have been provided.
Acceptance Testing	CPS-AT2922-V01	CPS Back Office	CPS Payment Processing	All testing shall be conducted according to the approved Acceptance Test Procedures (ATP).
Acceptance Testing	CPS-AT2923-V01	CPS Back Office	CPS Payment Processing	Testing shall be completed for each release to verify that the requirements have been addressed.
Acceptance Testing	CPS-AT2924-V01	CPS Back Office	CPS Payment Processing	At a minimum, testing shall include (as applicable): verification of necessary functions, communications and operational interfaces.

Acceptance Testing	CPS-AT2925-V01	CPS Back Office	CPS Payment Processing	Testing shall be completed on the system to confirm that the system meets the required functionality.
Acceptance Testing	CPS-AT2926-V01	CPS Back Office	CPS Payment Processing	Testing may be witnessed by City/COTA representatives (City/COTA staff and/or designated support consultants).
Acceptance Testing	CPS-AT2927-V01	CPS Back Office	CPS Payment Processing	The Offeror shall submit an ATP document for approval prior to undertaking testing.
Acceptance Testing	CPS-AT2928-V01	CPS Back Office	CPS Payment Processing	The ATP shall address how each testable requirement will be demonstrated, including the method for performing the test.
Acceptance Testing	CPS-AT2929-V01	CPS Back Office	CPS Payment Processing	The ATP shall address the results that will constitute success for each test.
Acceptance Testing	CPS-AT2930-V01	CPS Back Office	CPS Payment Processing	The ATP shall address the responsibilities of both the Offeror and City/COTA representatives during each test.
Acceptance Testing	CPS-AT2931-V01	CPS Back Office	CPS Payment Processing	The ATP shall include the test stage(s) at which each requirement will be demonstrated.
Acceptance Testing	CPS-AT2932-V01	CPS Back Office	CPS Payment Processing	A cross-reference shall link each requirement with the ATP test(s) being conducted to demonstrate the requirement.

Acceptance Testing	CPS-AT2933-V01	CPS Back Office	CPS Payment Processing	Dry-run tests shall be conducted by the Offeror prior to the formal start of any testing involving the City/COTA representatives to ensure that successful completion of the formal witnessed tests can be reasonably anticipated.
Acceptance Testing	CPS-AT2934-V01	CPS Back Office	CPS Payment Processing	The Offeror shall notify the City/COTA and receive authorization from the City to proceed with testing.
Acceptance Testing	CPS-AT2935-V01	CPS Back Office	CPS Payment Processing	The Offeror shall allow the City/COTA to witness any tests at each test stage.
Acceptance Testing	CPS-AT2936-V01	CPS Back Office	CPS Payment Processing	Test Results Documentation (TRD) shall be provided upon completion of testing.
Acceptance Testing	CPS-AT2937-V01	CPS Back Office	CPS Payment Processing	Any proposed time for testing shall be approved by the City/COTA.
Acceptance Testing	CPS-AT2938-V01	CPS Back Office	CPS Payment Processing	The TRD shall document version number of each software system component being tested.
Acceptance Testing	CPS-AT2939-V01	CPS Back Office	CPS Payment Processing	The TRD shall document details of the dataset used.
Acceptance Testing	CPS-AT2940-V01	CPS Back Office	CPS Payment Processing	The TRD shall document the result of each ATP procedure.

Acceptance Testing	CPS-AT2941-V01	CPS Back Office	CPS Payment Processing	The TRD shall document which contract requirements have been demonstrated.
Acceptance Testing	CPS-AT2942-V01	CPS Back Office	CPS Payment Processing	The TRD shall document list of failures and open issues identified during testing along with action plan to resolve them.
Acceptance Testing	CPS-AT2943-V01	CPS Back Office	CPS Payment Processing	The TRD shall be approved by the City/COTA before a test stage can be considered complete.
Acceptance Testing	CPS-AT2944-V01	CPS Back Office	CPS Payment Processing	All deficiencies shall be rectified and retested as part of completing each testing stage.
Acceptance Testing	CPS-AT2945-V01	CPS Back Office	CPS Payment Processing	SA shall not be granted until all test stages for that deployment phase are complete and all requirements formally demonstrated through Acceptance Testing.
Acceptance Testing	CPS-AT2946-V01	CPS Back Office	CPS Payment Processing	A requirement classified as having been demonstrated during a certain Acceptance Testing stage should be subsequently redefined as having been not demonstrated if compliance issues emerge prior to System Acceptance (SA).

Acceptance Testing	CPS-AT2947-V01	CPS Back Office	CPS Payment Processing	Any residual deficiencies shall be rectified, together with any outstanding training and documentation having been provided, before City/COTA will grant acceptance.
Maintainability	CPS-MT2948-V01	CPS Back Office	CPS Payment Processing	The Offeror shall be responsible for maintenance of the CPS Back Office and related functions.
Maintainability	CPS-MT2949-V01	CPS Back Office	CPS Payment Processing	The Offeror shall be responsible for maintenance of the CPS Landing Pages providing integration with MMTPA and EPM.
Maintainability	CPS-MT2950-V01	CPS Back Office	CPS Payment Processing	The Offeror shall be responsible for maintenance of the interfaces between the CPS and external systems identified in the CPS System Requirements document.

USER NEED:	**MMTPA/CPS-UN035-v02**	**USER: City/COTA**
Title:	**Future Growth and Maintainability**	
Description:	The MMTPA/CPS system needs to be architected to allow for incorporation of additional Mobility Providers in the future with minimal impact to the environment itself, such as need for redesign or rewrite of the application code, and minimum impact on the MMTPA/CPS, such as need to reinstall the application.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Functional	CPS-FN2496-V01	CPS Back Office	CPS Payment Processing	The CPS should provide the ability to bundle services of multiple Providers (monthly subscription plans).

Functional	CPS-FN2499-V01	CPS Back Office	Payment Processing	The CPS shall be capable of handling payments for non-emergency medical transportation (NEMT) trips funded through Medicaid accounts. This capability is considered “future state” and shall not be required in the final release of the CPS for the grant.
Policy and Regulation	CPS-RG2678-V01	CPS Back Office	Software Development Kit	APIs should use a semantic model that is close to the thing it describes (e.g., classes like "payment" and "Traveler").
Policy and Regulation	CPS-RG2679-V01	CPS Back Office	CPS Payment Processing	The CPS should follow open architecture with well-defined and documented interfaces that are public as opposed to proprietary.
Policy and Regulation	CPS-RG2676-V01	CPS Back Office	Software Development Kit	APIs should follow best practices to achieve the business needs and purposes for which they are designed.
Policy and Regulation	CPS-RG2677-V01	CPS Back Office	Software Development Kit	APIs should be well documented and follow an established coding standard.
Policy and Regulation	CPS-RG3154-V01	OS	Payment Broker	The Offeror shall package applications into a Docker Image to ensure version control, portability, isolation and security.

