On-Chip Services: Seamlessly Performing Payment Transactions within the Existing Transportation Ticketing Infrastructure

White Paper
January 2014
# Table of Contents

About GlobalPlatform ................................................................................................................... 3
Publication Acknowledgements .................................................................................................. 4
Intended Audience ...................................................................................................................... 4
IPR Disclaimer ........................................................................................................................... 4

1. INTRODUCTION ................................................................................................................. 5

2. BUSINESS REQUIREMENTS ............................................................................................... 5
   2.1  RATIONALE FOR ON-CARD TRANSACTION API ......................................................... 5
   2.2  USE CASES .................................................................................................................... 6
       2.2.1  USE CASE #1: NFC PHONE .......................................................................................... 7
       2.2.2  USE CASE #2: CONTACTLESS PAYMENT CARD WITH PRE-INSTALLED TRANSIT APPLICATION ........ 8
   2.3  TRANSACTION FLOW .................................................................................................... 8
       2.3.1  DISCOVERY AND AUTHENTICATION ....................................................................... 8
       2.3.2  FARE PAYMENT ....................................................................................................... 9
       2.3.3  ACCESS TO THE TRANSIT NETWORK ........................................................................ 9
   2.4  BENEFITS OF THE SOLUTION ..................................................................................... 9

3. TECHNICAL IMPLEMENTATION DETAILS ......................................................................... 9
   3.1  GLOBALPLATFORM EXISTING TECHNOLOGY ............................................................. 9
   3.2  DISCOVERY .................................................................................................................. 10
   3.3  AUTHENTICATION ......................................................................................................... 11
       3.3.1  OFFERING A SERVICE .............................................................................................. 11
       3.3.2  USING A SERVICE ................................................................................................. 11
   3.4  POTENTIAL ADDITIONAL STANDARDIZATION EFFORTS TO SIMPLIFY ON-CARD TRANSACTION ........ 11

Appendix A: On-Card Transaction Flows Using an NFC-Enabled Phone ............................... 13
Appendix B: On-Card Transaction Flows Using a Contactless Payment Card with Pre-Installed Transit Application ......................................................................................... 14
Appendix C: Table of Figures .................................................................................................... 15
Appendix D: Table of Tables ...................................................................................................... 15
Appendix E: References, Definitions, and Abbreviations ........................................................ 15
ABOUT GLOBALPLATFORM

GlobalPlatform is a cross industry, not-for-profit association which identifies, develops and publishes specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. Its proven technical specifications are regarded as the international industry standard for building a trusted end-to-end solution which serves multiple actors and supports several business models.

The freely available specifications provide the foundation for market convergence and innovative new cross-sector partnerships. The technology has been adopted globally across finance, mobile/telecom, government, healthcare, retail and transit sectors. GlobalPlatform also supports an open compliance program ecosystem to ensure the long-term interoperability of secure chip technology.

As a member-driven association with cross-market representation from all world continents, GlobalPlatform membership is open to any organization operating within this landscape. Its 100+ members contribute to technical committees and market-led task forces. www.globalplatform.org
**Publication Acknowledgements**

GlobalPlatform wishes to thank all members of the Transportation Sub Task Force, which developed the ideas throughout this document. Special thanks go out to the following GlobalPlatform members and their respective organizations:

*Contributors:*

Stephanie El Rhomri – FIME  
Marc Kekicheff – Visa  
Virginie Galindo – Gemalto

*GlobalPlatform Team Members:*

Alliances Management – Operations Secretariat  
Gil Bernabeu – GlobalPlatform Technical Director  
Kevin Gillick – Executive Director of GlobalPlatform

**Intended Audience**

This document is intended primarily for the use of the Transportation Sub Task Force, the Card Committee, payment schemes, Public Transport Operators (PTOs), and any other stakeholder who might have interest in an On-Card Transaction API. As noted above, the objective is to solicit feedback from parties in both the transportation and payment industries so as to define a technical solution that does not preclude any business agreements between parties.

