Transit Contactless Open Payments:

Technical Solution for Pay As You Go (PAYG)

- ❖ Use Case 1: PAYG with Card
- ❖ Use Case 2: PAYG with Mobile Device

Transit Contactless Open Payments Working Committee

Version 2.0

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

About the Transit Contactless Open Payments Working Committee

The goal of the Transit Contactless Open Payments Working Committee is for all interested stakeholders to work collaboratively to identify possible technical solutions that address the challenges associated with the implementation of contactless open loop acceptance terminals at gated customer points of entry within the unique retail environment of the U.S. and Canadian public transit market.

Version History

Version 2.0, September 2018 – Use Case 2: Pay As You Go/Mobile incorporated

Version 1.0, September 2017 – Initial publication with Use Case 1: Pay As You Go/Card

The U.S. Payments Forum has used best efforts to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. The U.S. Payments Forum disclaims all warranties as to the accuracy, completeness or adequacy of information in this document. Comments or recommendations for edits or additions to this document should be submitted to: Transit-Open-Payments@uspaymentsforum.org.

Table of Contents

1. Introduction

1.1 U.S. Payments Forum Antitrust Compliance Statement

This paper was prepared in compliance with the U.S. Payments Forum Antitrust Compliance Statement, which is stated below:

U.S. Payments Forum activities and meetings of U.S. Payments Forum members and participants necessarily involve cooperation of industry competitors. Accordingly, it is the express policy of the Forum to require that all of its activities be conducted strictly in accordance with applicable antitrust laws. It is therefore extremely important that members and meeting attendees adhere to meeting agendas, comply with the Forum bylaws and Secure Technology Alliance Antitrust Guidelines, and, at all times, be aware of and not participate in any activities that are prohibited under applicable U.S. state, federal or foreign antitrust laws.

Examples of types of actions that are prohibited at Forum meetings and in connection with its activities are: price fixing, agreements to allocate customers or markets, boycotts and other "concerted refusals to deal," as well as discussion of or agreements regarding discriminatory pricing, discounts, incentives, awards, penalties, compliance and enforcement programs and other related matters. Any discussion of such activity is strictly prohibited.

Forum bylaws are available at: http://www.uspaymentsforum.org/wp-content/uploads/2012/08/US_Payments_Forum_Bylaws-FINAL-June-2016.pdf

Secure Technology Alliance Antitrust Guidelines are available at: https://www.securetechalliance.org/wp-content/uploads/Secure-Technology-Alliance-Antitrust-Policy-Jan-2017.pdf

1.2 Key Terms

These key terms are defined for purposes of their use in this paper, including those key terms which are defined for use only within other key terms only.

- Access form factor (or a credential): A card associated in the merchant system with a stored fare product (dollar value or a pass) that has been purchased in advance, and which can be used to gain entry through a Paid In Advance transaction. Such card could be credit, debit, or prepaid, including gift cards and electronic benefit transfer (EBT) cards.
- Active Wearable: A wearable that includes the same functionality described for passive wearables (see definition of passive wearable), plus another connectivity option – for example, Bluetooth or WiFi – and requires a battery. The secure element has a means to connect to the rest of the world through an interface other than the ISO/IEC 14443 contactless interface.[1]
- Application Transaction Counter (ATC): A counter, maintained by the chip card application (incremented by the chip), that provides a sequential reference to each transaction. Each

[1] Referenced from Secure Technology Alliance white paper: Implementation Considerations for Contactless Payment-Enabled Wearables, October 2017, https://www.securetechalliance.org/publications-implementation-considerations-for-contactless-payment-enabled-wearables/.

payment application has its own ATC.[2] A duplicate ATC, a decrease in ATC or a large jump in ATC values may indicate data copying or other fraud to the issuer.

- Card: For purposes of this paper, a form factor for a payment credential that is a chip-enabled plastic card issued by a financial institution which has an EMV® contactless interface and with which a Pay As You Go transaction can be made. Such card could be a credit, debit, prepaid, gift or benefit transfer (e.g., transit, EBT) card.
- Certificate Authority (CA): A trusted third-party entity that manages and issues security certificates and public keys that are used for secure communication in a public network. The CA is part of the public key infrastructure (PKI) along with the registration authority (RA) who verifies the information provided by a requester of a digital certificate. If the information is verified as correct, the certificate authority can then issue a certificate.[3]
- Consumer Device Cardholder Verification Method (CDCVM): A method that uses a consumer's mobile payment device (e.g., phone, wearable, card) to authenticate cardholder identity in a mobile payment transaction (e.g., PIN or biometrics).[4] Also known as On-Device Cardholder Verification Method or ODCVM.
- Deferred Authorization: An authorization request or financial request that occurs when a merchant captures transaction information while connectivity is interrupted; the merchant holds the transaction until connectivity is restored. After connectivity is restored, the merchant sends the transaction to make an online authorization request, and receives an authorization response from the issuer. A subset of "Delayed Authorization." For the purpose of this document, the term "deferred authorization" will be used to describe any tap-related transaction authorization sent after the transit customer has been allowed entry to travel.
- Delayed Authorization: An authorization request sent any time after the transit customer has been allowed entry to travel. Refer to definition of Deferred Authorization.
- Device PAN (DPAN): "DPAN" (Device Primary Account Number also known as the "Digital" Primary Account Number) is a mobile-device-specific identifier that is a tokenized version of the FPAN of the card provisioned to the payment-enabled device. The tokenization is based on the EMVCo Tokenization Framework.[5] The DPAN is then used in place of the FPAN to securely handle payment transactions.
- Digital Wallet: A software representation of a physical wallet. For example, putting debit and credit cards into an application that holds payment credentials through which someone can pay, using the digital version of the debit or credit cards in that person's physical wallet, linking to the same account, to pay.[6]
- Dual Message: Payment processing method where an authorization message is sent to perform a status check or hold funds for a given time period, followed by a financial message and match to the hold.

[2] Referenced from the "EMV Migration Forum: Communications & Education Working Committee Standardization of Terminology," Version 2.1, January 2014, http://www.emv-connection.com/standardization-of-terminology/.

[3] Referenced from techopedia.com: https://www.techopedia.com/definition/29742/certificate-authority-ca.

[4] Referenced from the U.S. Payments Forum Mobile and Contactless Payments Glossary, V1.0, September 2017, http://www.uspaymentsforum.org/mobile-and-contactless-payments-glossary/.

[5] EMV® Payment Tokenisation Specification – Technical Framework," Version 2.0, Sept. 8, 2017, https://www.emvco.com/emv-technologies/payment-tokenisation/.

[6] Same as footnote 4.

- EMV® Payment Token: A token used in lieu of a PAN which is based on the EMVCo Tokenization Framework standard.[7]
- Fixed fare: The cost of a ride is constant or flat.
- Funding PAN (FPAN): See the definition of PAN.
- Host Card Emulation (HCE): HCE is a mechanism for an application running on the "host" processor (the mobile device's main processor–where most consumer applications run) to perform NFC card emulation transactions with an external reader. Examples of HCE implementations include the Android operating system (Android KitKat 4.4 and higher) and the BlackBerry operating system.[8]
- Merchant Host: The backend (or back office) of the merchant's payment acceptance system.
- Mobile Device: For purposes of this paper, a form factor for a payment credential that is an NFC-payment-enabled mobile device or active wearable and with which a Pay As You Go transaction can be made. Such device will be payment-enabled through a payment credential that has been added to a digital wallet or application resident on the device.
- Mobile Payment Device: This term can be both broadly and specifically defined. The broad use could be a device that supports payment, including wearables, both with passive power or battery-powered sources. Specifically, most common examples include smartphones and tablets.[9]
- Mobile Payment: Mobile payment transaction in which a consumer uses a mobile device to pay for goods or services at a physical POS.[10] With a mobile proximity payment (which type is covered in this white paper), payment credentials are transmitted from the mobile device to the physical POS.
- Mobile Wallet: The mobile version of a digital wallet, provisioned and accessed on a mobile device.[11]
- Non-payment Token: A token that is not an EMV payment token.
- Open Payments (or Contactless Open Payments): For the purpose of this document, "Open Payment" will mean a purchase transaction made with a card or mobile device at a transit point-of-entry terminal.
- Paid In Advance Transaction: A fare purchased in a completed financial transaction at a terminal other than the transit point-of-entry terminal before entry (e.g., purchased at a kiosk or attended booth, via mobile app, or online).
- Passive Wearable: A wearable that includes a chip/secure element that has an operating system and payment app (one or more), is connected to an antenna, and has an ISO/IEC 14443 interface. Passive wearables are powered through the contactless interface. While the wearables device may have a battery to power other functions (e.g., Jawbone), it requires no battery to power payment functionality, operate the secure element, or provision the device with payment credentials. Passive wearables may be stickers, key fobs, rings, or other form factors.[12]

[7] Same as footnote 5 above.
[8] Same as footnote 4 above.
[9] Same as footnote 4 above.
[10] Same as footnote 1 above.
[11] Same as footnote 4 above.
[12] Same as footnote 1 above.

- Pay As You Go Transaction (PAYG): A single ride fare purchased by "tapping" at the transit point of entry with a card (as defined above) or other NFC-enabled form factor provisioned with a payment credential issued by a financial institution . The single ride fare may be fixed or variable.
- Payment Credential: Generally used within this document to refer to the electronic identification of a funding account, such as a credit, debit, prepaid, gift or benefit transfer card (e.g., transit, EBT) account issued by a financial institution, which identifier may reside in technology embedded on a plastic card (e.g., in the magnetic stripe or chip) or provisioned to a mobile device, via a mobile wallet or other application, in order to enable the device to be used to make payments.
- Payment Account Reference (PAR): A non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to its affiliated payment tokens.[13] This 29-character identification number can be used in place of sensitive consumer identification fields, and transmitted across the payments ecosystem.[14]
- Payment-enabled Wearable: See definition of "Wearable."
- Primary Account Number (PAN): The 8 to 19-digit number that appears on the primary account holder's physical payment card. Often, the PAN is also simply called the account number. If the account has a secondary account holder, the secondary user's payment card may have a different account number, or both users' cards may use the same account number, depending on the card issuer's policy.[15]
- Provisioning: An initial set-up process that handles authentication of a user account, the exchange of keys to unlock the NFC chip installed on a mobile device, the service activation and the secure download of mobile payment account information.[16]
- Secure Element or SE: The secure element resides in a microcontroller chip capable of performing cryptographic operations. It offers a dynamic environment to store data securely, process data securely and perform communication with external entities securely. If tampered with, it may self-destruct, but will not allow unauthorized access.[17]
- Single Message: Payment processing method that uses a single message to authorize a transaction and immediately debit the cardholder's account. No batch processing is involved.
- Token: Generic term for a placeholder or surrogate. In the context of payment card transactions, a token refers to a surrogate card number that is submitted in the payment stream in place of the real card number.[18]
- Tokenization: Process by which a placeholder or surrogate (payment token) is substituted for a primary account number. Typically, tokenization is a service offered by a payment network, acquirer, token service provider or third-party service provider.[19]

[13] Same as footnote 4 above.

[14] Referenced from: "Payment Account Reference (PAR) Overview", Chandra Srivastava, Visa at the Smart Card Alliance Payments Summit, April 6, 2016.

[15] https://www.investopedia.com/terms/p/primary-account-number-pan.asp

[16] Same as footnote 4 above.

[17] Same as footnote 4 above.