Policy and Regulation	CPS-RG3158-V01	OS	Payment Broker	The Offeror shall provide application production support for failure analysis and remediation commensurate to the contracted SLA to ensure proper operation of the Microservice environment.
Policy and Regulation	CPS-RG3155-V01	OS	Payment Broker	The Offeror shall validate the interoperability of their application with other Microservices and the OS core in a sandbox environment.
Policy and Regulation	CPS-RG3157-V01	OS	Payment Broker	The Offeror shall provide the ability to monitor the microservice health and performance of externally built applications deployed to the OS Microservice environment to ensure health of the Microservices environment.
Policy and Regulation	CPS-RG3156-V01	OS	Payment Broker	The Offeror shall inform the OS architectural team when promotion from the sandbox environment to production is ready, to follow production deployment procedures.

USER NEED:	MMTPA/CPS-UN036-v02	USER: City/COTA
Title:	**Compliance**	
Description:	The MMTPA/CPS system needs to be responsible for compliance tasks related to the act of processing and handling payments between the Travelers and the Mobility Providers.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Policy and Regulation	CPS-RG2681-V01	CPS Back Office	PCI Compliance	The CPS shall be responsible for all applicable card transaction security rules and regulations including PCI and DSS compliance, all laws, and any other governing authority requirements as may apply.
Policy and Regulation	CPS-RG2680-V01	CPS Back Office	PCI Compliance	The CPS shall be responsible for PCI compliance.

USER NEED:	MMTPA/CPS-UN038-v02	USER: City/COTA
Title:	**Audit Capability**	
Description:	The MMTPA/CPS system needs to provide the City and COTA with an ability to audit the system. This need includes the ability to conduct a financial audit of system.	
Priority:	Desirable	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2570-V01	CPS Back Office	Reporting	The CPS shall have the ability to generate financial audit reports (CSV and PDF).
Functional	CPS-FN2575-V01	CPS Back Office	Reporting	Financial audit reports shall include unused and remaining value associated with a Traveler account.
Functional	CPS-FN2574-V01	CPS Back Office	Reporting	Financial audit reports shall include pay transactions by location and trip.

Functional	CPS-FN2571-V01	CPS Back Office	Reporting	Financial audit reports shall include fraudulent account activity where the Traveler has informed administrative Users of unrecognized account transactions.
Functional	CPS-FN2572-V01	CPS Back Office	Reporting	Financial audit reports shall include financial reconciliation and pay settlement.
Functional	CPS-FN2573-V01	CPS Back Office	Reporting	Financial audit reports shall include insufficient funds associated with a Traveler account.
Functional	CPS-FN2578-V01	CPS Back Office	Reporting	Financial audit reports shall include reports of transactions that could not be completed due to missing data.
Functional	CPS-FN2576-V01	CPS Back Office	Reporting	Financial audit reports shall include faults and errors.
Functional	CPS-FN2577-V01	CPS Back Office	Reporting	Financial audit reports shall include incomplete transactions.
Functional	CPS-FN3148-V01	CPS Back Office	Reporting	Financial audit reports shall include Service Provider reconciliation of trips made and paid for.

USER NEED:	MMTPA/CPS-UN040-v02	USER: Mobility Provider
Title:	**Mobility Provider Accounts**	
Description:	The MMTPA/CPS System needs to provide Mobility Providers with the ability to manage payment preferences, and to query and view transactions related to payments. Mobility Provider Accounts will facilitate payment transactions and ensure that each Mobility Provider receives payment. The process of payout for each individual Mobility Provider will be defined in the CPS requirements document. Payout timing will be at a negotiated frequency with the Mobility Providers.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2514-V01	CPS Web Portal	Account Management	Service Providers shall have an API to add their existing Traveler accounts to the shared account ledger.
Functional	CPS-FN2511-V01	CPS Web Portal	Account Management	Service Provider accounts shall be administered by the Service Providers.
Functional	CPS-FN2512-V01	CPS Back Office	Provider Accounts	Service Provider accounts shall be created by authorized individuals at the City and COTA, pending review and approval procedures.
Functional	CPS-FN2513-V01	CPS Web Portal	Account Management	Service Provider accounts shall have administrative parameters for setting rates for base cost per trip, distance, travel time, and surge pricing (if applicable).
Functional	CPS-FN2597-V01	CPS Back Office	Notifications and Alerts	Service Providers shall be able to create and manage notifications.

Security	CPS-SR2588-V01	CPS Back Office	Provider Accounts	Service Provider account passwords shall have a minimum of 12 characters with a mix of upper- and lower-case, alphanumeric and special characters.
Security	CPS-SR2586-V01	CPS Back Office	Provider Accounts	Service Providers shall have the ability to reset a lost password.
Security	CPS-SR2590-V01	CPS Back Office	Provider Accounts	Service Providers who have not accessed an account in 90 days of more shall be required to reset password upon next login.
Data	CPS-DR2774-V01	CPS Back Office	PCI Compliance	The CPS Back Office shall manage Provider account data.
Interface	CPS-IF3167-V01	OS	Payment Broker	The CPS shall provide an interface to send transaction information (request ID, amount, request type, Traveler, Provider) from the OS to CPS to be used in payment processing.
Interface	CPS-IF3168-V01	CPS Back Office	Payment Processing	The CPS shall provide an interface to send payment authorization and funds availability from the CPS to OS.

Interface	CPS-IF3172-V01	CPS Web Portal	Provider Account Management	The CPS shall provide an interface to send security credentials, service Provider account information, modifications to service rates and options, report request parameters, and communications requests from the Service Provider's Web Portal to CPS.
Functional	CPS-FN3144-V01	CPS Web Portal	Account Management	The CPS shall provide a secure Web Portal to allow Service Providers to manage accounts in the CPS Back Office.

USER NEED:	**MMTPA/CPS-UN041-v02**	**USER: Mobility Provider**
Title:	**One-to-One and One-to-Many Payment Requests**	
Description:	The MMTPA/CPS System needs to be able to handle one-to-one and one-to-many payment requests, in which payment for multimodal trips is split between numerous Mobility Providers. For example, a Traveler using the MMTAP/CPS system to book a multimodal trip will pay once for the total trip and the Traveler's funds will be split for each trip mode to pay each Mobility Provider separately.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	**Identifier**	**FG**	**Sub-Component**	**Description**
Functional	CPS-FN2482-V01	CPS Back Office	Traveler Accounts	The CPS shall process and clear payments from Travelers directly through a conventional financial payment gateway, or blockchain gateway, not through a middleman merchant account.