**IPR Disclaimer**

GlobalPlatform draws attention to the fact that compliance with this specification may involve the use of a patent or other intellectual property right (collectively, “IPR”); claims concerning this specification may be published at [https://www.globalplatform.org/specificationsipdisclaimers.asp](https://www.globalplatform.org/specificationsipdisclaimers.asp). GlobalPlatform takes no position concerning the evidence, validity, and scope of these IPR claims.
1. **INTRODUCTION**

For some travelers, such as foreigners in a new country, the public transportation ticketing process requires several cumbersome steps—including interfacing with a ticketing agent or kiosk, conducting a separate payment card transaction, and the issuance of a paper ticket. There are in fact some very good reasons for this multi-step process, including broadly installed legacy systems and the need to ensure that transactions are secure.

This document explores how to work within existing transportation networks and ticketing processes to seamlessly deploy applications that require interaction between the public transportation and payment industries. For any solution to gain mass market traction, it must work within the existing infrastructure and allow ticketing transactions to be initiated either through the transportation network or the payment application.

With this in mind, this document examines the current network infrastructure (including the transit operator gate and card application) and explains how a ticket payment can be generated via a banking application that uses a new concept called an On-Card Transaction. Next, the document discusses current GlobalPlatform technology that could be leveraged to implement this On-Card Transaction mechanism. GlobalPlatform technology provides an end-to-end framework for the mobile wallet, but it is acknowledged that it may be possible to simplify the deployment of applications using on-card transactions.

In discussing this solution, the aim of the GlobalPlatform Transportation Sub Task Force is to solicit feedback from interested parties in both the transportation and payment industries. The end objective is to define a simple technical solution for On-Card Transaction APIs that does not preclude any business agreements between parties.

Note that, for the sake of simplicity, this document focuses on the transit use case since there is an immediate need. However, the same technology could also be used for other use cases, such as ticketing payment.

Feedback is encouraged; please submit comments and ideas to secretariat@globalplatform.org.

2. **BUSINESS REQUIREMENTS**

   2.1 **RATIONALE FOR ON-CARD TRANSACTION API**

As contactless payment cards become more prevalent, the transit sector has an increased opportunity to facilitate access to transit networks for payment card holders. In fact, high-level requirements for contactless payment card acceptance in the transit industry have already been defined in ISO/TR 14806: Public transport requirements for the use of payment applications for fare media [14806].

Nevertheless, existing fare structures and Fare Collection System (FCS) infrastructures complicate the ability of the transit industry to accept contactless payment cards. There are several challenges that may impact the FCS:

- Whether the contactless reader complies to the EMV Contactless specification
- The contactless reader’s online capability
- The card exception file, aggregation, and authentication/authorization

The trend toward use of NFC handsets offers a new opportunity to simplify the acceptance of contactless payment cards: a payment application and a transit application can both be
downloaded and hosted on the same Secure Element within the mobile device. This offers a
natural opportunity to allow collaboration between the payment and transit industries without
impacting the Public Transport Operator (PTO) gate infrastructure. The only impact would be on
the applications hosted within the Secure Element.

2.2 Use Cases

In the use cases considered here, the passenger could have an NFC-enabled phone or a payment
card that has a pre-installed transit application. In either use case, the On-Card Transaction could
take place online or offline.

Critically, within each of these use cases we explore how it is possible for the
transaction to be initiated either by the payment application or the transit application:
GlobalPlatform technologies make both possible. While the transaction flows for each of
these scenarios are similar, it is important to illustrate how different business models
are supported.

Prior to examining specific use cases, consider Figure 1 below, which illustrates a high-level
overview of the potential use cases. What is important here is to understand the following:

- The passenger can use either an NFC-enable mobile device or a payment card with a pre-
  installed payment application;
- The Secure Element contains both the Transportation and Payment applications, which can
  communicate with one another according to the defined transaction flows; and
- Both the Transportation and Banking applications can possibly communicate with their
  respective back-office systems.

Figure 1: High-Level Transaction Flow for On-Card Transaction
2.2.1 Use Case #1: NFC Phone

In this first use case, the passenger has an NFC-enabled phone. We assume that the passenger pays the fare for a single trip prior to accessing the transit network. This includes paying a fare to extend a journey.

For the sake of simplicity, we do not specify the handset power state: it is assumed that the handset may be powered-on or turned off, depending on the action in progress.

With respect to the applications, we assume the following:

- The NFC service (transit application or payment application) encompasses both a mobile application and a Secure Element application;
- Whatever the tariff structure (flat fare, time based, zonal, distance based, etc.), the transit application calculates the fare; and
- The payment application may perform the transaction, either with an online acquirer host or an on-device POS application.