[18] Same as footnote 4 above.

[19] Referenced from U.S. Payments Forum white paper: Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud, http://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/.

- Token Requestor: Entity that initiates requests that PANs be tokenized by submitting token requests to the token service provider.[20]
- Token Service Provider (TSP): Entity within the payments ecosystem that provides registered token requestors with 'surrogate' PAN values, otherwise known as payment tokens by managing the operation and maintenance of the token vault, deployment of security measures and controls, and registration process of allowed token requestors.[21]
- Transit Point of Entry: Generally, used within this document to refer to a fare gate with a barrier (for entry and/or exit), a bus entry either next to an operator or at a rear door, a train platform device or other space within the transit area through which a customer will need to pass to access and/or pay for the travel service. For the purpose of this document with respect to any discussion of Transit Use Case 1, however, "transit point of entry" shall be used to refer specifically to only an unattended contactless-only fare gate or bus entry used to control access in/out of the transit network (which network may include trams and ferries).
- Transit Point-of-Entry Terminal (Transit POE Terminal, Transit POE or POE): For the purpose of this document, a contactless-only (i.e., no contact or magnetic stripe acceptance) point-of-sale terminal placed at a transit point of entry and, in some cases, integrated with the entry-point barrier (e.g., a terminal at a turnstile or at a bus entry).
- Transit Use Case 1: A specific retail scenario defined in this paper in Section 3.
- Transit Use Case 2: A specific retail scenario defined in this paper in Section 6.
- Trusted Execution Environment (TEE): An execution environment that runs alongside the mobile device or wearable operating system (the rich OS). A TEE provides security services and isolates access to its hardware and software security resources from the rich OS and associated applications.[22]
- Variable fare: The cost of a ride is contingent on time of day, distance travelled and/or other factor.
- Wearable [Device]: A wearable device or "wearable" is defined as a small electronic device that is worn or easily carried, incorporates one or more technology-related functions, and supports contactless transactions using technology that complies with ISO/IEC 14443. Wearables are implemented with two types of hardware technologies: passive or active. Wearables may support open payment (e.g., credit and debit card payment) or closed payment (e.g., transit, event) systems. Examples of wearable devices include: watches, rings, bracelets/wristbands, clothing, key fobs, and stickers/micro-tags. A mobile phone that has payment functionality is not considered a wearable in this document.[23]

1.3 General Background

This paper is a deliverable of the Transit Contactless Open Payments Working Committee (TWC). The goal of the Transit Contactless Open Payments Working Committee is for interested stakeholders to work collaboratively to identify possible solutions that address the challenges associated with the implementation of contactless acceptance terminals at gated customer points of entry within the unique retail environment of the U.S. and Canadian public transit market.

[20] Same as footnote 4 above.

[21] Same as footnote 4 above.

[22] Same as footnote 4 above.

[23] Same as footnote 4 above.

The TWC is using a use case approach to identify specific scenarios and the challenges associated with those scenarios for transit merchants of contactless open payments acceptance in order to meet the following objectives of the TWC (as stated in the TWC Statement of Work):

- Create and/or identify potential technology- and payment network-agnostic solutions that meet stakeholder needs and preferences for POE contactless payment card acceptance, for both attended and unattended terminals, specific to the distinct features of the transit retail environment.
    - Viable solutions will need to address acceptance challenges for mobile and other form factors that are valid contactless payment credentials that can be resolved through technical implementations.
    - Viable solutions will need to encompass acceptance of prepaid and gift cards, electronic benefit cards and transit-issued cards, along with credit and debit cards.
    - Areas that require a business solution(s) and best practices for resolving those business issues may be identified but will be out of scope for resolution as Working Committee activities.
- Understand each stakeholder group's business needs and preferences for contactless payments acceptance at transit POEs.
- Understand the potential impact of identified solutions on each stakeholder group, including customers.

The TWC first identified several possible transit scenarios, considering variations in fare types and payment technologies, shown in Table 1.

Table 1. Potential Transit Scenarios to Address

TRANSIT FARE SCENARIOS	• Pay-As-You-Go/Single Ride Fare • Paid-In-Advance • Aggregated Pay-As-You-Go • Post-ride Customer Service
PAYMENT TECHNOLOGIES SCENARIOS	• Plastic Cards • Prepaid, including Transit Benefit Cards, EBT • Mobile Devices • Wearables • Tokenization, PAR, F-PAN to D-PAN • EMV Debit Implementation

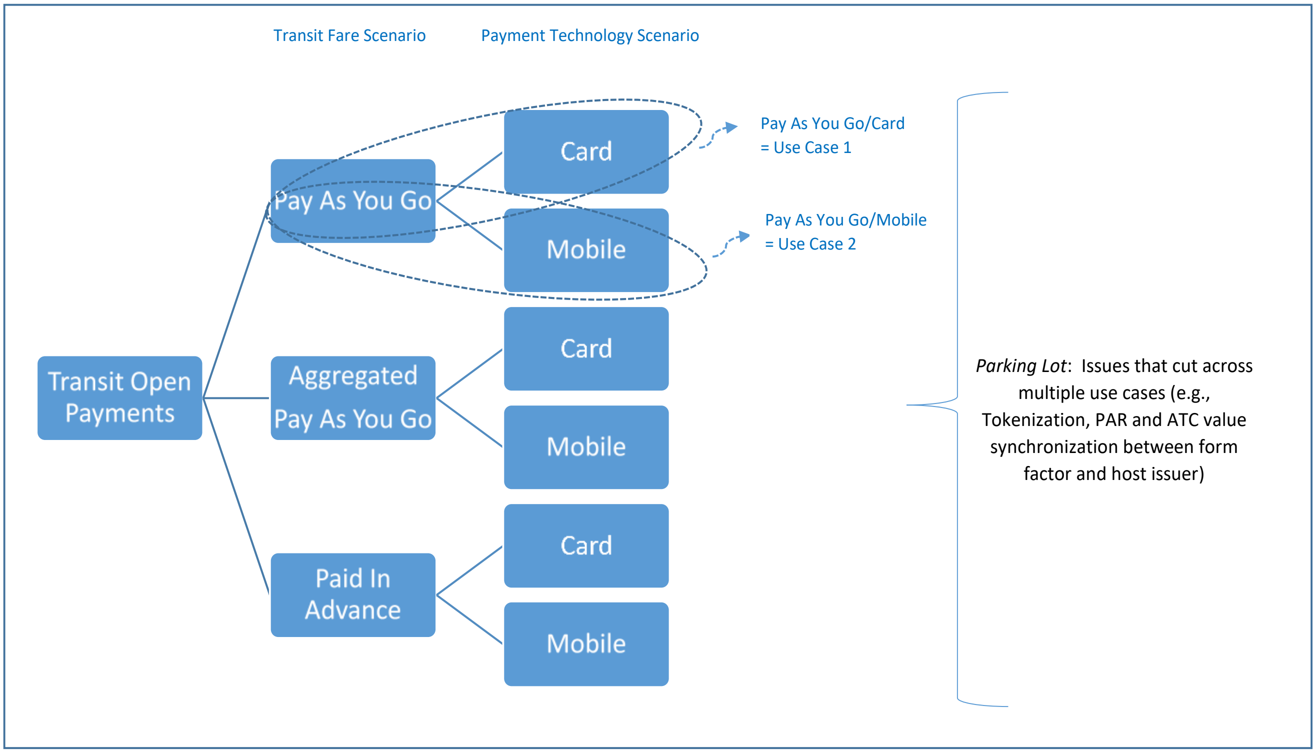
The TWC also captured items in a "parking lot" that were challenges that cut across multiple scenarios. These items, such as tokenized primary account number with deferred authorization and card positioning (*when multiple contactless cards are in physical wallet, and the card closest to reader is read)*, may turn into individual use cases later or be addressed with one or more of the scenarios in Table 1.

The TWC discussed the various identified scenarios, and initially proceeded with "Pay As You Go/Card" as Use Case 1. This scenario, further discussed in Section 3, was selected primarily because it was a relatively simple scenario that would also result in solutions that would be the foundation for other scenarios.

The TWC Co-Chairs designated a Technical Work Group to address the stated objectives for Use Case 1. The Technical Work Group was comprised of technical experts, including representatives from American Express, Discover, Mastercard, Visa, FIS Global on behalf of the U.S. debit networks, Interac, transit merchants, and payments consultants.

Upon completion of the Use Case 1 technical solution paper,[24] the TWC identified a framework to use to identify future use cases for the committee to address. Figure 1 shows the framework that the TWC is using going forward to select use cases to address.

Figure 1. TWC Framework for Use Case Structure


Transit Fare Scenario
Payment Technology Scenario
Transit Open Payments
Pay As You Go
Aggregated Pay As You Go
Paid In Advance
Card
Mobile
Card
Mobile
Card
Mobile
Pay As You Go/Card = Use Case 1
Pay As You Go/Mobile = Use Case 2
Parking Lot: Issues that cut across multiple use cases (e.g., Tokenization, PAR and ATC value synchronization between form factor and host issuer)

The TWC decided based on the framework shown in Figure 1 to then continue work on technical solutions for the use cases associated with Pay As You Go fare transactions. Pay As You Go/Mobile, with active wearables included, became Use Case 2 and has now been incorporated into the original Pay As You Go technical solution paper. Aggregated Pay As You Go transactions will be the next use case in this particular series, which the TWC expects to incorporate in the paper in the near future.

[24] http://www.uspaymentsforum.org/technical-solution-for-transit-contactless-open-payments-use-case-1-pay-as-you-gocard/.

The solutions presented in this paper cover the global networks and the domestic U.S. and Canadian debit networks. The following should be noted:

- JCB expects to follow Discover requirements for JCB transactions acquired in the U.S. via Discover, and expects to follow American Express requirements in Canada.
- UnionPay expects to follow Discover requirements where its transactions use Discover rails.
- Debit Network Alliance (DNA) expects to have a contactless solution that each of the debit networks can use, in addition to cards enabled with the U.S. Common Debit AID.

1.4 Purpose

The scope for this paper is to identify and provide guidance for technological solutions that could be used in the transit environment to implement acceptance of contactless open payments for Pay As You Go transactions under Use Case 1 and Use Case 2 as described in Sections 3 and 4.

Business risks and challenges, such as the following, are out of scope: network or other payment industry business rules, terms or similar matters; pricing, fares, penalties, discounts, and related policies and matters, including but not limited to incentives for cardholders to more rapidly adapt to usage of contactless open payments; and any allocation or sharing of risk, liability, payments or similar matters.

Additional use cases shown in Figure 1 are expected to be addressed by the TWC in further iterations of this paper and/or additional white papers.

2. Background on the Transit Environment

2.1 Overview

At points of entry, legacy fare payment systems present minor risk to transit merchants. Fare transactions at transit points of entry are typically based on fares purchased in advance and the required presentment of a transit-issued closed loop stored value magnetic-stripe or chip card, paper ticket with bar code or magnetic stripe, or physical token or exact change at a point of entry. The customer must complete a financial transaction to obtain the required fare media at a terminal located other than the point of entry (e.g., kiosk, attended booth, via mobile app or online). Thus, today's point of entry transactions are relatively low risk to the transit merchant since authentication and payment are already confirmed with the purchase of fare media before the customer uses fare media to gain entry. It should be noted, however, that such purchase transactions are subject to being charged back after the fare media is used to gain entry. Many transit agencies that issue electronic fare media can also quickly shut down a transit card should, for example, there be value remaining on a card after a fraudulent purchase.