USER NEED:	MMTPA/CPS-UN042-v02	USER: Mobility Provider
Title:	**Funds in Reserve**	
Description:	The MMTPA/CPS System needs to be able to hold Traveler funds in reserve for a period of time before being used for services. For example, a Traveler using the MMTPA/CPS to book transportation services may have funds held in reserve until the event has taken place, such as when payment is required at the end of a trip, to ensure that adequate funds are available.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	FG	Sub-Component	Description
Functional	CPS-FN2528-V01	CPS Back Office	Administration	The CPS shall permit administrative Users with limited access to transfer the balance (stored cash value) of one registered CPS account to another registered CPS account.
Functional	CPS-FN2557-V01	CPS Back Office	Payment Processing	In the event that the service for which the funds are being held is not realized, the hold on the funds shall be removed and credit restored to the Traveler account as necessary.
Functional	CPS-FN2556-V01	CPS Back Office	Payment Processing	The CPS shall be capable of holding funds in reserve for a period of time as a credit guarantee for services where cost is not fixed (such as fares based on surge pricing, distance or duration) or when an event has yet to occur (such as when payment is required at the end of the trip).

Source: City of Columbus

Appendix D. Mapped System Interfaces

Table 27: Mapped System Interfaces provides a relational mapping of each system interface to the requirements that were created based off that User defined in **Chapter 3**. This organization is intended for ease of use and quick reference during system design.

Table 27: Mapped System Interfaces

Interface ID	Reference	Requirement ID
CPS-IX2817-V01	Interface 1.1	CPS-IF3159-V01
CPS-IX2818-V01	Interface 1.2	CPS-IF3160-V01 CPS-PR3152-V01
CPS-IX2819-V01	Interface 1.3	CPS-IF3161-V01 CPS-PR3152-V01
CPS-IX2820-V01	Interface 1.4	CPS-IF3162-V01 CPS-PR3152-V01
CPS-IX2821-V01	Interface 1.5	CPS-IF3163-V01 CPS-PR3152-V01
CPS-IX2822-V01	Interface 1.6	CPS-IF3164-V01 CPS-PR3152-V01
CPS-IX2823-V01	Interface 1.7	CPS-IF3165-V01 CPS-PR3152-V01
CPS-IX2824-V01	Interface 1.8	CPS-IF3166-V01 CPS-PR3152-V01
CPS-IX2825-V01	Interface 2.1	CPS-IF3167-V01
CPS-IX2826-V01	Interface 2.2	CPS-IF3168-V01
CPS-IX2827-V01	Interface 2.3	CPS-IF3169-V01
CPS-IX2828-V01	Interface 3.1	CPS-IF3170-V01
CPS-IX2829-V01	Interface 3.2	CPS-IF3171-V01
CPS-IX2830-V01	Interface 3.3	CPS-IF3172-V01
CPS-IX2831-V01	Interface 3.4	CPS-IF3173-V01
CPS-IX2832-V01	Interface 3.5	CPS-IF3174-V01
CPS-IX2833-V01	Interface 3.6	CPS-IF3175-V01
CPS-IX2834-V01	Interface 3.7	CPS-IF3176-V01
CPS-IX2835-V01	Interface 3.8	CPS-IF3177-V01
CPS-IX2836-V01	Interface 4	CPS-IF3178-V01
CPS-IX2837-V01	Interface 5	CPS-IF3179-V01

Interface ID	Reference	Requirement ID
CPS-IX2838-V01	Interface 6	CPS-IF3180-V01
CPS-IX2839-V01	Interface 7.1	CPS-IF3181-V01 CPS-PR3153-V01
CPS-IX2840-V01	Interface 7.2	CPS-IF3182-V01 CPS-PR3153-V01
CPS-IX2841-V01	Interface 7.3	CPS-IF3183-V01 CPS-PR3153-V01
CPS-IX2842-V01	Interface 7.4	CPS-IF3184-V01 CPS-PR3153-V01
CPS-IX2843-V01	Interface 7.5	CPS-IF3185-V01 CPS-PR3153-V01
CPS-IX2844-V01	Interface 7.6	CPS-IF3186-V01 CPS-PR3153-V01
CPS-IX2845-V01	Interface 8.1	CPS-IF3187-V01
CPS-IX2846-V01	Interface 8.2	CPS-IF3188-V01
CPS-IX2856-V01	Interface 100	CPS-IF3189-V01
CPS-IX2857-V01	Interface 101	CPS-IF3190-V01
CPS-IX2858-V01	Interface 102	CPS-IF3191-V01
CPS-IX2859-V01	Interface 103	CPS-IF3192-V01
CPS-IX3194-V01	Interface 104.1	CPS-IF3169-V01
CPS-IX3195-V01	Interface 104.2	CPS-IF3169-V01

Source: City of Columbus

Appendix E. Mapped Constraints

Table 28: Mapped Constraints provides a relational mapping of each project constraint to the requirements that were created based off that User defined in **Chapter 3**. This organization is intended for ease of use and quick reference during system design.

Table 28: Mapped Constraints

Constraint ID	Reference	Requirement ID
CPS-CN2813-V01	Constraint 1	CPS-FN2559-V01 CPS-FN2561-V01 CPS-FN2560-V01
CPS-CN2814-V01	Constraint 2	CPS-RG2678-V01 CPS-RG2676-V01 CPS-RG2677-V01
CPS-CN2815-V01	Constraint 3	CPS-FN2510-V01 CPS-FN2484-V01 CPS-FN2496-V01 CPS-FN2511-V01 CPS-FN2470-V01 CPS-FN2471-V01 CPS-FN2596-V01 CPS-IF2724-V01

Source: City of Columbus

Appendix F. Other Requirement Relations

Table 29: Other Requirement Relations provides a relational mapping of each requirement. This organization is intended for ease of use and quick reference during system design.

Table 29: Other Requirement Relations

ReqID	Related Requirements
CPS-FN2464-V01	MMTPA/CPS-UN006-v02
CPS-FN2465-V01	MMTPA/CPS-UN006-v02
CPS-FN2466-V01	MMTPA/CPS-UN022-v02
CPS-FN2468-V01	MMTPA/CPS-UN022-v02
CPS-FN2469-V01	MMTPA/CPS-UN022-v02
CPS-FN2470-V01	MMTPA/CPS-UN006-v02 CPS-CN2815-V01
CPS-FN2471-V01	MMTPA/CPS-UN006-v02 CPS-CN2815-V01
CPS-FN2472-V01	MMTPA/CPS-UN025-v02
CPS-FN2473-V01	MMTPA/CPS-UN025-v02
CPS-FN2474-V01	MMTPA/CPS-UN022-v02
CPS-FN2475-V01	MMTPA/CPS-UN022-v02
CPS-FN2476-V01	MMTPA/CPS-UN027-v02
CPS-FN2477-V01	MMTPA/CPS-UN027-v02
CPS-FN2478-V01	MMTPA/CPS-UN022-v02
CPS-FN2479-V01	MMTPA/CPS-UN007-v02
CPS-FN2480-V01	MMTPA/CPS-UN022-v02
CPS-FN2481-V01	MMTPA/CPS-UN022-v02
CPS-FN2482-V01	MMTPA/CPS-UN041-v02
CPS-FN2484-V01	MMTPA/CPS-UN021-v02 CPS-CN2815-V01
CPS-FN2487-V01	MMTPA/CPS-UN025-v02
CPS-FN2488-V01	MMTPA/CPS-UN026-v02
CPS-FN2490-V01	MMTPA/CPS-UN026-v02
CPS-FN2491-V01	MMTPA/CPS-UN026-v02
CPS-FN2493-V01	MMTPA/CPS-UN028-v02
CPS-FN2494-V01	MMTPA/CPS-UN028-v02