It should also be noted that this use case assumes that the PTO has a contract in place with a bank. A PTO may operate in several cities, and a bank may have agreements with different PTOs. Accordingly, the passenger may be offered access to different networks, cities, and infrastructure. Thus, either the PTO or the bank may attempt to make things easier for the user by listing the authorized networks—either via an NFC tag in the transit station or the user interface—so as to allow the appropriate application to be downloaded.

Nonetheless, these different models are supported as the passenger completes a transaction. For the sake of clarity, Table 1 compares the transaction flows for the On-Card Transaction on an NFC-enabled phone when initiated by the Transit Application versus the Payment Application. Appendix A has diagrams of these transaction flows.

### Table 1: On-Card Transaction Flows When Using an NFC-Enabled Phone

<table>
<thead>
<tr>
<th>Transaction Initiated by Transit Application</th>
<th>Transaction Initiated by Payment Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prior to accessing the transit network, the passenger downloads the NFC transit service pre-authorized by the passenger's Bank to her/his mobile handset.</td>
<td>• Prior to accessing the transit network, the passenger downloads to her/his mobile handset an extension of the NFC banking for transit service that includes the transit application.</td>
</tr>
<tr>
<td>• The passenger selects a fare through the transit operator's UI.</td>
<td>• The passenger selects payment for a transit ticket through the Banking service UI.</td>
</tr>
<tr>
<td>• The transit application sends a payment request to the payment application, which resides in the same secure element.</td>
<td>• The payment application loads a ticket into the transit application.</td>
</tr>
<tr>
<td>• The payment application returns a payment confirmation to the transit application.</td>
<td>• The transit application triggers the fare update.</td>
</tr>
<tr>
<td>• The transit application triggers the fare update.</td>
<td>• The passenger taps her/his phone at the gate or the ticket validator.</td>
</tr>
<tr>
<td>• The passenger taps her/his phone at the gate or bus validator.</td>
<td>• The transit application grants the passenger access to the transit network.</td>
</tr>
</tbody>
</table>
2.2.2 Use Case #2: Contactless Payment Card with Pre-installed Transit Application

The process is somewhat different for a passenger with a payment card that has a pre-installed transit application. In wanting to purchase a fare, the passenger taps the payment card in a kiosk that allows the user to interact with the application. The passenger then pays for the fare prior to entering the transit network.

For this to work, it is important to note that both applications must reside on the passenger’s payment card. However, by using standard GlobalPlatform commands, the transit application could be loaded onto the payment card post-issuance and at a transit kiosk.

Table 2 compares the transaction flows for an On-Card Transaction on a contactless payment card when initiated by the Transit Application versus the Payment Application. Appendix B has diagrams of these transaction flows.

<table>
<thead>
<tr>
<th>Transaction Initiated by Transit Application</th>
<th>Transaction Initiated by Payment Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The kiosk selects the transit application, which sends a payment request to the payment application.</td>
<td>• The kiosk selects the payment application, which performs a banking transaction using the kiosk infrastructure.</td>
</tr>
<tr>
<td>• The payment application performs a payment transaction using the kiosk infrastructure.</td>
<td>• The payment application loads a ticket into the transit application.</td>
</tr>
<tr>
<td>• The payment application returns a payment confirmation to the transit application.</td>
<td>• The transit application triggers the fare update.</td>
</tr>
<tr>
<td>• The transit application triggers the fare update.</td>
<td>• The transit application grants the passenger access through the transit network.</td>
</tr>
<tr>
<td>• The transit application grants the passenger access through the transit network.</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: On-Card Transaction Flows When Using a Contactless Payment Card with Pre-installed Transit Application

2.3 Transaction Flow

As previously discussed, whether the passenger is using an NFC-enabled phone or a contactless payment card with a pre-installed transit application, both applications reside in the same Secure Element. This is what the On-Card Transaction API enables, but the transaction flow requires three phases: Discover and Authentication, Fare Payment, and Access to the Transit Network. Each of these is explained below.

2.3.1 Discovery and Authentication

Regardless of which application initiates the transaction, the transit application needs to discover the payment application available in the card, and vice versa. This can happen when the applications are installed. Alternatively, it can be triggered by the user prior to entering the transportation network.