Transit is looking to deploy retail-like "open payment" systems. This provides the potential for *financial* transactions to move:

- FROM being made in advance and away from the entry point (e.g., at vending machines)
- TO being made at the entry point when the customer is ready to travel

A customer no longer has to use his/her own payment form factor to first obtain transit-issued fare media for entry; s/he can use his/her own form factor at the entry point. However, authentication and payment may not be as certain for the transit merchant as it is with, for example, a purchased ticket.

Through discussion of the applicable transit use cases, the objective is to understand and identify the technological changes needed in the payments ecosystem for open payments and contactless EMV chip cards to be a viable option to supplant or supplement the transit closed loop system.

2.2 Unique Aspects of the Transit Environment

The transit retail environment has several distinct features:

- **Contactless-only terminals are at transit points of entry**. Given current processing speed capabilities and rider safety concerns, it will not be feasible to accept magnetic-stripe or contact EMV payments at the transit point of entry. The transit rider must have an EMV-based[25] contactless payment card to tap in order to be able to enter for a ride.
- **Point-of-entry terminals are not always online**. Given their use in a subway environment (which may be wired and/or wireless) and/or on board a bus (which is only wireless), payment terminals may lose connectivity to the merchant host periodically (i.e., be offline).
- **Point-of-entry terminal must have capability to be able to process 100% of the time.** Regardless of the online/offline availability of the terminal, the terminal needs to be able to transact in order to ensure a consistent customer experience.

[25] Magnetic stripe data (MSD) contactless cards are still in the market today and accepted at transit non-EMV terminals configured/deployed to process non-EMV contactless transactions. However, MSD functionality is not addressed in this paper, since both the definition of the use case and the approach to developing the solution are EMV-based.

- **No cardholder verification is possible at the point-of-entry terminal**. There is no terminal ability to capture a PIN or signature at the transit point of entry (unattended, low value payment). The only EMV cardholder verification method (CVM) available on the transit POE for a card is "No CVM."
- **No real-time authorization response is possible at the point-of-entry terminal prior to go/no customer prompt**. There is no ability to perform consistent real-time online authorization as currently defined in networks' operating rules within a sub-second timeframe needed to provide safe, consistent, passenger flow through the transit point of entry.
- **Transaction amount at the point-of-entry terminal is unknown due to variable fare.** The fare applicable to the transit rider may not be known at the time of the tap and could have a dollar value that varies with location, time of day, or other factors, or have no dollar value such as if associated with a pass purchased in advance or a free transfer.
- **Ability for transit merchant to "hot list" a card quickly is critical in preventing recurring fraud.** The ability to block a card so that it will be declined at every transit POE is critical in preventing use of a fraudulent card or fraudulent use of a payment card once it is known there was or could be fraud perpetrated with a tap.
- **Transactions are predominantly low value (e.g., single fare ride).** With open payments, the transit rider initiates payment for a single ride and gains entry using a single tap of his/her card. Acceptance of cards at transit points of entry is expected to increase the number of single ride purchases in the merchant system and on cardholders' cards.
- **Transit is a public service**. As a public service, transit agencies cannot require payment devices for fare payment that would serve to limit access to transit. Transit has to provide a contactless card both for customers who do not have a card that can be used at a transit POE and for customers who prefer not to use their own card.

3. Description of Use Case 1: Pay As You Go / Card

This section describes the Use Case 1 scenario that the Work Group was tasked with addressing through technical solutions, and the risks and challenges that arise from this scenario as seen from the transit merchant perspective.

3.1 Definition

The customer taps a card at the POE to pay for a single ride through a Pay As You Go transaction and gain access to the subway or bus. The customer taps in only. The customer must receive a go/no go type prompt within a sub-second.

3.2 Transit Merchant Use Case 1 Requirements

The unique features of the transit environment as described in Section 2 create risks for the transit merchant under Use Case 1. For example, it was noted that: (i) the POE cannot wait for the issuer authorization response prior to signaling the entry decision to the customer; (ii) the terminal could be offline and not able to conduct online authentication, let alone online authorization; and (iii) the POE will not be able to support CVM processing. All of these conditions increase counterfeit risk and/or card lost/stolen risk for the merchant. Additionally, receipt of the online authorization response after a customer has been allowed entry creates a new type of financial risk for transit agencies moving to open payments – "first tap risk" or the risk of a decline response and not collecting fare payment for a ride that's been taken already. Generally, with open payments, there could be a higher probability of wrongly-allowed customer entries and wrongly-denied entries, opening up the merchant to not only financial risks, but also the risks of poor quality customer experience.

In order to address the risks of Use Case 1, the requirements for a card to be securely processed at a transit POE within the scope of the Use Case 1 scenario from the transit merchant perspective are listed in Table *2*.

Table 2. Transit Merchant Requirements for Transit Open Payments Use Case 1

Index #	Requirement
M1	Solution must be able to validate that cards presented are genuine.
M2	Solution must support acceptance/processing of a card with 'No CVM' transaction only. There is no fallback to magnetic stripe or other CVMs possible.
M3	Solution must support processing of transaction when price is unknown at time of entry.
M4	Solution must support POE provision of *go/no go* customer entry prompt within a sub-second (typically no more than 500 milliseconds) of valid customer tap.
M5	POE should not need to connect to merchant host to make the *go/no go* entry decision for customer. All necessary decisions should be available locally at the terminal.
M6	Solution provides for secure transactions meeting EMV standards for authentication and online authorization of chip transactions.
M7	Solution must support merchant ability to identify transaction as PAYG or as Paid-In-Advance before an authorization request is sent.
M8	Solution supports acceptance of all validly issued cards that meet transit requirements (e.g., meet M1 requirement).

Index #	Requirement
M9	Solution is payment card agnostic.
M10	Solution does not limit ability to provide effective customer messaging (e.g., what is shown to customer when a tap is approved or declined) at POE.
M11	Solution must be cost effective to deploy – minimized cost of deployment at POE and merchant host, minimal to no deviation from payment networks' contactless related standards, minimal to no terminal kernel changes for implementing this use case.
M12	Solution preserves standard U.S. EMV routing choices through use of U.S. Common Debit AID.
M13	Solution must be future proofed; it should allow support for possible future changes in the solution parameters to support additional use cases and, to the extent possible, for possible future changes in the authentication and/or authorization processes.

3.3 Acquirer/Processor Transit Use Case 1 Requirements

The requirements for a card to be securely processed at a transit POE within the Use Case 1 scenario from the acquirer/processor perspective are listed in Table 3.

Table 3. Acquirer/Processor Requirements for Transit Open Payments Use Case 1

Index #	Requirement
A1	Able to identify and handle transactions when amount is unknown for PAYG transactions, meeting network transit message requirements and rules.
A2	Solution must support acquirer/processor processing of deferred EMV authorization requests from transit merchant.
A3	Solution does not directly impede processing ability to handle large volumes of authorization requests from transit merchant.
A4	Solution must support single message and dual message, according to network requirement.
A5	Solution must preserve standard U.S. EMV routing choices through use of U.S. Common Debit AID.
A6	Solution supports processing of authorization and clearing messages (dual or single message transactions), for all EMV contactless-enabled cards that support the solution.
A7	POE used by transit merchants is EMV and/or payment network Level 1 and 2 certified.
A8	Solution must not add unnecessary complexity to the existing transit merchant end-to-end transaction certification process with payment networks (Level 3 certification).
A9	Support robust network for Certificate Authority public key life cycle management and loading keys into/removing keys from the transit POE.
A10	Solution must support ability to pass on the business reason for negative authorization responses to the transit merchant, to the extent provided by issuer or acquirer, without converting all to "issuer decline."

Index #	Requirement
A11	Solution must support ability for processor to submit reversals or repeat authorizations for PAYG transactions for transit merchants.

3.4 Issuer Transit Use Case 1 Requirements

The requirements for a contactless EMV card to be securely processed at a transit POE within the Use Case 1 scenario from the issuer perspective are listed in Table 4.

Table 4. Issuer Requirements for Transit Open Payments Use Case 1

Index #	Requirement
I1	Able to identify and handle transactions when final amount is unknown for PAYG transactions, i.e., when the amount authorized is not necessarily the final amount settled, meeting network transit message requirements and rules.
I2	Solution does not impede issuer ability to handle large volumes of authorizations from transit merchant.
I3	Able to issue cards according to network guidelines while fulfilling proposed solution.
I4	Solution enables issuer to manage post-authorization customer-service-driven authorizations and reversals associated with original authorization request. May be transit merchant-initiated or cardholder-initiated via in-app or e-commerce channel.

4. Technical Functional Proposal for Use Case 1

4.1 Approach to Developing the Solution

Given the transit POE's inability to rely on real-time, online issuer authorizations to address counterfeit and credit risk, the approach would ideally afford Transit the same or better protections as provided by real-time online authorizations assuming a prescribed set of offline risk practices are performed and satisfied. The approach to developing the Use Case 1 solution, therefore, was to consider the key factors required to ensuring a secure transaction.

4.2 Three Pillars to a Secure Transaction: Card Authentication, Cardholder Verification, Financial Authorization

Card Authentication. Card authentication is performed in an EMV-based process to prevent counterfeit fraud. The authentication process validates that the card being used in the transaction is genuine and was issued by the issuer. The authentication process may be supplemented by the merchant's list management process based on the merchant's deny list and the payment networks' negative files.

Cardholder Verification. Cardholder verification is performed in an EMV-based process to ensure that the cardholder is genuine and that the card has not been lost or stolen.[26]

Financial Authorization. Financial authorization is performed in an EMV-based process in order to ensure funding is available in the cardholder's account.

4.3 Step 1: Card Authentication

4.3.1 Online and Offline Authentication

There are two ways to ensure the card is genuine and not a clone or fake: online and offline authentication.

With online authentication, the issuer host verifies a cryptogram generated by the card, ensuring the card is legitimate due to the fact of using the same secret payment key present on the card and known to the issuer host. The challenge for Transit with this form of card authentication is that the data must reach the issuer host for validation.

Using Offline Data Authentication (ODA) technology, which allows the terminal (instead of the issuer host) to validate the card being used for payment is genuine and not counterfeit, is one of the key attributes that contactless EMV offers the transit agencies. Figure 2 shows the difference between card authentication with and without ODA support (both illustrations assume "No CVM" as the cardholder verification method).

[26] As indicated in Section 2.2, no cardholder verification is possible at the point-of-entry terminal and No CVM is the only possible CVM that can be processed.