ReqID	Related Requirements
CPS-FN2495-V01	MMTPA/CPS-UN024-v02
CPS-FN2496-V01	MMTPA/CPS-UN035-v02 CPS-CN2815-V01
CPS-FN2499-V01	MMTPA/CPS-UN035-v02
CPS-FN2500-V01	MMTPA/CPS-UN022-v02
CPS-FN2503-V01	MMTPA/CPS-UN023-v02
CPS-FN2504-V01	MMTPA/CPS-UN023-v02
CPS-FN2505-V01	MMTPA/CPS-UN034-v02 CPS-FN2506-V01
CPS-FN2506-V01	MMTPA/CPS-UN034-v02 CPS-FN2505-V01 CPS-FN2528-V01 CPS-FN2529-V01 CPS-FN2569-V01
CPS-FN2507-V01	MMTPA/CPS-UN022-v02
CPS-SR2508-V01	MMTPA/CPS-UN022-v02
CPS-FN2509-V01	MMTPA/CPS-UN022-v02
CPS-FN2510-V01	MMTPA/CPS-UN022-v02 CPS-CN2815-V01
CPS-FN2511-V01	MMTPA/CPS-UN040-v02 CPS-CN2815-V01
CPS-FN2512-V01	MMTPA/CPS-UN040-v02
CPS-FN2513-V01	MMTPA/CPS-UN040-v02
CPS-FN2514-V01	MMTPA/CPS-UN040-v02
CPS-FN2515-V01	MMTPA/CPS-UN022-v02
CPS-FN2516-V01	MMTPA/CPS-UN022-v02
CPS-FN2517-V01	MMTPA/CPS-UN022-v02
CPS-FN2518-V01	MMTPA/CPS-UN022-v02
CPS-FN2520-V01	MMTPA/CPS-UN022-v02
CPS-FN2521-V01	MMTPA/CPS-UN022-v02
CPS-FN2522-V01	MMTPA/CPS-UN022-v02
CPS-FN2523-V01	MMTPA/CPS-UN022-v02
CPS-FN2524-V01	MMTPA/CPS-UN022-v02
CPS-FN2525-V01	MMTPA/CPS-UN022-v02
CPS-FN2526-V01	MMTPA/CPS-UN022-v02
CPS-FN2527-V01	MMTPA/CPS-UN022-v02

ReqID	Related Requirements
CPS-FN2528-V01	MMTPA/CPS-UN034-v02 MMTPA/CPS-UN042-v02 CPS-FN2506-V01
CPS-FN2529-V01	MMTPA/CPS-UN034-v02 CPS-FN2506-V01
CPS-FN2530-V01	MMTPA/CPS-UN022-v02
CPS-FN2531-V01	MMTPA/CPS-UN022-v02
CPS-FN2532-V01	MMTPA/CPS-UN022-v02
CPS-FN2533-V01	MMTPA/CPS-UN022-v02
CPS-FN2534-V01	MMTPA/CPS-UN026-v02
CPS-FN2536-V01	MMTPA/CPS-UN026-v02
CPS-FN2537-V01	MMTPA/CPS-UN026-v02
CPS-FN2538-V01	MMTPA/CPS-UN026-v02
CPS-FN2539-V01	MMTPA/CPS-UN022-v02
CPS-FN2540-V01	MMTPA/CPS-UN022-v02
CPS-FN2542-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02
CPS-FN2544-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02
CPS-FN2545-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02
CPS-FN2546-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02
CPS-FN2547-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02
CPS-FN2548-V01	MMTPA/CPS-UN024-v02
CPS-FN2549-V01	MMTPA/CPS-UN024-v02
CPS-FN2550-V01	MMTPA/CPS-UN024-v02
CPS-FN2551-V01	MMTPA/CPS-UN024-v02
CPS-FN2553-V01	MMTPA/CPS-UN022-v02
CPS-FN2554-V01	MMTPA/CPS-UN021-v02
CPS-FN2555-V01	MMTPA/CPS-UN020-v02
CPS-FN2556-V01	MMTPA/CPS-UN042-v02
CPS-FN2557-V01	MMTPA/CPS-UN042-v02
CPS-SR2558-V01	MMTPA/CPS-UN029-v02

ReqID	Related Requirements
CPS-FN2559-V01	MMTPA/CPS-UN026-v02 CPS-CN2813-V01
CPS-FN2560-V01	MMTPA/CPS-UN026-v02 CPS-CN2813-V01
CPS-FN2561-V01	MMTPA/CPS-UN026-v02 CPS-CN2813-V01
CPS-FN2566-V01	MMTPA/CPS-UN029-v02
CPS-FN2567-V01	MMTPA/CPS-UN029-v02
CPS-FN2568-V01	MMTPA/CPS-UN029-v02
CPS-FN2569-V01	MMTPA/CPS-UN034-v02 CPS-FN2506-V01
CPS-FN2570-V01	MMTPA/CPS-UN038-v02
CPS-FN2571-V01	MMTPA/CPS-UN038-v02
CPS-FN2572-V01	MMTPA/CPS-UN038-v02
CPS-FN2573-V01	MMTPA/CPS-UN038-v02
CPS-FN2574-V01	MMTPA/CPS-UN038-v02
CPS-FN2575-V01	MMTPA/CPS-UN038-v02
CPS-FN2576-V01	MMTPA/CPS-UN038-v02
CPS-FN2577-V01	MMTPA/CPS-UN038-v02
CPS-FN2578-V01	MMTPA/CPS-UN038-v02
CPS-FN2579-V01	MMTPA/CPS-UN033-v02
CPS-FN2580-V01	MMTPA/CPS-UN033-v02
CPS-FN2581-V01	MMTPA/CPS-UN033-v02
CPS-FN2582-V01	MMTPA/CPS-UN033-v02
CPS-FN2583-V01	MMTPA/CPS-UN033-v02
CPS-SR2584-V01	MMTPA/CPS-UN022-v02
CPS-SR2585-V01	MMTPA/CPS-UN022-v02
CPS-SR2586-V01	MMTPA/CPS-UN040-v02
CPS-SR2587-V01	MMTPA/CPS-UN022-v02
CPS-SR2588-V01	MMTPA/CPS-UN040-v02
CPS-SR2589-V01	MMTPA/CPS-UN022-v02
CPS-SR2590-V01	MMTPA/CPS-UN040-v02
CPS-FN2591-V01	MMTPA/CPS-UN022-v02
CPS-FN2592-V01	MMTPA/CPS-UN022-v02
CPS-FN2593-V01	MMTPA/CPS-UN022-v02