Additionally, the payment application should authenticate the transit application, and vice versa. This can be done when the application is installed by sharing some type of authentication token, or it can be directly managed in the applications when performing the on-card transaction.
2.3.2 Fare Payment

Thanks to an On-Card Transaction between a payment application and a transit application, the end user is able to add a new transit ticket to her/his phone or card.

If the device hosting the Secure Element is connected to a communications network, the payment application may want to transmit information to the Bank’s back-office systems. This can be done during or after the payment transaction.

Depending on the network connectivity of the kiosk or the NFC phone, the payment application may want to perform online authorization before allowing the ticket to be loaded.

2.3.3 Access to the Transit Network

The transit application will complete the transaction at the gate/validator. While this mechanism varies from one transport network to another, it should be noted that the PTO and bank systems may communicate to acknowledge that the transaction has been completed.

2.4 Benefits of the Solution

This solution allows transit and payment applications to interact within the Secure Element—while limiting the impact to the PTO’s legacy infrastructure. It enables passengers to access a transit network with no change to gates, ticket validators, or the Fare Collection System.

Conforming to existing gate processing procedures is important because it helps the transit authority ensure performance and maximize passenger flow at the gate. The additional time related to the banking transaction is performed prior to accessing the transit network while the real-time transaction is performed using the transportation technology.

The impact to the Bank’s back office is also limited: at most, the kiosk infrastructure is updated if online authorizations and/or transit application loading are needed.

The primary impacts of this solution are on the applications that hosted in the Secure Element (whether this is a smart card, UICC, or embedded secure element) and the front office systems (kiosk or mobile application).

3. Technical Implementation Details

All of the use cases outlined herein require the same technological approach: application discovery, authentication, and communication. Most of those features are already available in the current set of GlobalPlatform specifications.

3.1 GlobalPlatform Existing Technology

GlobalPlatform already offers all required technical features to implement On-Card Transaction. The critical requirement for the On-Card Transaction is the ability to get access to a service offered by another application. This requires communication between two applications within the same card or Secure Element, a feature enabled by the Global Services APIs described in the GlobalPlatform Card Specification ([GPCS]).
3.2 Discovery

Figure 2 below illustrates the Discovery process in the instance that the transaction is initiated by the transit application. As previously noted, the payment application could just as easily initiate this process, but for the sake of simplicity, we show only one diagram here.

Step 1 in Figure 2 illustrates the fact that, to offer a unique service on a Secure Element, an application must first register a service with a service name that is unique for that Secure Element. This application must be registered within the Card Registry, a database that contains information about all applications and actors’ rights, for Discovery to be possible.

Whether an NFC-enabled phone or contactless card is being used, Step 2 of Figure 2 illustrates that the transit application retrieves the service by asking the GlobalPlatform Environment (which contains all rules defined within GlobalPlatform for a card) to permit access to a service registered by either i) a specific name or ii) an association of service name and AID. A similar discovery process occurs in the event that the payment application initiates the transaction, but in this scenario, the payment application would retrieve the transit service by asking the GlobalPlatform Environment to permit access.

Finally, assuming the service is available on the Secure Element, the transit application will be able to use the service.

Figure 2: Registering and Using an On-Card Service (Initiated by Transit)
3.3 Authentication

3.3.1 Offering a Service

The application offering a service will receive a request from the GlobalPlatform Environment. The application will authenticate the requester and, if the requester is authorized, grant access to the service.

GlobalPlatform does not mandate any authentication service: authentication is business-driven and related to the specific security requirements of the proposed service.

3.3.2 Using a Service

The transit application (or the payment application in other scenarios) verifies the security environment of each service before using it. GlobalPlatform offers different options to allow a service provider (bank or PTO) to decide whether to load and later to use a service.

By retrieving information from the Secure Element, it is possible for the service provider to either directly or indirectly retrieve certification status information by communicating with the back office systems managing the Secure Element. The GlobalPlatform Messaging Specifications offer different messages that allow IT systems to exchange such information.

GlobalPlatform is currently working to standardize access to a Secure Element’s certification status, including access to all the security certificates related to a specific Secure Element throughout its lifecycle.