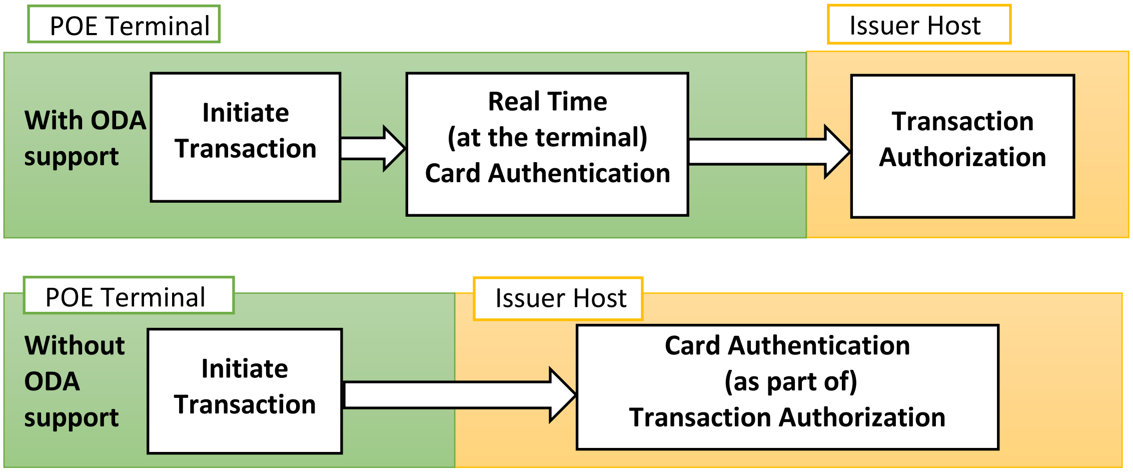

POE Terminal
Issuer Host
With ODA support
Initiate Transaction
Real Time (at the terminal) Card Authentication
Transaction Authorization
POE Terminal
Issuer Host
Without ODA support
Initiate Transaction
Card Authentication (as part of) Transaction Authorization

Figure 2. Card Authentication with and without ODA Support

ODA allows the POE to determine the card's authenticity by rigorously validating unique card and transaction information in a secure manner. Most notably, ODA protects against cloned cards and wedge attacks, which provides the extra protections needed for the transit merchant, issuer, and acquirer in a transit open payment environment.

ODA uses a cryptographic algorithm called RSA, which is based on asymmetric cryptography (PKI – Public Key Infrastructure) and is supported by the EMVCo specifications. Successful authentication at the POE does not mean the account is in good standing, or that an authorization will be approved. It just means that the card has passed the offline security checks and is determined to be an authentic card.

If a card fails an ODA authentication check, it will be because:

- The card is expired or in some way damaged, preventing security checks from taking place; or
- The card is fraudulent, e.g., cloned; or
- The card terminal has not been set up correctly; e.g., Certificate Authority Public Keys (CAPKs) may not be loaded properly into the terminal.

In such cases as these, the transaction will terminate at the terminal and the customer is denied entry at the POE unless the customer utilizes another fare payment method.

4.3.2 Types of Offline Authentication

There are three types of ODA:

i. Static Data Authentication (SDA) – The entry level of ODA in EMV. SDA is no longer accepted as an industry standard. This only protects against counterfeit and not skimming, and cards using SDA can be copied and reused.

ii. Dynamic Data Authentication (DDA) – Used for EMV and in some contactless implementations (where it is termed 'fDDA' for "fast" DDA) to protect against counterfeit and skimming. Each transaction is unique and the digital signature cannot be reused.

iii. Combined DDA and Application Cryptogram Generation (CDA) – Used for EMV and contactless implementations to protect against counterfeit, skimming and man-in-the-middle attacks (between the card and the terminal).

4.3.3 Differences between Credit and Debit Card Authentication

For the transit POE terminal to perform dynamic ODA, the card application selected at the time of tap at the POE has to support dynamic ODA. The AID of the application selected may support a variation of the ODA functionality as defined by the payment network providing the AID.

Credit: Typically, credit cards have only one AID – payment application.

Debit: Typically, debit cards offer two AIDs, one to support transactions within the country and another to support global payment networks.

U.S. Debit Implementation

The Transit POE terminal may select either the global AID or the U.S. Common AID, which can be routed to any payment network associated with the card as long as the AID selected provides the necessary functionality to facilitate ODA.

Canada Debit Implementation

For Canadian domestic POS acceptance, the Canada Application Selection Flag (ASF) in debit cards today typically points to the Interac AID. In this case, the Interac Corporation network is to provide the means of ODA as defined in the Interac Flash contactless specifications.

4.3.4 Solution

In the transit environment, where connectivity is an issue, and if there is deferred authorization, ODA becomes a critical first step in risk mitigation. Without ODA, there's minimal ability to detect counterfeit cards. Transit agencies cannot effectively manage access to the transit network or limit their financial exposure if they cannot be assured of a card's authenticity each time the card is used at the POE terminal that is offline.

CDA and fDDA are the ideal options to be used for contactless open loop payments as they provide the highest level of protection for authenticating the card at the POE terminal.[27]

4.3.5 Stakeholder Impact

The North American market is online only with zero floor limits and has not historically required offline data authentication (or offline authorization) for bank-issued payment cards. Some issuers, however, have chosen to issue DDA/CDA-capable cards. Enabling ODA capability is critical to ensuring security at the transit POE terminal and the integrity of the payment process.

How each network or issuer or acquirer or any other party chooses to support ODA is beyond the scope of this document. However, each payment network has a position regarding supporting, recommending and requiring ODA for their issuers. Table 5 provides the current position of each payment network (as of the publication date of this paper) regarding ODA enablement on cards and mobile devices for use in transit open payments acceptance in North America.[28]

[27] An issuer will perform online authentication of the Authorization Request Cryptogram (ARQC) cryptogram regardless of use of ODA, as required by all networks.

[28] Networks' ODA positions regarding use in other market verticals in North America are not addressed in this paper. Entities interested in ODA support for other market verticals would need to check with the networks.

Table 5. ODA Position by Payment Network for Transit Open Payments*

Network: Position:	American Express	Discover	DNA[29] Debit Networks[30]	Interac	Mastercard	Visa
Type	CDA	CDA	CDA	CDA	CDA	fDDA
Supported	Yes	Yes	Yes	Yes	Yes	Yes
Recommended	Yes	Yes	Yes	Yes	Yes	Yes
Required	Yes	Yes	No	Yes	Yes	No
ODA Support for U.S. Common AID	N/A	Yes	N/A*	N/A	Yes	No**

* Issuers utilizing specifications from any of the payment networks listed in this table would need to check with those networks for the corresponding support for ODA on the U.S. Common Debit AID regarding details about support rollout.

** Technically possible, however, the Visa U.S. Common Debit profile is not currently personalized for ODA. A separate contactless certificate must be created and CA root keys specific to the U.S. Common Debit AID would need to be provided to the transit POE terminals.

There are impacts from utilization of authentication at the POE on various stakeholders. A few examples follow:

Merchant: Implement ODA at the POE.

Issuer: Authentication at the POE involves personalizing the card with public key certificates as supported by each of the payment networks, and managing their related lifecycles. Depending on whether the issuer already supports ODA, this may add to the issuer's cost and complexity to support ODA functionality. An issuer who decides to issue contactless EMV cards with a network that does not mandate ODA, has a business choice to make as to whether the issuer wants their cards to be accepted at transit POEs or not.

Acquirer: The acquirer must perform the provisioning and lifecycle management of each payment network's public key certificates into their transit merchant clients' terminals. This includes the additional terminal testing and certification involved to demonstrate support for offline contactless acceptance.

4.4 Step 2: Cardholder Verification

Each of the payment networks has established transaction amounts, which may vary by Merchant Category Code (MCC), above which cardholder verification must take place (either using signature, PIN or biometric) in order to protect merchants from lost/stolen chargebacks. If a transaction is below this threshold, then no cardholder verification is required. For transactions above this threshold amount, then CVM processing is required and performed based on what the card and terminal both support.

[29] Debit Network Alliance.

[30] Response for debit networks relates to proprietary cards. Check with debit networks using the U.S. Common Debit AID regarding their individual policies.

Table 6 describes various CVM options applicable to cards supported by EMV; the CVM option relevant to contactless open payments is discussed later in this section. For Use Case 1, other CVM options such as Consumer Device CVM (CDCVM) on mobile devices and biometric verification are not applicable.

Table 6. CVM Options Specific to Cards

CVM	Description
Online PIN[31]	The PIN Pad prompts the cardholder for a PIN and encrypts it using the same key used for magnetic stripe debit PIN encryption. The encrypted PIN block is sent to the issuer host in the online authorization message. Note: PIN can only be performed in a Payment Card Industry (PCI) PIN Transaction Security (PTS)-approved terminal.
Signature	This method operates in the same manner as in the magnetic-stripe environment. The cardholder signs the transaction receipt and the merchant compares this signature to the signature on the card. All stakeholders should note that since April 2018, signature capture is now optional pursuant to rule changes across all global payment networks and no longer a requirement for all EMV contactless chip-enabled merchants. For debit networks, whether the signature is optional depends on the network.
No CVM	This method operates in the same manner as in the magnetic-stripe environment where transaction authorization is independent of cardholder verification. No cardholder verification is usually supported in merchant environments, such as certain unattended low-value transaction environments (e.g., vending machines), quick service restaurants and other small ticket environments.

4.4.1 Differences between Credit and Debit Cardholder Verification

There is little to no difference between debit and credit transaction processing from the cardholder verification perspective, although the specific No CVM technique used may differ across payment networks.

4.4.2 Solution

The purchase amount associated with an individual Pay As You Go transaction is expected to be lower than any of the transaction amount thresholds (or CVM floor limits) that most payment networks have established before requiring cardholder verification of some type. This low-value transaction, coupled with the POE's inability to perform cardholder verification, means the only acceptable CVM is No CVM.[32]

[31] Offline PIN may be a CVM option in Canada and on international cards. This method is widely used in Canada and outside North America. However, Offline PIN cannot be used with the contactless interface of a card.

[32] While not in the scope of Use Case 1, the mobile form factor may involve its own verification separate from what the POE requests, and does not involve interaction with the terminal.

4.4.3 Stakeholder Impact

The support for No CVM is fairly standard on most card types and supported in all terminal configurations; therefore, its use at POE terminals is not anticipated to impact the stakeholders, including issuers, networks, acquirers, cardholders, or customer service.

How each network or issuer or acquirer or any other party chooses to support No CVM is beyond the scope of this document. However, each payment network has a position regarding supporting, recommending and requiring No CVM for their issuers. Table 7 provides the current position of each payment network (as of the publication date of this paper) regarding "No CVM" as a verification method for use in transit open payments acceptance in North America.[33]

Table 7. No CVM Position by Payment Network for Transit Open Payments

Network: Position:	American Express	Discover	Debit Networks[34]	Interac	Mastercard	Visa
Supported	Yes	Yes	Yes	Yes	Yes	Yes
Recommended	Yes	Yes	Yes	Yes	Yes	Yes
Required	Yes	Yes	Yes	Yes[35]	Yes	Yes

4.5 Step 3: Financial Authorization

As indicated earlier in this paper, one of the unique features of the transit retail environment is the need to ensure rider safety – i.e., a payment process that supports a smooth or uninterrupted flow of riders through gated points of entry minimizing queuing at these points of entry. Ensuring rider safety requires sub-second transactions as measured from the time of the customer's tap to the time the customer receives a go/no go prompt to ensure safety-based throughput speeds. At today's typical network communication rates, an online authorization of a card results in a transaction time that is far greater than that acceptable at gated points of entry for transit.

As a result, with a Pay As You Go transaction, it is expected that access to the transit service will have to be granted *before* funds can be secured with an online authorization. This is very different from traditional ticketing whereby payment assurance is obtained *before* any travel occurs.

Financial authorizations of contactless EMV transactions can be carried out offline to verify funding is available prior to the entry decision. However, the U.S. and Canada are online-only markets, with no offline solution available today in those markets. Moreover, even if offline capability were available, the Working Committee determined it would be difficult to utilize an offline authorization model while providing a good customer experience. Also, the U.S. Common Debit AID does not support offline authorization; it requires online authorization, further challenging an offline authorization solution. Lastly, an offline authorization solution is not expected to be deployed in the U.S. and Canada markets in the foreseeable future. As a result, the Working Committee did not further consider the offline-authorization-only option for Transit.