ReqID	Related Requirements
CPS-FN2594-V01	MMTPA/CPS-UN022-v02
CPS-FN2595-V01	MMTPA/CPS-UN022-v02
CPS-FN2596-V01	MMTPA/CPS-UN022-v02 CPS-CN2815-V01
CPS-FN2597-V01	MMTPA/CPS-UN040-v02
CPS-FN2598-V01	MMTPA/CPS-UN021-v02
CPS-FN2599-V01	MMTPA/CPS-UN021-v02
CPS-FN2600-V01	MMTPA/CPS-UN021-v02
CPS-FN2601-V01	MMTPA/CPS-UN021-v02
CPS-FN2602-V01	MMTPA/CPS-UN019-v02
CPS-FN2603-V01	MMTPA/CPS-UN019-v02
CPS-FN2604-V01	MMTPA/CPS-UN021-v02
CPS-FN2605-V01	MMTPA/CPS-UN021-v02
CPS-FN2606-V01	MMTPA/CPS-UN021-v02
CPS-FN2607-V01	MMTPA/CPS-UN021-v02
CPS-FN2608-V01	MMTPA/CPS-UN021-v02
CPS-FN2609-V01	MMTPA/CPS-UN021-v02
CPS-FN2610-V01	MMTPA/CPS-UN021-v02
CPS-FN2611-V01	MMTPA/CPS-UN021-v02
CPS-FN2612-V01	MMTPA/CPS-UN021-v02
CPS-FN2613-V01	MMTPA/CPS-UN021-v02
CPS-FN2614-V01	MMTPA/CPS-UN021-v02
CPS-FN2615-V01	MMTPA/CPS-UN019-v02
CPS-FN2616-V01	MMTPA/CPS-UN021-v02
CPS-FN2617-V01	MMTPA/CPS-UN008-v02
CPS-FN2621-V01	MMTPA/CPS-UN022-v02
CPS-FN2622-V01	MMTPA/CPS-UN022-v02
CPS-FN2623-V01	MMTPA/CPS-UN022-v02
CPS-FN2624-V01	MMTPA/CPS-UN028-v02
CPS-FN2625-V01	MMTPA/CPS-UN028-v02
CPS-FN2626-V01	MMTPA/CPS-UN028-v02
CPS-FN2627-V01	MMTPA/CPS-UN028-v02
CPS-FN2628-V01	MMTPA/CPS-UN028-v02
CPS-FN2629-V01	MMTPA/CPS-UN022-v02
CPS-FN2630-V01	MMTPA/CPS-UN008-v02

ReqID	Related Requirements
CPS-FN2631-V01	MMTPA/CPS-UN022-v02
CPS-FN2632-V01	MMTPA/CPS-UN027-v02
CPS-FN2633-V01	MMTPA/CPS-UN028-v02
CPS-FN2634-V01	MMTPA/CPS-UN028-v02
CPS-FN2636-V01	MMTPA/CPS-UN016-v02
CPS-FN2637-V01	MMTPA/CPS-UN016-v02
CPS-FN2638-V01	MMTPA/CPS-UN011-v02
CPS-FN2639-V01	MMTPA/CPS-UN011-v02
CPS-FN2640-V01	MMTPA/CPS-UN011-v02
CPS-FN2641-V01	MMTPA/CPS-UN033-v02
CPS-FN2644-V01	MMTPA/CPS-UN006-v02
CPS-FN2645-V01	MMTPA/CPS-UN006-v02
CPS-FN2646-V01	MMTPA/CPS-UN022-v02
CPS-DR2647-V01	MMTPA/CPS-UN033-v02
CPS-SR2648-V01	MMTPA/CPS-UN031-v02
CPS-SR2649-V01	MMTPA/CPS-UN031-v02
CPS-SR2650-V01	MMTPA/CPS-UN031-v02
CPS-SR2651-V01	MMTPA/CPS-UN031-v02
CPS-SR2652-V01	MMTPA/CPS-UN031-v02
CPS-SR2653-V01	MMTPA/CPS-UN031-v02
CPS-SR2654-V01	MMTPA/CPS-UN031-v02
CPS-SR2655-V01	MMTPA/CPS-UN031-v02
CPS-SR2656-V01	MMTPA/CPS-UN031-v02
CPS-SR2657-V01	MMTPA/CPS-UN031-v02
CPS-SR2658-V01	MMTPA/CPS-UN031-v02
CPS-SR2659-V01	MMTPA/CPS-UN031-v02
CPS-PY2660-V01	MMTPA/CPS-UN021-v02
CPS-IM2661-V01	MMTPA/CPS-UN034-v02
CPS-LC2662-V01	MMTPA/CPS-UN034-v02
CPS-LC2663-V01	MMTPA/CPS-UN034-v02
CPS-LC2664-V01	MMTPA/CPS-UN034-v02
CPS-LC2665-V01	MMTPA/CPS-UN034-v02
CPS-LC2666-V01	MMTPA/CPS-UN034-v02
CPS-LC2667-V01	MMTPA/CPS-UN034-v02

ReqID	Related Requirements
CPS-LC2668-V01	MMTPA/CPS-UN034-v02
CPS-LC2669-V01	MMTPA/CPS-UN034-v02
CPS-LC2670-V01	MMTPA/CPS-UN034-v02
CPS-LC2671-V01	MMTPA/CPS-UN034-v02
CPS-LC2672-V01	MMTPA/CPS-UN034-v02
CPS-LC2673-V01	MMTPA/CPS-UN034-v02
CPS-LC2674-V01	MMTPA/CPS-UN034-v02
CPS-LC2675-V01	MMTPA/CPS-UN034-v02
CPS-RG2676-V01	MMTPA/CPS-UN035-v02 CPS-CN2814-V01
CPS-RG2677-V01	MMTPA/CPS-UN035-v02 CPS-CN2814-V01
CPS-RG2678-V01	MMTPA/CPS-UN035-v02 CPS-CN2814-V01
CPS-RG2679-V01	MMTPA/CPS-UN035-v02
CPS-RG2680-V01	MMTPA/CPS-UN036-v02
CPS-RG2681-V01	MMTPA/CPS-UN036-v02
CPS-DP2682-V01	MMTPA/CPS-UN034-v02
CPS-AR2710-V01	MMTPA/CPS-UN034-v02
CPS-AR2711-V01	MMTPA/CPS-UN034-v02
CPS-AR2712-V01	MMTPA/CPS-UN034-v02
CPS-AR2713-V01	MMTPA/CPS-UN034-v02
CPS-AR2714-V01	MMTPA/CPS-UN034-v02
CPS-DR2715-V01	MMTPA/CPS-UN033-v02
CPS-DR2716-V01	MMTPA/CPS-UN013-v02
CPS-PR2718-V01	MMTPA/CPS-UN028-v02 MMTPA/CPS-UN022-v02
CPS-SR2719-V01	MMTPA/CPS-UN031-v02
CPS-SR2720-V01	MMTPA/CPS-UN031-v02
CPS-SR2721-V01	MMTPA/CPS-UN031-v02
CPS-SR2722-V01	MMTPA/CPS-UN031-v02
CPS-SR2723-V01	MMTPA/CPS-UN031-v02
CPS-IF2724-V01	CPS-CN2815-V01
CPS-IF2725-V01	MMTPA/CPS-UN032-v02
CPS-IF2726-V01	MMTPA/CPS-UN012-v02