After the loading decision, the application must determine whether to use the service of another on-card application. Since only an authorized application is able to register a service within the Secure Element, GlobalPlatform ensures that the application offering the services has been authorized by the original Secure Element issuer.

An application should use a specific service only if that service supports the authentication mechanism defined by the application.

3.4 Potential Additional Standardization Efforts to Simplify On-Card Transaction

As noted at the outset, GlobalPlatform’s objective is to develop an international industry standard for building a trusted end-to-end solution for On-Card Transactions. To be successful, it must support different business models and accommodate multiple actors.

As a neutral entity, GlobalPlatform provides the foundation for market convergence and innovative new cross-sector partnerships. It supports development of open solutions that are in turn supported by different vendors.

Since the On-Card Transaction technology will be shared by different markets, GlobalPlatform is considering offering the following:

- A global registration of the service name (so as to ensure uniqueness)
- A standard authentication mechanism validated by multiple industries

In all cases, it is not in GlobalPlatform’s scope to define the format or the content of any data element of an On-Card Transaction.
Feedback on the use of existing GlobalPlatform technologies for On-Card Transactions, or on additional potential standardization efforts, is encouraged; please submit comments and ideas to secretariat@globalplatform.org.
APPENDIX A: ON-CARD TRANSACTION FLOWS USING AN NFC-ENABLED PHONE

Figure 3: NFC Phone On-Card Transaction Initiated by Transit Application

Figure 4: NFC Phone On-Card Transaction Initiated by Payment Application
APPENDIX B: ON-CARD TRANSACTION FLOWS USING A CONTACTLESS PAYMENT CARD WITH PRE-INSTALLED TRANSIT APPLICATION

Figure 5: Contactless Payment Card On-Card Transaction Initiated by Transit Application

Figure 6: Contactless Payment Card On-Card Transaction Initiated by Payment Application
APPENDIX C: TABLE OF FIGURES

Figure 1: High-Level Transaction Flow for On-Card Transaction ........................................... 6
Figure 2: Registering and Using an On-Card Service – Scenario 1A or 2A ............................... 10
Figure 3: NFC Phone On-Card Transaction Initiated by Transit Application .......................... 13
Figure 4: NFC Phone On-Card Transaction Initiated by Payment Application ....................... 13
Figure 5: Contactless Payment Card On-Card Transaction Initiated by Transit Application ...... 14
Figure 6: Contactless Payment Card On-Card Transaction Initiated by Payment Application ... 14

APPENDIX D: TABLE OF TABLES

Table 1: On-Card Transaction Flows When Using an NFC-Enabled Phone ............................... 7
Table 2: On-Card Transaction Flows When Using a Contactless Payment Card with Preinstalled Transit Application ................................................................. 8

APPENDIX E: REFERENCES, DEFINITIONS, AND ABBREVIATIONS

References

Normative References

<table>
<thead>
<tr>
<th>Standard / Specification</th>
<th>Description</th>
<th>Ref</th>
</tr>
</thead>
</table>

Informative References

<table>
<thead>
<tr>
<th>Standard / Specification</th>
<th>Description</th>
<th>Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/TR 14806</td>
<td>Intelligent transport systems – Public transport requirements for the use of payment applications for fare media</td>
<td>[14806]</td>
</tr>
</tbody>
</table>

Terminology and Definitions

Selected technical terms used in this document are included below. Additional technical terms are defined in [GPCS].

Terminology and Definitions
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMV</td>
<td>A global standard, with contact and contactless specifications that facilitate worldwide interoperability and acceptance of integrated circuit (IC)-based payment instruments.</td>
</tr>
<tr>
<td>Secure Element</td>
<td>A tamper-resistant component which is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models. May exist in any number of form factors, such as card, UICC, embedded SE, smartSD, smart microSD, etc.</td>
</tr>
</tbody>
</table>

**Abbreviations and Notations**

Selected abbreviations and notations used in this document are included below. Additional abbreviations and notations are defined in [GPCS].

<table>
<thead>
<tr>
<th>Abbreviation / Notation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AID</td>
<td>Application ID</td>
</tr>
<tr>
<td>FCS</td>
<td>Fare Collection System</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sale</td>
</tr>
<tr>
<td>PTO</td>
<td>Public Transport Operator</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
</tbody>
</table>