[33] Networks' "No CVM" positions regarding use in other market verticals in North America are not addressed in this paper. Entities interested in No CVM support for other market verticals would need to check with the networks.

[34] Each debit network determines the parameters for its own "No CVM" support.

[35] No CVM for Interac – A simple proprietary mechanism is used to ensure that no CVM is required for contactless payment within certain purchase amount limits.

4.5.1 Differences between Credit and Debit Authorization

Support for online authorization: None, as both credit and debit are typically online authorized in the U.S. and Canada markets.

Guarantee of payment to merchant: Prior to completion of online authorization, it may not be possible to guarantee merchant receipt of funds using credit or debit (unless other allowances are made for risk sharing).

Transaction routing and processing:

Credit Typically uses Dual Message System (DMS) network messages (authorization request message separate from clearing and settlement message).

1. Authorization Request Message:
    - To check account's "Open to Buy" position and to place a hold on funds
    - Doesn't actually charge the account
2. Clearing and Settlement Message:
    - Typically submitted in an offline batch file at end of merchant's processing day
    - Charges account for amount of settlement transaction, which typically (may be some exceptions) must be less than or equal to the approved authorization amount

Debit Can support single or dual message transaction processing, dependent on the payment network.

Pre-Authorizations: Used for credit and debit when final amount of transaction is not known at the time the payment form factor is presented to the payment terminal and a final authorization will occur when the fare is known. Since payment networks set their own rules, which may differ slightly from each other, stakeholders should always clarify with each network the applicable rules and amounts required or permitted for pre-authorizations.

Credit

- Used across multiple merchant types.
- Typically reserves funds up to the amount of the Pre-Authorization Request.
- May be some exceptions where final amount may be permitted to be a percentage over the pre-authorized amount.
- Funds reserved. Depending on the merchant type; funds may be reserved for days, weeks, or longer.
- Multiple transactions involving different merchants may be completed against the same account while a Pre-Authorization Request remains open.

Debit

- Used across multiple merchant types.
- Historically, may or may not place a hold on funds for the authorized amount.
- Typically, must be completed/settled within a payment-network-defined time period.

Funds can be, but may not be, reserved dependent on the pre-authorization message and payment network rules. Multiple transactions involving different merchants may be completed against the same account while a Pre-Authorization Request remains open.

Liability and Dispute Resolution: The purpose of this solution is to reduce counterfeit fraud and otherwise minimize merchant liability, while maintaining transaction speed throughput at the POE.

Liability and dispute resolution are handled based on payment network rules and are outside the scope of this document.

4.5.2 Solution

As described earlier, with a Pay As You Go transaction, a real-time authorization is not possible to obtain prior to when the entry decision for a customer has to be made. This type of transaction will require a deferred authorization process.

Deferred financial authorizations may occur at any time *after* a rider has been allowed to enter the transit service. This includes authorizations initiated at the time of entry, or when connectivity is restored after an interruption, or those performed a day or more later. In any event, a deferred authorization is deemed to have occurred whenever access to the transit network is provided *before* an online authorization request is received by the issuer.

Stakeholders should confer with the individual payment networks to determine the appropriate data element(s) to use to indicate the authorization request is a deferred authorization request being submitted under the network's rules.

4.5.3 Stakeholder Impact

How each network or issuer or acquirer or any other party chooses to support deferred financial authorizations is beyond the scope of this document. However, each payment network has a position regarding supporting, recommending and requiring deferred authorization for their issuers. Table 8 provides the current position of each payment network (as of the publication date of this paper) regarding deferred authorization for use in transit open payments acceptance in North America.[36]

Table 8. Deferred Financial Authorization Position by Payment Network for Transit Open Payments

Network: Position:	American Express	Discover	Debit Networks[37]	Interac	Mastercard	Visa
Supported	Yes	Yes	Yes	Yes	Yes	Yes
Recommended	Yes	Yes	No	Yes	Yes	Yes
Required	No	No	No	No	No	No

Merchant:

First Tap Risk: The biggest impact of deferred authorization on transit would be the new financial risk from non-assured payment. An authorization deferred for any reason exposes the transit merchant to financial risk given that the issuer may decline the transaction due to insufficient funds – the "first tap

[36] Networks' deferred financial authorization positions regarding use in other market verticals in North America are not addressed in this paper. Entities interested in deferred financial authorization support for other market verticals would need to check with the networks.

[37] Determined by the Registered Application Provider Identifier (or "RID") owner specifications and the operating rules for each debit network. Please see "Merchant Processing During Communications Disruptions," Version 1.0 - April 2016, EMV Migration Forum, http://www.emv-connection.com/merchant-processing-during-communications-disruption/.

risk" mentioned earlier – and therefore, funding is not assured even though the customer already received transit service.

In such event, the card account should be added to the transit merchant's deny list until funds received, or based on other criteria (e.g., expiry for listing on deny list). Depending on the amount of time required for the merchant to add the card account to its deny list, however, there could be *further* financial risk from additional taps of the card.

Bank Holds: Transit merchants that charge a fixed fare for transit can seek a deferred authorization for the full fare amount upon entry. This ensures only exact funding is requested, but still poses the risk of non-payment if the transaction is declined.

Agencies that charge a variable fare, perhaps time or distance-based, have another challenge since the amount to authorize for at the time of entry is unknown. Any authorization performed at the time of entry is simply a best estimate. If the merchant estimates too high, then it can adversely impact low-income riders by securing more funds than are needed (resulting in not enough money for the rider's other expenses), or it could trigger a decline due to low available funds. If the amount authorized is too low, then the merchant risks inadequate funding for the travel it already provided. For some payment networks, an alternative to estimating the authorization amount is to allow the merchant to perform an account status check instead.

An **Account Status Check** can be a $0 or $1 authorization sent to the issuer to identify if the account exists. While an approval isn't necessarily a guarantee of payment, the agency knows the issuer is continuing to allow the cardholder to transact. Depending on network rules, an "approved" status check can provide some degree of financial protection too. This occurs in the petroleum industry today, which also utilizes unattended terminals similar to transit.

Solutions to First Tap Risk and Bank Holds in Other Industries: Automated fuel-dispensers (AFD) perform authorizations for $1 not knowing how much fuel will be dispensed. If the status check is "approved," the gas station is protected up to $X amount, where X varies (and could be, for example, $50, or up to $100 today), based on payment network rules. This solution addressed the shared financial exposure between parties. A similar approach has been taken to reallocate first tap risk in the European transit market between global payment networks and the UK's Transport for London (TfL).

It should also be noted that AFD and POE devices differ; many AFD devices require zip code checks, although not in Canada, which reduce risk. This would not be feasible to duplicate at POEs.

Customer Messaging:

Issuers and transit merchants should be aware that different transaction amounts may be presented to the customer during the processing of a transit open payments transaction and should consider the process flow associated with transit open payment transactions and its effect on the presentment of values to the customer from an online banking app.

For networks that permit transit merchants to make a deferred authorization, the amount used to make a deferred authorization may be different from the fare charged to the customer after any post-ride adjustments are made by the transit merchant host upon settlement of the transaction. (Since payment networks set their own rules, which may differ slightly from each other and may involve differing authorization models, stakeholders should always clarify with each network the applicable rules and amounts.) This presents a potential customer experience issue given availability of real-time purchase transaction information to the customer, such as through online account access or online banking text alerts.

Amounts could differ for one of several reasons. Example scenarios include:

- The choice by the merchant to use a pre-selected authorization amount for all deferred authorizations that is not always equal to the exact fare that will be owed;
- The pre-selected authorization amount not being the same as the fare that is actually charged;
- Transaction processing timing when the transit merchant has not yet processed a prior transaction (from a prior tap) which would make the second tap a free ride due to the merchant's free transfer policy; and/or
- An authorization model that involves only an authorization for the actual amount to be settled under transit aggregation rules.

Such scenarios could potentially result in customer confusion since the customer may not recognize the amount in the notification or alert and/or not understand why the actual charge made to their account differs from the amount contained in an earlier notification or alert.

Providing a solution to mitigate this issue is outside the scope of this paper; however, issuers, payment networks and any other stakeholders in transit open payments should always consider the customer experience implications of any technical solutions and seek to deploy technical approaches that support clear messaging to transit customers.

Other impacts:

- POE terminal logic for estimated authorization and/or account status verification
- Deny list management
- Need to inform customers of impact on issuer holds ("open to buy") from card use at POE
- Customer service and passenger education

Issuer:

- Customer service and cardholder education
- Ability to handle out of sequence and deferred authorizations in terms of the Application Transaction Counter (ATC)

Issuers that validate the ATC in authorization messages should be aware that the use of deferred authorization might cause ATCs in authorization requests to arrive out of order. Out-of-sequence ATC values (especially from transit merchants) do not necessarily indicate fraud and issuers should take this into account in their authorization decisions.

Authorization request messages that are delayed in their transmission to the issuer due to communications outages or other factors can lead to the ATC value on file at the issuer host system being out of synchronization with the value provided in an authorization request message. Similarly, fare enforcement transactions may increment the ATC on the form factor, but the ATC may not be sent to the issuer. Issuers should review their ATC checking edits (where applicable) and update if/as necessary to accommodate this. Where ATC checking is performed at the issuer host, the issuer may want to expand the plus/minus range of acceptable ATC values in comparison to the value on file at the issuer host, and may wish to only increment the ATC value at the issuer host when the ATC value in the incoming authorization request or settlement message exceeds the value currently on file at the issuer host.

As detailed in payment network guidelines for transit merchant processing, the Amount, Authorized value used for cryptogram generation by the card, is likely to be different from the actual amount authorized used for the transaction due to the deferred authorization mechanisms employed by the transit industry. Issuers should use only data contained in Field 55 for cryptogram validation, and should not attempt to cross-check data that appears in Field 55 with data that appears in other fields of the authorization message (for example the Amount, Authorized contained in tag 9F02 in Field 55 against the amount in Field 4). Otherwise, the cryptogram may not validate and the authorization request may be declined when it should not be if all else is valid.