ReqID	Related Requirements
CPS-IF2727-V01	MMTPA/CPS-UN012-v02
CPS-IF2728-V01	MMTPA/CPS-UN012-v02
CPS-FN2730-V01	MMTPA/CPS-UN021-v02
CPS-IM2732-V01	MMTPA/CPS-UN034-v02
CPS-IM2735-V01	MMTPA/CPS-UN034-v02
CPS-IM2736-V01	MMTPA/CPS-UN034-v02
CPS-IM2737-V01	MMTPA/CPS-UN034-v02
CPS-IM2738-V01	MMTPA/CPS-UN034-v02
CPS-IM2739-V01	MMTPA/CPS-UN034-v02
CPS-DR2764-V01	MMTPA/CPS-UN007-v02
CPS-DR2765-V01	MMTPA/CPS-UN007-v02
CPS-DR2766-V01	MMTPA/CPS-UN028-v02
CPS-DR2767-V01	MMTPA/CPS-UN028-v02
CPS-DR2768-V01	MMTPA/CPS-UN016-v02
CPS-DR2769-V01	MMTPA/CPS-UN016-v02
CPS-DR2770-V01	MMTPA/CPS-UN016-v02
CPS-DR2771-V01	MMTPA/CPS-UN016-v02
CPS-DR2772-V01	MMTPA/CPS-UN029-v02
CPS-DR2773-V01	MMTPA/CPS-UN022-v02
CPS-DR2774-V01	MMTPA/CPS-UN040-v02
CPS-DR2775-V01	MMTPA/CPS-UN033-v02
CPS-DR2776-V01	MMTPA/CPS-UN021-v02
CPS-DR2777-V01	MMTPA/CPS-UN021-v02
CPS-SR2778-V01	MMTPA/CPS-UN029-v02
CPS-SR2779-V01	MMTPA/CPS-UN029-v02
CPS-SR2780-V01	MMTPA/CPS-UN029-v02
CPS-SR2781-V01	MMTPA/CPS-UN029-v02
CPS-SR2782-V01	MMTPA/CPS-UN029-v02
CPS-SR2783-V01	MMTPA/CPS-UN029-v02
CPS-SR2784-V01	MMTPA/CPS-UN029-v02
CPS-SR2785-V01	MMTPA/CPS-UN029-v02
CPS-SR2786-V01	MMTPA/CPS-UN029-v02
CPS-SR2787-V01	MMTPA/CPS-UN029-v02
CPS-SR2788-V01	MMTPA/CPS-UN029-v02

ReqID	Related Requirements
CPS-SR2789-V01	MMTPA/CPS-UN029-v02
CPS-SR2790-V01	MMTPA/CPS-UN029-v02
CPS-SR2791-V01	MMTPA/CPS-UN029-v02
CPS-AT2921-V01	MMTPA/CPS-UN034-v02
CPS-AT2922-V01	MMTPA/CPS-UN034-v02
CPS-AT2923-V01	MMTPA/CPS-UN034-v02
CPS-AT2924-V01	MMTPA/CPS-UN034-v02
CPS-AT2925-V01	MMTPA/CPS-UN034-v02
CPS-AT2926-V01	MMTPA/CPS-UN034-v02
CPS-AT2927-V01	MMTPA/CPS-UN034-v02
CPS-AT2928-V01	MMTPA/CPS-UN034-v02
CPS-AT2929-V01	MMTPA/CPS-UN034-v02
CPS-AT2930-V01	MMTPA/CPS-UN034-v02
CPS-AT2931-V01	MMTPA/CPS-UN034-v02
CPS-AT2932-V01	MMTPA/CPS-UN034-v02
CPS-AT2933-V01	MMTPA/CPS-UN034-v02
CPS-AT2934-V01	MMTPA/CPS-UN034-v02
CPS-AT2935-V01	MMTPA/CPS-UN034-v02
CPS-AT2936-V01	MMTPA/CPS-UN034-v02
CPS-AT2937-V01	MMTPA/CPS-UN034-v02
CPS-AT2938-V01	MMTPA/CPS-UN034-v02
CPS-AT2939-V01	MMTPA/CPS-UN034-v02
CPS-AT2940-V01	MMTPA/CPS-UN034-v02
CPS-AT2941-V01	MMTPA/CPS-UN034-v02
CPS-AT2942-V01	MMTPA/CPS-UN034-v02
CPS-AT2943-V01	MMTPA/CPS-UN034-v02
CPS-AT2944-V01	MMTPA/CPS-UN034-v02
CPS-AT2945-V01	MMTPA/CPS-UN034-v02
CPS-AT2946-V01	MMTPA/CPS-UN034-v02
CPS-AT2947-V01	MMTPA/CPS-UN034-v02
CPS-MT2948-V01	MMTPA/CPS-UN034-v02
CPS-MT2949-V01	MMTPA/CPS-UN034-v02
CPS-MT2950-V01	MMTPA/CPS-UN034-v02
CPS-FN3132-V01	MMTPA/CPS-UN022-v02

ReqID	Related Requirements
CPS-FN3133-V01	MMTPA/CPS-UN022-v02
CPS-FN3134-V01	MMTPA/CPS-UN022-v02
CPS-FN3135-V01	MMTPA/CPS-UN022-v02
CPS-FN3136-V01	MMTPA/CPS-UN022-v02
CPS-FN3137-V01	MMTPA/CPS-UN022-v02
CPS-FN3138-V01	MMTPA/CPS-UN022-v02
CPS-FN3139-V01	MMTPA/CPS-UN021-v02
CPS-FN3140-V01	MMTPA/CPS-UN022-v02
CPS-FN3141-V01	MMTPA/CPS-UN013-v02
CPS-FN3142-V01	MMTPA/CPS-UN019-v02 MMTPA/CPS-UN021-v02
CPS-FN3143-V01	MMTPA/CPS-UN019-v02 MMTPA/CPS-UN021-v02
CPS-FN3144-V01	MMTPA/CPS-UN028-v02 MMTPA/CPS-UN040-v02
CPS-FN3145-V01	MMTPA/CPS-UN028-v02
CPS-FN3146-V01	MMTPA/CPS-UN022-v02
CPS-FN3147-V01	MMTPA/CPS-UN022-v02
CPS-FN3148-V01	MMTPA/CPS-UN038-v02
CPS-FN3149-V01	MMTPA/CPS-UN021-v02
CPS-FN3150-V01	MMTPA/CPS-UN011-v02
CPS-FN3151-V01	MMTPA/CPS-UN021-v02
CPS-PR3152-V01	MMTPA/CPS-UN022-v02 CPS-IX2818-V01 CPS-IX2819-V01 CPS-IX2820-V01 CPS-IX2821-V01 CPS-IX2822-V01 CPS-IX2823-V01 CPS-IX2824-V01
CPS-PR3153-V01	MMTPA/CPS-UN022-v02 CPS-IX2839-V01 CPS-IX2840-V01 CPS-IX2841-V01 CPS-IX2842-V01 CPS-IX2843-V01 CPS-IX2844-V01
CPS-RG3154-V01	MMTPA/CPS-UN035-v02