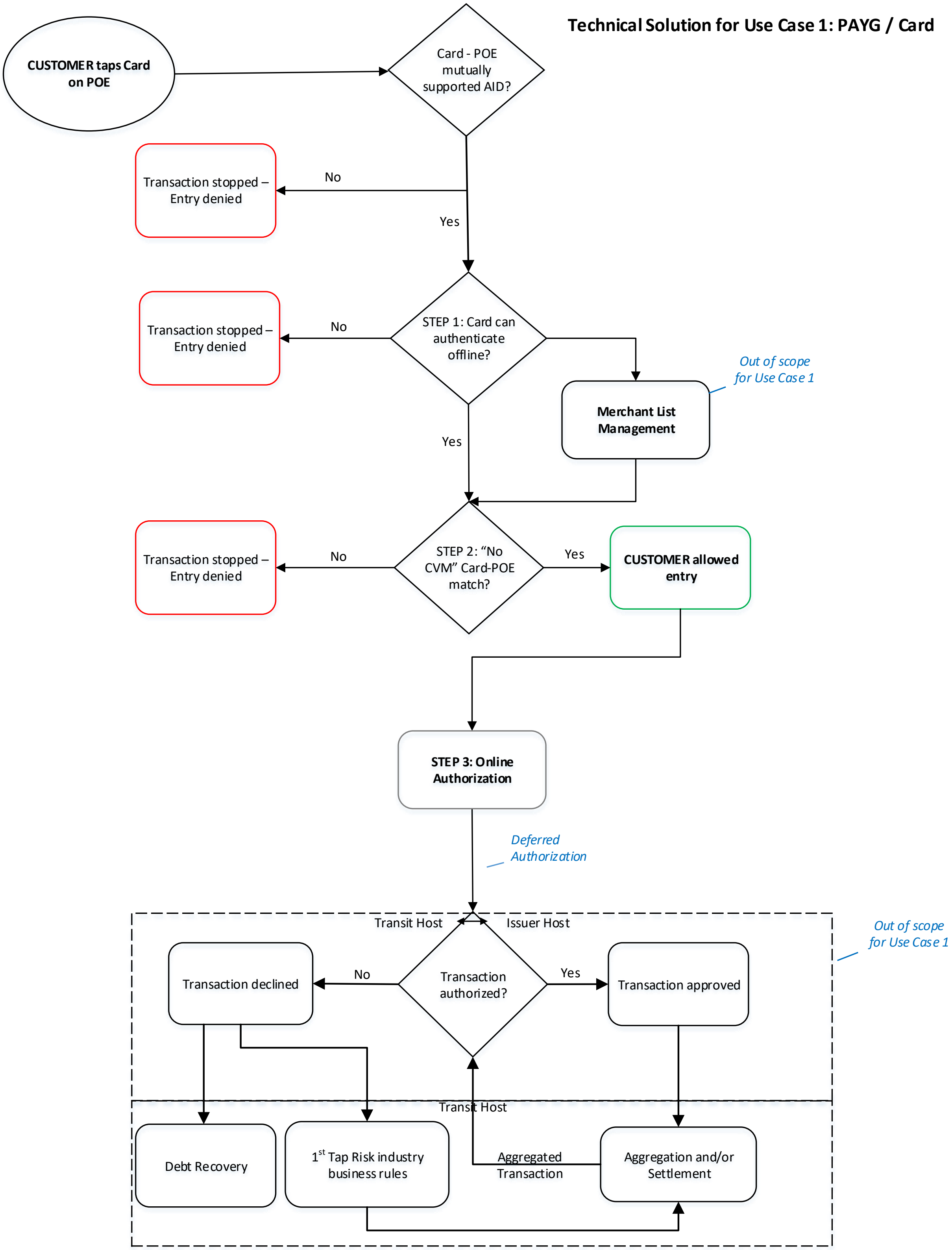
Network:

- Some networks: rule changes; no technical impact expected
- Other networks may require updates to permit end-of-day calculation of final amount(s) and clearing at that time and other special features of transit transaction processing

4.6 Transaction Flow Diagram

The transaction flow for a Pay As You Go transaction made with a card based on the solutions for the three pillars (i.e., Steps 1, 2 and 3) is depicted in the following diagram.

Technical Solution for Use Case 1: PAYG / Card


CUSTOMER taps Card on POE
Card - POE mutually supported AID?
No
Transaction stopped – Entry denied
Yes
STEP 1: Card can authenticate offline?
No
Transaction stopped – Entry denied
Merchant List Management
Out of scope for Use Case 1
Yes
STEP 2: "No CVM" Card-POE match?
No
Transaction stopped – Entry denied
Yes
CUSTOMER allowed entry
STEP 3: Online Authorization
Deferred Authorization
Transit Host
Issuer Host
Out of scope for Use Case 1
Transaction declined
No
Transaction authorized?
Yes
Transaction approved
Transit Host
Debt Recovery
1st Tap Risk industry business rules
Aggregated Transaction
Aggregation and/or Settlement

5. Use Case 1 Conclusion

The Pay As You Go/Card technical solution proposed in this paper delivers against the three pillars of a secure EMV transaction – card authentication, cardholder verification and financial authorization. Table 9 describes at a high level the three pillars of a secure EMV transaction that are covered in more detail as part of the document.

Table 9. Summary of Three Pillars of a Secure EMV Transaction as Described for the Use Case 1 Technical Solution

Secure EMV Transaction Pillar	Risk Prevented	Use Case 1 Technical Solution
Card authentication	Counterfeit fraud	• Dynamic ODA • Supplemented by merchant list management*
Cardholder verification	Lost/stolen fraud	• No CVM • Supplemented by network negative file updates • Supplemented by deny list management (using authorization response)
Financial authorization	Funding not available	• Deferred authorization

* ”Merchant list management” refers to lists of blocked cards maintained at the POE and transit merchant host.

All technical criteria outlined in this white paper – except where noted – are found in and addressed by the existing payment network contactless EMV specifications. Readers of this document are encouraged to visit the applicable payment network’s website or the EMVCo website for the most recent versions of contactless specifications. Contactless card issuers will need to consider the guidelines provided in this document when determining how cards are personalized if transit acceptance is a requirement of their portfolio.

Table 10 summarizes the stakeholder requirements listed in Table 2, Table 3 and Table 4, and indicates whether the proposed technical solution has addressed each requirement purely from a technological perspective. It is important to note that although a requirement is indicated as being addressed in Table 10, the table does not address business and risk decisions that stakeholders will need to make and which, as noted, are out of scope.

Table 10. Stakeholder Requirements for Transit Open Payments Use Case 1 Addressed/Not Addressed by Solution

Index #	Requirement	Addressed in Solution
	TRANSIT REQUIREMENTS	
M1	Solution must be able to validate that cards presented are genuine.	Yes
M2	Solution must support acceptance/processing of a contactless with 'No CVM' transaction only. There is no fallback to magnetic stripe or other CVMs possible.	Yes
M3	Solution must support processing of transaction when price is unknown at time of transaction.	Yes
M4	Solution must support POE provision of *go/no go* customer entry prompt within a sub-second (typically no more than 500 milliseconds) of valid customer tap.	Yes
M5	POE should not need to connect to merchant host to make the *go/no go* entry decision for customer. All necessary decisions should be available locally at the terminal.	Yes
M6	Solution provides secure transaction meeting EMV standards for authentication and authorization of chip transactions.	Yes
M7	Solution must support merchant ability to identify transaction as PAYG or as Paid-In-Advance through closed loop processing in merchant host backend before an authorization request is otherwise sent to the acquirer/processor.	Yes
M8	Solution supports acceptance of all validly issued cards that meet transit requirements (e.g., meet M1 requirement).	Yes
M9	Solution is payment card agnostic.	Yes
M10	Solution does not limit ability to provide effective customer messaging at POE.	Yes
M11	Solution must be cost effective to deploy – minimized cost of deployment at POE and merchant host, minimal to no deviation from payment networks' contactless related standards, minimal to no terminal kernel changes for implementing this use case.	Yes
M12	Solution preserves standard U.S. EMV routing choices through use of U.S. Common Debit AID.	Yes
M13	Solution must be future proofed; it should allow support for possible future changes in the solution parameters to support additional use cases and to extent possible, for possible future changes in the authentication and/or authorization processes.	Partially[38]
	ACQUIRER/PROCESSOR REQUIREMENTS	
A1	Able to identify and handle transactions when amount is unknown for PAYG transactions, meeting network transit message requirements and rules.	Yes

[38] This table only covers Use Case 1, which is the use case the solution addresses. Until all other use cases are completely defined, it cannot be determined if the solution as described in the document will support all possible future changes/requirements.

A2	Solution must support acquirer/processor processing of deferred EMV authorization requests from transit merchant.	Yes
A3	Solution does not directly impede processing ability to handle large volumes of authorization requests from transit merchant.	Yes
A4	Solution must support single message and dual message, according to network requirement.	Yes
A5	Solution must preserve standard U.S. EMV routing choices through use of U.S. Common Debit AID.	Yes
A6	Solution supports processing of authorization and clearing messages (dual or single message transactions), for all EMV contactless-enabled cards that support the solution	Yes
A7	POE used by transit merchants are EMV and/or payment network Level 1 and 2 certified.	Yes
A8	Solution must support a simple and streamlined transit merchant end-to-end transaction certification process with payment networks (Level 3 certification).	Yes
A9	Support robust network for Certificate Authority public key life cycle management and loading keys into/removing keys from transit POE.	Yes
A10	Solution must support ability to pass on the business reason for negative authorization responses to the transit merchant, to the extent provided by issuer, without converting all to “issuer decline.’’	Yes
A11	Solution must support ability for processor to submit reversals or repeat authorizations for PAYG transactions for transit merchants.	Yes
ISSUER REQUIREMENTS		
I1	Able to identify and handle transactions when final amount is unknown for PAYG transactions, i.e., when the amount authorized is not necessarily the final amount settled, meeting network transit message requirements and rules.	Yes
I2	Solution does not impede issuer ability to handle large volumes of authorizations from transit merchant.	Yes
I3	Able to issue cards according to network guidelines while fulfilling proposed solution.	Yes
I4	Solution enables issuer to manage post-authorization customer-service-driven authorizations and reversals associated with original authorization request. May be transit-merchant-initiated or cardholder-initiated via in-app or e-commerce channel.	Partially[39]

The solution proposed alone does not solve for the existing differences, if any, in the positions of the payment networks toward support of each of the three pillar solutions as indicated in Table 5, Table 7, and Table 8.

The solution also does not solve for financial risks and business impacts, or for all of the requirements of transit merchants that arise with Use Case 1. In particular, the technical solution does not address the new financial risks to transit merchants with the Pay As You Go transaction – first tap risk (the risk of not

[39] The solution is based on the current capabilities of the payment networks. As such, only at such time that a final implementation is deployed will this requirement be able to be addressed fully.

getting paid when a transaction is declined) and the potential for second tap risk (if a card account is not added to merchant’s deny list before one or more subsequent taps are made).

Stakeholders interested in participating in Transit Open Payments should each independently assess how to address their respective financial risk and business considerations in connection with the Use Case 1 technical solution.

6. Description of Use Case 2: Pay As You Go / Mobile

6.1 Introduction

This section addresses Use Case 2: Pay As You Go / Mobile, which is similar to Use Case 1 on the fare side (single ride fare) but involves a different form factor (mobile device instead of plastic card).

The mobile device form factors in scope for Use Case 2 include: NFC-enabled mobile devices using open loop accounts and contactless payment-enabled active wearables, but not passive wearables.

Examples of active wearables include: Apple Watch, Lumia, FitBit Ionic, and Samsung S3.

The most common wearables today are extensions of mobile phones. Wearable apps have little independent functionality, except for the collection of data from the parent devices using the attached sensors. The wearable can perform a payment transaction in the same manner as a mobile device at transit POEs but requires the mobile device to be wirelessly connected to the wearable. The other kind of wearable is the independent device, such as the Apple Watch with cellular, that can operate as a standalone device using a WiFi connection or a data plan from a mobile operator. These wearables will also perform a payment transaction in the same manner as a mobile device at Transit POEs. Both of these types of wearables are "active."

Passive wearables function similar to a plastic card, and therefore, the technical solution for a passive wearable in the transit environment is the same as the Use Case 1 solution.

A transaction made by an active wearable will be a tokenized payment (with an EMV payment token), making it a different type of transaction from a transaction made with a plastic card.

In scope for Use Case 2 are contactless payments made by NFC-enabled mobile devices using open loop accounts.