ReqID	Related Requirements
CPS-RG3155-V01	MMTPA/CPS-UN035-v02
CPS-RG3156-V01	MMTPA/CPS-UN035-v02
CPS-RG3157-V01	MMTPA/CPS-UN035-v02
CPS-RG3158-V01	MMTPA/CPS-UN035-v02
CPS-IF3159-V01	MMTPA/CPS-UN006-v02 CPS-IX2817-V01
CPS-IF3160-V01	MMTPA/CPS-UN006-v02 CPS-IX2818-V01
CPS-IF3161-V01	MMTPA/CPS-UN016-v02 CPS-IX2819-V01
CPS-IF3162-V01	MMTPA/CPS-UN006-v02 CPS-IX2820-V01
CPS-IF3163-V01	MMTPA/CPS-UN006-v02 MMTPA/CPS-UN027-v02 CPS-IX2821-V01
CPS-IF3164-V01	MMTPA/CPS-UN006-v02 MMTPA/CPS-UN027-v02 CPS-IX2822-V01
CPS-IF3165-V01	MMTPA/CPS-UN006-v02 MMTPA/CPS-UN027-v02 CPS-IX2823-V01
CPS-IF3166-V01	MMTPA/CPS-UN006-v02 MMTPA/CPS-UN027-v02 CPS-IX2824-V01
CPS-IF3167-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN040-v02 CPS-IX2825-V01
CPS-IF3168-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN040-v02 CPS-IX2826-V01
CPS-IF3169-V01	MMTPA/CPS-UN016-v02 CPS-IX2827-V01
CPS-IF3170-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02 CPS-IX2828-V01
CPS-IF3171-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02 CPS-IX2829-V01

ReqID	Related Requirements
CPS-IF3172-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN040-v02 CPS-IX2830-V01
CPS-IF3173-V01	MMTPA/CPS-UN022-v02 MMTPA/CPS-UN023-v02 CPS-IX2831-V01
CPS-IF3174-V01	MMTPA/CPS-UN027-v02 CPS-IX2832-V01
CPS-IF3175-V01	MMTPA/CPS-UN016-v02 MMTPA/CPS-UN027-v02 CPS-IX2833-V01
CPS-IF3176-V01	MMTPA/CPS-UN022-v02 CPS-IX2834-V01
CPS-IF3177-V01	MMTPA/CPS-UN022-v02 CPS-IX2835-V01
CPS-IF3178-V01	MMTPA/CPS-UN021-v02 CPS-IX2836-V01
CPS-IF3179-V01	MMTPA/CPS-UN021-v02 CPS-IX2837-V01
CPS-IF3180-V01	MMTPA/CPS-UN021-v02 CPS-IX2838-V01
CPS-IF3181-V01	MMTPA/CPS-UN022-v02 CPS-IX2839-V01
CPS-IF3182-V01	MMTPA/CPS-UN022-v02 CPS-IX2840-V01
CPS-IF3183-V01	MMTPA/CPS-UN022-v02 CPS-IX2841-V01
CPS-IF3184-V01	MMTPA/CPS-UN022-v02 CPS-IX2842-V01
CPS-IF3185-V01	MMTPA/CPS-UN022-v02 CPS-IX2843-V01
CPS-IF3186-V01	MMTPA/CPS-UN022-v02 CPS-IX2844-V01
CPS-IF3187-V01	MMTPA/CPS-UN006-v02 CPS-IX2845-V01
CPS-IF3188-V01	MMTPA/CPS-UN006-v02 CPS-IX2846-V01
CPS-IF3189-V01	MMTPA/CPS-UN022-v02 CPS-IX2856-V01

ReqID	Related Requirements
CPS-IF3190-V01	MMTPA/CPS-UN022-v02 CPS-IX2857-V01
CPS-IF3191-V01	MMTPA/CPS-UN022-v02 CPS-IX2858-V01
CPS-IF3192-V01	MMTPA/CPS-UN033-v02 CPS-IX2859-V01

Source: City of Columbus

Appendix G. Acronyms and Abbreviations

Table 30: Acronym List contains definitions for project-specific acronyms and abbreviations used throughout this document.

Table 30: Acronym List

Abbreviation/Acronym	Definition
API	Application Programming Interface
AT	Acceptance Testing (**Table 9: List of Requirement Types**)
ATP	Acceptance Test Plan
AR	Availability and Recovery
BLE	Bluetooth Low Energy
CCV	Card Verification Value
CFMS	Central Fare Management System
CITY	City of Columbus (**Table 3: System Functional Groups**)
ConOps	Concept of Operations
COTA	Central Ohio Transit Authority (**Table 3: System Functional Groups**)
CPS	Common Payment System (**Table 3: System Functional Groups**)
DoS	Denial of Service
DP	Disposal (**Table 9: List of Requirement Types**)
DR	Date Requirements (**Table 9: List of Requirement Types**)
e-	Electronic
EN	Enabling (**Table 9: List of Requirement Types**)
EPM	Event Parking Management
EPMCS	Event Parking Management Central System (**Table 3: System Functional Groups**)
FBOX	COTA Onboard Payment Equipment (Farebox) (**Table 3: System Functional Groups**)
FG	Functional Group
FHWA	Federal Highway Administration
FIN	Financial Institution (**Table 3: System Functional Groups)**
FN	Functional (**Table 9: List of Requirement Types**)
HUBS	Smart Mobility Hubs (**Table 3: System Functional Groups**)
IEEE	Institute of Electrical and Electronics Engineers
IF	Interfaces (**Table 9: List of Requirement Types**)

Abbreviation/Acronym	Definition
IM	Information Management (**Table 9: List of Requirement Types**)
IPSec	Internet Protocol Security
ISO	International Standards Organization
IT	Information Technology
ITS	Intelligent Transportation System
IVR	Interactive Voice Response (**Table 3: System Functional Groups**)
JPO	Joint Program Office
LC	Life-Cycle (**Table 9: List of Requirement Types**)
LUM	Limited Use Media
MaaS	Mobility as a Service
MCO	Managed Care Organization
MMTPA	Multimodal Trip Planning Application
MPCS	Mobility Provider Central Systems (**Table 3: System Functional Groups**)
MPE	Mobility Provider Payment Equipment (**Table 3: System Functional Groups**)
MT	Maintainability (**Table 9: List of Requirement Types**)
NEMT	Non-Emergency Medical Transportation
NF	Non-Functional (**Table 9: List of Requirement Types**)
NFC	Near Field Communication
O/D	Origin and Destination
OS	Smart Columbus Operating System (**Table 3: System Functional Groups**)
PAYD	Payment Device (**Table 3: System Functional Groups**)
PCI	Payment Card Industry
PID	Personal Information Device (**Table 3: System Functional Groups**)
PII	Personally Identifiable Information
PY	Physical (**Table 9: List of Requirement Types**)
POS	Point of Sale (**Table 3: System Functional Groups**)
PR	Performance Requirements (**Table 9: List of Requirement Types**)
QR	Quick Response
RFID	Radio-Frequency Identification
RG	Policy and Regulation (**Table 9: List of Requirement Types**)
RTVM	Requirements Traceability Verification Matrix
SA	System Acceptance
SC	Smart Columbus
SDD	System Design Documentation

Abbreviation/Acronym	Definition
SDK	Software Development Kit
SEMP	Systems Engineering Management Plan
SOS	System of Systems
SR	Security Requirements (**Table 9: List of Requirement Types**)
ST	Storage and Transport (**Table 9: List of Requirement Types**)
SyRS	System Requirements Specification
TBD	To Be Determined
THRD	Third-Party User (**Table 3: System Functional Groups**)
TNC	Transportation Network Company
TRD	Test Results Documentation
TVM	Ticket Vending Machine
UC	Use Case
UI	User Interface
USDOT	U.S. Department of Transportation
WCAG	Web Content Accessibility Guidelines
WEB	Web Portal (**Table 3: System Functional Groups**)

Source: City of Columbus

Appendix H. Glossary

Table 31: Glossary contains project specific terms used throughout this document.

Table 31: Glossary

Term	Definition
311 Columbus Call Center	The City of Columbus Service Center, which is the single point of contact for requesting all non-emergency City services and is available to residents, City businesses and visitors
Agile	A method of project management that is characterized by the division of tasks into short phases of work and frequent reassessment and adaptation of plans
Anonymous payment data	
App	Software application
Banked Users	Banked Users have set-up a User account with funds deposited in their account or credit card information saved.
Travelers (end Users)	The Travelers (residents and visitors) in Columbus who will be interacting with the EPMCS to view, plan, reserve, and navigate to desired parking
COTA Central Fare Management System (CFMS)	System implemented through a recently executed contract with SPX/Genfare that will accept various forms of payment including cash, magnetic cards, smart cards and mobile tickets
Commercial-off-the-shelf system (COTS)	Software or hardware products that are ready-made and available for sale to the public
Data privacy	The reasonable expectation that data of a sensitive nature will be kept confidential, sanitized and/or encrypted, and respectfully and responsibly maintained by all Users, managers and collectors of the data.
Data retention	The continued storage of data for compliance or business reasons
Data security	The tools, policies, practices, and procedures used to protect data from being accessed, manipulated or destroyed or being leveraged by those with a malicious intent or without authorization, as well as the corrective actions taken when data breaches are suspected or have been identified.
Dependency	When one Project, agency or entity requires data or functionality provided by another Project, agency or entity to meet its objectives
Enabling Technologies	An innovation that alone or paired with an existing solution produces a better end User solution at a rapid rate
Experience Columbus	An organization whose mission is to market and promote Columbus services, attractions and facilities to visitors, meeting planners, convention delegates, and residents
Failure operations	When a complete failure of the intersection occurs, primarily due to loss of power or other malfunctions
Fare collection system	A system, either automated or manual, that collects fares for Transportation Service Providers (TSPs)

Term	Definition
Multimodal transportation	Travel that is performed with more than one mode of transportation
Open-data	Information freely available for anyone to use and republish as they wish
Open-source concepts	The notion of open collaboration and voluntary contribution for software development by writing and exchanging programming code
Payment data	
Payment settlement	The process by which funds are sent by an issuing bank to the CPS for processing and dispersal to the Transportation Network Companies
Personally Identifiable Information (PII)	Information used in security and privacy laws that can be used to identify an individual, such as vehicle, Traveler, and payment information
Parking facility	Land or a structure used for light-duty vehicle parking
Parking management system	A system intended to aggregate location, availability, payment information, and reservation capabilities across all public and private parking options
Procurement	The act of obtaining or acquiring goods, services or works, from a competitive bidding process
Push notifications	Alert Users to relevant information pertaining to a route or selected mode of transportation, such as the approach of a transfer location, congestion or other impediment to travel, or pricing change
Quick Response barcode	Commonly referred to as a QR code. A barcode that stores information that can be used for marketing or sharing information and can be read using a digital device such as a smartphone.
Real-time data	Information that is delivered immediately after collection.
Smart parking meter	A parking meter equipped with technology to collect data and make interactions easier for the end User.
Smart sensors	A device that takes input from the physical environment and uses built-in technology to perform functions upon detection of specific input and then process data before passing it on.
System analytics or data analytics	The analysis of data, procedures or business practices to locate information which can be used to create more efficient solutions.
Systems Engineering (waterfall) approach	A linear and sequential product or software development model that includes Conception, Initiation, Analysis, Design, Construction, Testing, Production/Implementation and Maintenance phases.
Third party	Organizations not affiliated with the Smart Columbus Program
Transportation Network Companies (TNCs)	Private businesses, non-profits, and quasi-governmental agencies that offer one or more types of transportation for use in exchange for payment
Trip data	Origin, destination, start time, end time, mode, transfer, transfer time, transfer location, disembarked location, embarked location.
Unbanked Users	Unbanked Users are those who pay for each transaction separately at the time of the trip request.
Unified parking availability and reservation system	One system that would allow parking availability information and reservations for parking lots and garages without concern for lot or garage ownership

Source: City of Columbus

Appendix I. Version History

Table 32: Version History

Version Number	Date	Author(s), Agency	Summary of Changes
0.1	10/5/2018	Andy Wolpert, City of Columbus, Alex Kavanagh and Jessica Baker, HNTB Corporation	Initial version for CoC review
0.2	10/22/2018	Andy Wolpert, City of Columbus, Alex Kavanagh and Robert James, HNTB Corporation	Draft version for USDOT review
0.3	12/11/2018	Andy Wolpert, City of Columbus, Alex Kavanagh and Robert James, HNTB Corporation	Revised draft version for CoC review
0.4	12/19/2018	Andy Wolpert, City of Columbus, Alex Kavanagh and Robert James, HNTB Corporation	Final version for USDOT

THE CITY OF
COLUMBUS
ANDREW J. GINTHER, MAYOR