Out of scope for Use Case 2 are payments made using bar codes and QR codes. Also, it is possible to use a mobile device to conduct proof of payment made by another mobile device; i.e., to check a transit rider's mobile device for whether a fare payment was made with a payment credential provisioned on it, or to verify payment was made within a ticketing app. However, this functionality is not in scope for Use Case 2, but may provide a future use case for exploration by the TWC.

For more information on wearables, please refer to the Secure Technology Alliance white paper: "Implementation Considerations for Contactless Payment-Enabled Wearables, October 10, 2017."[40]

[40] https://www.securetechalliance.org/publications-implementation-considerations-for-contactless-payment-enabled-wearables/.

6.2 Description of Use Case 2: Pay As You Go / Mobile

This section describes the Use Case 2 scenario that the TWC was tasked with addressing through technical solutions, including the risks and challenges that arise from this scenario as expressed through the perspective of stakeholder requirements.

6.2.1 Definition

The customer taps a mobile device at the POE to pay for a single ride through a Pay As You Go transaction and gains access to the subway or bus. The customer taps in only. The customer must receive a go/no go type prompt within a sub-second.

6.2.2 Transit Merchant Use Case 2 Requirements

Table 11 lists the transit merchant requirements for a transaction made with an NFC-enabled mobile device to be securely processed at a transit POE within the scope of the Use Case 2 scenario.

The Use Case 1 transit merchant requirements M1 through M13 listed in Section 3.2 apply to Use Case 2 as well. For purposes of Use Case 2, those Use Case 1 requirements should be read with NFC-enabled mobile device replacing references to plastic card, as needed. For purposes of Use Case 2, the requirements in Table 11 are supplemental to the Use Case 1 requirements and are specific to an NFC-enabled mobile device.

Table 11. Transit Merchant Supplemental Requirements for Transit Open Payments Use Case 2

Index #	Requirement
M14	With the solution deployed and from the user experience perspective, a mobile device should work the same as a card works for fare payment, with only a single tap at a transit POE terminal required to start a transaction.[41] The expectation is that device authentication should not be prompted when a mobile device is tapped at the POE.
M15	The solution should be security technology (e.g., SE, HCE and TEE) agnostic for a mobile device, regardless that different handsets and operating systems work differently from each other.
M16	Solution supports use of EMV payment tokens (DPANs) in lieu of FPANs for payment acceptance at the Transit POE, including changed or reissued DPANs.
M17	Solution supports use of non-payment tokens, such as tokens issued by an acquirer or transit merchant,[42] in addition to EMV payment tokens.
M18	Solution must enable merchant identification of each unique customer at the FPAN level, otherwise associated with only a DPAN, in order for the merchant to provide post-ride customer service, including fare processing and debt recovery, as well as fraud prevention.

6.2.3 Acquirer/Processor Transit Use Case 2 Requirements

Table 12 lists the acquirer/processor requirements for a transaction made with an NFC-enabled mobile device to be securely processed at a transit POE within the Use Case 2 scenario.

[41] It is understood that from the data perspective, the transaction message may work differently.

[42] Merchant should consult with their acquirer or system integrator for non-payment token options.

The Use Case 1 acquirer requirements A1 through A11 listed in Section 3.3 apply to Use Case 2 as well. For purposes of Use Case 2, those Use Case 1 requirements should be read with NFC-enabled mobile device replacing references to plastic card, as needed. For purposes of Use Case 2, the requirements in Table 12 are supplemental to the Use Case 1 requirements and are specific to an NFC-enabled mobile device.

Table 12. Acquirer/Processor Supplemental Requirements for Transit Open Payments Use Case 2

Index #	Requirement
A12	Solution must enable acquirer/processor to support the merchant ability to identify each unique customer at the FPAN level, otherwise associated with only a DPAN, in order for the merchant to provide post-ride customer service, including fare processing and debt recovery, as well as fraud prevention.

6.2.4 Issuer Transit Use Case 2 Requirements

Table 13 lists the issuer requirements for a transaction made with an NFC-enabled mobile device to be securely processed at a transit POE within the Use Case 2 scenario.

The Use Case 1 acquirer requirements I1 through I4 listed in Section 3.4 apply to Use Case 2 as well. For purposes of Use Case 2, those Use Case 1 requirements should be read with NFC-enabled mobile device replacing references to plastic card, as needed. For purposes of Use Case 2, the requirements in Table 13 are supplemental to the Use Case 1 requirements and are specific to an NFC-enabled mobile device.

Table 13. Issuer Supplemental Requirements for Transit Open Payments Use Case 2

Index #	Requirement
I5	Solution should be transparent to the provisioning of a payment credential to an NFC-enabled mobile device.
I6	Solution should not require any different card provisioning mechanism for transit than that supported by mobile security technology (e.g., HCE, SE, TEE) in broad use today.
I7	Solution performance should not be impacted by the tokenization that may be a part of the transaction.

6.3 Technical Functional Proposal for Use Case 2

The form factor change from dual-interface plastic card to NFC-enabled mobile device or active wearable does not affect the applicability of the Use Case 1 technical solution to Use Case 2 or suggest any other viable solution. The Use Case 1 technical solutions for the three pillars of a secure transaction (card authentication, cardholder verification and financial authorization) – namely ODA, No CVM and Deferred Authorization – are the same solutions for providing a secure transaction under Use Case 2.

This section will address aspects of the ODA and No CVM support solutions that are unique to NFC-enabled mobile devices and active wearables and which may impact certain stakeholders as discussed below.

6.3.1 ODA and Mobile Device Security Technology (SE, HCE and TEE)

Both secure element (SE) and Host Card Emulation (HCE)-based wallets can perform in the transit environment discussed in this paper, including when wireless connectivity may not be available. The approach to implementing ODA on a mobile device, however, is different for applications that use an SE (used by Apple devices) for which no additional configuration is required to enable ODA, and for applications that use HCE (used by Samsung and Android devices) for which additional configuration may be required. HCE support for ODA may also differ by global payment network.[43]

While these differences may have some impact for wallet personalization, they are transparent to the transit merchant and transit customer. Issuers need to work with the payment networks and mobile device/wallet providers to implement the Use Case 2 technical solution.

Also, stakeholders should note that a payment network may not qualify all cards for ODA enablement, such as a nonreloadable prepaid card, which qualification would not be altered by the card's provisioning on a mobile device. Also, ODA may not be available on all mobile devices.

Issuers utilizing any of the debit networks' specifications would need to check with those networks for the corresponding support for ODA with their respective U.S. Common Debit AIDs.

6.3.1.1 Active Wearables

Most active wearables employ typical mobile device security technology (SE, HCE or TEE) and support ODA in a manner similar to cards, based on the underlying operating system (e.g., iOS, Android, Windows).

6.3.2 No CVM and CDCVM (Device Unlock/Wallet Access)

Mobile devices and mobile wallets typically require the device or wallet user to take steps to unlock them.

Possible device unlock/wallet access methods available to the device owner/holder range from a numerical passcode, or a lock screen pattern, to a fingerprint scan (e.g., Touch ID) or other form of biometrics, such as facial recognition. Or it could be none of those, depending on the combination of device and operating system (OS) and decisions made by the device owner/holder. Device/wallet unlock/wallet access is a step for mobile device use that is not related to or required for the security of a payment transaction.[44]

That being said, the device unlock and wallet access methods may also have shared uses, such as the device unlock also serving as a CDCVM. CDCVM uses a mobile phone's passcode or biometric user authentication to verify the cardholder for a payment transaction, removing the need for the cardholder to enter a PIN or provide a signature. However, based on transit merchant requirements and as indicated earlier, the No CVM cardholder verification method is the technical solution for Use Case 2, as it is with Use Case 1. As such, even if a device holder unlock method generates CDCVM data and the

[43] For example, for cloud-based solutions, such as Android Pay, Mastercard uses Local Data Authentication (LDA) not CDA (per Table 5) to accommodate a needed modification for how data is passed.

[44] Apple devices will require a terminal indication to securely determine that a given terminal is a transit terminal and, combined with appropriate software on Apple devices, allow a transaction without authentication (Touch ID or Face ID). To support this functionality, providers must implement Apple's specification. This specification can be requested under a non-disclosure agreement (NDA) from Apple.

results are shared in tap data between the mobile device and the terminal, the action is not read by the terminal as performance of a CVM method.[45]

As a result, CDCVM is out of scope for this paper.[46]

It is anticipated that the Use Case 2 solution would have minimal or no effect on throughput at the gate, and could provide the same throughput as is enabled with acceptance of cards. (With the Use Case 2 solution deployed, to the extent the mobile device or wallet requires the customer to first perform a device or wallet unlock, then the use of such devices will affect required throughput.)

It is anticipated that transit merchants will be capable of configuring Transit POE terminals to enable fare payment made with a mobile device and mobile wallet to be as simple as when it is made with a plastic card, i.e., with a single tap.

For acceptance of NFC-enabled mobile devices and mobile wallets for which this is not feasible, transit merchants may seek to include messaging in applicable customer communications about how to perform the device unlock prior to approaching a transit fare gate or boarding a vehicle.

Customers performing device unlock or wallet access at the transit POE may create bottlenecks that could affect safety and adversely impact customer experience.

For purposes of Use Case 2, it is assumed that any required device unlock and/or wallet access step is completed successfully by the device owner/holder in advance of reaching the POE or is otherwise not required for the device/wallet to be used in transit.

6.3.3 Tokenization

Security standards and the payments ecosystem have evolved to further diminish the value of the PAN through tokenization.

EMVCo has defined a Payment Tokenization Specification Technical Framework[47] which describes the generation and use of surrogate values that replace the genuine PAN or Funding PAN (FPAN) with a tokenized PAN (termed 'EMV payment token' by EMVCo) on bank-issued payment credentials such as cards, mobile phones and wearables. The format of the payment token used by most bank issuers uses a 16-digit format that is identical to the FPAN format; the payment token is sometimes restricted to use within a context, such as online or contactless only. This use of tokens, combined with issuer risk management, limits the usefulness of a stolen PAN in that an EMV payment token recovered from a contactless interface, cannot be used for ecommerce transactions.

Another form of tokenization that exists in the payment ecosystem is the non-payment token. Non-payment tokens are sometimes known as security tokens; they are implemented by merchants and acquirers storing surrogate values for PANs using different methods such as random number generation, encryption or hashing the original PAN. The primary reason for using non-payment tokens is to limit the

[45] Some wallets have been modified to render the unlock action unnecessary; however, identifying which wallet providers have done this is out of scope for this paper. Also, note, at this time, some networks may not currently support CDCVM with the U.S. Common AID. Issuers should contact the payment networks for updates.

[46] If a device unlock or wallet access step is required of the device holder prior to making a single tap to pay the fare, this process may run counter to Transit Merchant Requirement M14. Transit Open Payments will still work, but will not fully comply with the technical solution described in this white paper.

[47] See https://www.emvco.com/emv-technologies/payment-tokenisation/.

merchant's or acquirer's scope of Payment Card Industry Data Security Standard (PCI DSS) compliance by reducing the value of the stored data. In this case, the PAN to token exchange is managed within a Hardware Security Module (HSM), a secure server that meets industry standards for tamper evidence, such as logging, alerts and tamper resistance such as deleting keys upon tamper detection.

6.3.3.1 Tokenization in Transit

If customers use NFC-enabled mobile devices at transit POEs, transit merchants (per transit merchant requirement M18 in Table 11) have expressed a need to be able to identify each unique transit customer to meet the operational requirements for open payment acceptance, including fare processing, and to provide an appropriate level of customer service. Transit merchants have traditionally accomplished this using the FPAN as the identifier; transit merchants believe the use of an EMV payment token or non-payment token *alone* in connection with a transaction removes this ability.

Example scenarios where identification of customers at the FPAN account level may be required to address requirement M18 and enable transit merchants to resolve certain customer service situations, include the following:

1. Customer taps an NFC-enabled mobile device at the POE using a mobile wallet, which results in only a DPAN (and not an FPAN) being "known" to the transit merchant's system. The customer then needs post-ride customer service (e.g., via call center or web). The customer may only know the FPAN and not the DPAN, and may not be able to provide sufficient information to enable the transit merchant to address his/her issue.
2. Customer taps an NFC-enabled mobile device at the POE using a mobile wallet which results in the merchant getting the DPAN. For whatever reason (e.g., reset, lost phone), the customer (or wallet provider) re-provisions the card with the same FPAN as originally provisioned to the mobile wallet and gets a new DPAN. The customer then taps his/her mobile device again at a POE using the mobile wallet, which results in the transit merchant getting the new DPAN. The transit merchant may be unable to link the two DPANs, which may impact its ability to meet certain customer requests or process with applicable business rules that involve transactions using both DPANs.
3. Customer A taps an NFC-enabled mobile device at a POE using a mobile wallet and the merchant processes a DPAN that is related to the FPAN for card X. Customer B taps the actual card X at a POE and the merchant receives the FPAN. The merchant is not able to link the FPAN and DPAN to determine that the two taps were made using the same underlying FPAN, even if used on separate payment devices. As such, the transit merchant may be unable to enforce certain fare or business rules. However, for this scenario, the simplest solution may be for the transit merchant to establish a rule requiring the same credential to be used for each unique and complete trip, and to charge separately for each credential used. This avoids issues like having two people use the same underlying FPAN to make two separate trips at roughly the same time.
4. Customer wants access to his/her transit account to view trip history, buy products or reconcile transactions to his/her credit or debit account statement. During account creation, the customer can enter an FPAN in their account to see applicable transactions. The transit account will not include any DPAN-based information; it will only include FPAN-based information. If any of the customer's journeys have been carried out using a mobile device or wearable, there is no way for the transit merchant to know the FPAN associated with the DPANs the customer used and to add that trip history to the account. Without some mechanism to identify those transactions at the FPAN account level, the merchant will not be able to show complete

information in a customer’s account or fulfill customer service requests, which can lead to disputes and chargebacks.

These examples illustrate that the transit merchant needs to be able to identify a customer and/or transaction at the FPAN level and show the limitations of reliance on only a DPAN for post-ride customer service and other related operations.

6.3.4 Payment Account Reference (PAR)

As described in Section 6.3.3, transit merchants will need to be able to link tokenized PANs and FPANs in order to display journey information, properly describe applied pricing and billing, and provide customer service associated with the underlying FPAN. The EMVCo-defined Payment Account Reference (PAR)[48] is a new solution to the transit merchant’s challenge of identifying customers at the FPAN level where the FPAN is not otherwise available. It is a unique identifier associated with a specific PAN, regardless of device, and not with a cardholder. Use of the PAR allows acquirers and merchants to track and manage accounts across multiple changing EMV payment tokens without relying on an FPAN.[49]

Where supported by the payment network(s), the merchant can obtain PAR (i) as part of the authorization response message, and/or (ii) via query, and/or (iii) from the form factor interaction at the terminal. PAR via form factor interaction depends on either card personalization which is at the issuer’s discretion or mobile application personalization which may depend on wallet providers requiring a re-rollout period for an application that was personalized before the PAR was added. Once a PAR is generated, it accompanies the associated EMV payment tokens and PAN (where necessary) by populating an additional data field in transaction messages. For the transit merchant, obtaining PAR in the authorization response is the recommended best practice.

PAR may be available now from one or more payment networks. However, obtaining a PAR requires support from the merchant’s acquirer so that PAR is included in authorization responses for all tokenized and non-tokenized accounts and/or query functionality.

Also, it should be noted that PAR may not be available for all card types (e.g., non-reloadable prepaid cards) depending on the network, nor have all handset manufacturers indicated support for PAR or a timetable for support. A transit merchant should consider these implications in the payment system design and the functions that would otherwise be supported by PAR.

Additionally, with regard to any planned use of PAR, such as for various customer service and debt recovery functions, transit merchants will need to confirm with their acquirers and the payment networks whether such planned use is acceptable under applicable rules.

The Use Case 2 solution does not preclude the use of PAR. At the time of publication of this paper, the technical approach and timelines for consistent deployment of PAR across all payment networks and issuers are being determined. Stakeholders interested in the timing of PAR implementation by any of the payment networks would need to check with those networks for information regarding details about PAR rollout.

[48] https://www.emvco.com/emv-technologies/payment-tokenisation/

[49] Source: “Payment Account Reference (PAR) Overview”, Chandra Srivastava, Visa at the Smart Card Alliance Payments Summit, April 6, 2016.

6.3.5 Deferred Authorization and Customer Messaging Impact

Mobile wallet and mobile app providers[50] should be aware that different transaction amounts may be presented to the customer during the processing of a transit open payments transaction and should consider the process flow associated with transit open payment transactions and its effect on the presentment of values to the customer from the mobile wallet or app.

For networks that permit transit merchants to make a deferred authorization, the amount used to make a deferred authorization may be different from the fare charged to the customer after any post-ride adjustments are made by the transit merchant host upon settlement of the transaction. (Since payment networks set their own rules, which may differ slightly from each other and may involve differing authorization models, stakeholders should always clarify with each network the applicable rules and amounts.) This presents a potential customer experience issue given availability of real-time purchase transaction information to the customer, such as with wallet-based in-app notifications or online banking text alerts.

Amounts could differ for one of several reasons. Example scenarios include: the choice by the merchant to use a pre-selected authorization amount for all deferred authorizations that is not always equal to the exact fare that will be owed; transaction processing timing when the transit merchant has not yet processed a prior transaction (from a prior tap), which would make the second tap a free ride due to the merchant's free transfer policy; and/or an authorization model that involves only an authorization for the actual amount to be settled under transit aggregation rules.

Such scenarios could potentially result in customer confusion since the customer may not recognize the amount in the notification or alert and/or not understand why the actual charge made to their account differs from the amount contained in an earlier notification or alert.

Providing a solution to mitigate this issue is outside the scope of this paper; however, mobile wallet providers, issuers, payments networks and any other stakeholders in transit open payments should always consider the customer experience implications of any technical solutions and seek to deploy technical approaches that support clear messaging to transit customers.

6.4 Use Case 2 Conclusion

The Use Case 2: Pay As You Go/Mobile proposed technical solution is the same as the Use Case 1 technical solution for the three pillars of a secure EMV transaction (card authentication, cardholder verification and financial authorization). Please refer to Table 9 for a summary of the solution.

The addition of Use Case 2 addresses some of the unique aspects of mobile devices and active wearables and their impact, if any, on the technical solution for Use Case 1, such as CDCVM. Various stakeholder (i.e., transit merchant, acquirer/processor, and issuer) requirements were considered in developing the solution for a transaction to be made with a mobile device and processed at a transit POE within the scope of the Use Case 2 scenario.

Table 14 summarizes the stakeholder requirements listed in Table 11, Table 12, and Table 13, and indicates whether the proposed technical solution has addressed each requirement purely from a technological perspective. It is important to note that although a requirement is indicated as being

[50] Real-time notifications are in the control of the wallet owner based on specifications agreed between the wallet owner and the networks.

addressed in the Table 14, the table does not address business and risk decisions that stakeholders will need to make which, as noted, are out of scope.

Table 14. Stakeholder Requirements for Transit Open Payments Use Case 2 Addressed/Not Addressed by Solution

Index #	Requirement	Addressed in Solution
	TRANSIT REQUIREMENTS	
M14	With the solution deployed and from a user experience perspective, a mobile device should work the same as a plastic card works for fare payment with only a single tap at a transit POE terminal required to start a transaction.[51] The expectation is that device authentication should not be prompted when a mobile device is tapped at the POE.	Yes
M15	The solution should be security technology (e.g., SE, HCE and TEE) agnostic for a mobile device, regardless that different handsets and operating systems work differently from each other.	Yes
M16	Solution supports use of EMV payment tokens (DPANs) in lieu of FPANs for payment acceptance at Transit POE, including changed or reissued EMV payment tokens.	Yes
M17	Solution supports use of non-payment tokens such as tokens issued by an acquirer or transit merchant, in addition to EMV payment tokens.	Yes
M18	Solution must enable merchant to identify the customer at the FPAN level, otherwise associated with only a DPAN, in order for the merchant to provide post-ride customer service, including fare processing and debt recovery, as well as fraud prevention.	Partially[52,53]
	ACQUIRER/PROCESSOR REQUIREMENTS	
A12	Solution must enable acquirer/processor ability to support merchant ability to identify the customer, at the FPAN level, otherwise associated with only a DPAN, in order for merchant to provide post-ride customer service, including fare processing and debt recovery, as well as fraud prevention.	Partially[54,55]
	ISSUER REQUIREMENTS	
I5	Solution should be transparent to the provisioning of a payment credential to an NFC-enabled mobile device.	Yes
I6	Solution should not require any different card provisioning mechanism for transit than that supported by mobile security technology (e.g., HCE, SE, TEE) in broad use today.	Yes

[51] Same as 43 above.

[52] There are scenarios where the DPAN may not be enough to enable the merchant to meet all post-ride customer service needs.

[53] This is true to the extent that network rules allow the acquirer/processor to allow transit merchants to identify customers at the FPAN account level (such as by returning the FPAN to the transit merchant in the authorization response).

[54] Same as footnote 52.

[55] Same as footnote 53.

I7	Solution performance should not be impacted by the tokenization that may be a part of the transaction.	Yes

As with Use Case 1, readers of Use Case 2 are encouraged to visit the applicable payment network's website or the EMVCo website for the most recent versions of contactless specifications, and to work with the applicable payment network and other service providers as needed to obtain specific requirements for implementing the solution.

7. Legal Notice

This document is intended solely to assist interested stakeholders in identifying potential technological solutions that may be useful in helping to enable open payments with contactless EMV chip cards and NFC-enabled mobile devices as a viable option for the U.S. and Canadian public transit markets. While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual or otherwise. All warranties of any kind are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

It is important to note that the information provided in this document is necessarily limited in various respects. Among other things, it is limited to the payment networks and other sources specifically identified. It is also limited to the specific use case(s) under consideration and is focused on the technological aspects of implementing open payments in the specified markets; associated business rules and arrangements are out of scope, but could nonetheless pose significant implementation considerations or hurdles.

This document reflects the payment networks' respective current positions today. Whether one or more of the networks change their position in the future specifically for transit will depend on the future decision of each payment network. Note also that each payment network determines its own rules, requirements, policies and procedures, all of which are subject to change, and that applicable industry rules, processing, liability and/or results may impact or be impacted by the specific facts, circumstances or decisions of a given solution or implementation.

Prior to implementation, merchants, issuers, acquirers, processors and others interested in implementing open payments, contactless EMV chip cards and NFC-enabled mobile devices in the U.S. and Canadian transit markets are therefore strongly encouraged to consult with all applicable stakeholders regarding associated rules, requirements, policies and procedures, including but not limited to their respective payment networks and testing and certification entities, as well as state and local requirements.