GlobalPlatform’s Value Proposition for the Public Transportation Industry:
Seamless, Secure Travel Throughout Multiple Transportation Networks

White Paper
November 2009
GlobalPlatform’s Value Proposition for the Transportation Industry: Seamless, Secure Travel Throughout Multiple Transportation Networks

Contents
About GlobalPlatform
Publication Acknowledgements
Executive Summary
SECTION 1: Introduction to Public Transportation Fare Management
  1.1. Advantages of Electronic Ticketing Systems
  1.2. Interoperability between e-Ticketing Schemes
SECTION 2: Current Challenges for Public Transportation
  2.1. Looking for Ticketing Interoperability and Intermodality
  2.2. Enabling Competitive Procurement
  2.3. Managing Privacy Requirements
  2.4. Enhancing the Security of Transportation Passes
  2.5. Taking Advantage of New Contactless Media
  2.6. Moving from Smart Ticketing to Smart Urban Mobility
SECTION 3: Benefits to the Transportation Industry of Leveraging GlobalPlatform
  3.1. Context
  3.2. GlobalPlatform: The Standard for Smart Card Application Management
  3.3. Improving Ticketing Interoperability and Intermodality
  3.4. Relying on Standards and Open Products
  3.5. Fulfilling Privacy Requirements
  3.6. Securing Transportation Passes
  3.7. Enabling the Usage of New Media in Transportation
  3.8. Benefiting from and Complying with a Cross-Industry Certification Process
  3.9. Managing Additional Services
SECTION 4: Conclusion
APPENDIX A: References and Standards Bodies
APPENDIX B: Publications
APPENDIX C: Abbreviations
APPENDIX D: Definitions
APPENDIX E: Table of Figures
About GlobalPlatform

GlobalPlatform is the leading, international association, focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technology supports multi-application, multi-actor and multi-business model implementations, which delivers benefits to issuers, service providers and technology suppliers.

GlobalPlatform is a member driven association with cross-industry representation from all world continents. As of October 2009, an estimated 449 million GlobalPlatform-based smart cards had been deployed. Additionally, 2.2 billion mid range USIM/SIM cards worldwide are estimated to use GlobalPlatform card technology to enable over-the-air (OTA) application downloads for 3G and GSM mobile networks.

GlobalPlatform is an independent, not-for-profit organization and its strategy is defined and prioritized by a Board of Directors. GlobalPlatform is currently chaired by Sebastien Tormos, Vice-President of Marketing, Datacard Group, and vice-chaired by Marc Kekicheff, Vice President Product Technology, Visa Inc. Kevin Gillick serves the membership on a full-time basis as its Executive Director.

For further information, visit www.globalplatform.org.
Publication Acknowledgements

GlobalPlatform wishes to offer special thanks to the members of the Transportation Task Force and their respective organizations for their involvement in developing this white paper.

Contributors include the following:

Full Members:

Gil Bernabeu – Gemalto
Dominique Brulè - Gemalto
Marc Vauclair - NXP
Emmanuel Mellery – NXP
Michele Struvay – NXP

Participating Members:

Rogier Boogaard – Collis
Christian Demeer – GALITT

Observer Members:

Stephanie El Rhomri – FIME
Laurence Gizzi – NEC Corporation

Consultant Members:

Jean Philippe Amiel – Nextendis

Members of a Public Entity:

Michel Barjansky – RATP
François Guillaume - RATP
Pierre Terrée – RATP

GlobalPlatform Team Members:

Kevin Gillick – Executive Director of GlobalPlatform
Alliances Management – Operations Secretariat
Executive Summary

Current trends in public transportation have led to an increased interest in smart ticketing systems. Driven by a myriad of forces—including governmental privacy requirements and the desire to improve travel efficiency—public transportation organizations are seeking ways to offer better services, reduce operating expenses, increase ticketing efficiency, integrate different transportation modes, improve safety, reduce fraud, and maximize the opportunities for fare price discrimination.

The resulting desire is for a ticketing system that allows for uninterrupted travel between Public Transportation Operators (PTOs), whether this be between cities or entire countries. Simply put, one ticketing system should allow for a seamless travel experience between geographies, allowing the traveler to have an uninterrupted door-to-door travel experience. But because traditional Electronic Fare Management systems have catered to the needs of each independent PTO, it has become increasingly difficult to achieve mutual acceptance among different PTOs. Accordingly, there are three options to accomplish this interoperability from the traveler’s perspective: on the card level, the application level, or the product level.

Today’s technologies—contactless USB dongles, NFC phones, and contactless banking cards—enable this seamless travel experience to become a reality. However, implementing such e-ticketing systems requires considerable thought so as to maximize customer privacy and minimize the possibility of fraud.

GlobalPlatform technology provides a solution not only to the e-ticketing needs of PTOs, transportation authorities, fare management system integrators, and equipment providers, but also to the security and privacy concerns of transportation authorities and the end user. GlobalPlatform enables a complete “transportation application” management.

Leveraging the GlobalPlatform specification for transportation uses does not require customization; rather, it can be used now with existing systems. More importantly, it enables the use of third-party media, such as NFC phones, smart cards, or USB tokens. Because it supports both standard and non-vendor-specific products, the GlobalPlatform solution favors competitive procurement and allows each PTO to enrich its existing service offering by adding new applications and services even after the media have been issued. Most importantly, by enabling the coexistence of multiple local transportation applications on the same media, GlobalPlatform enhances interoperability and thus meets the needs of today’s PTOs.

As a technology that is already embraced by the major card business sectors (telecoms, payment, health care and government), GlobalPlatform is the ideal technology solution to help the public transportation industry better master the management of customer services that are embedded in transportation cards or in any new transportation pass form factor. As the technology is already rolled out in NFC phones and implemented for card payment, leveraging the GlobalPlatform Secure Element for multiple applications is a simple process.

Accordingly, all stakeholders in the public transportation industry can benefit from the ability to preserve their unique service structure while leveraging a field-proven process for application downloading and personalization.
SECTION 1: Introduction to Public Transportation Fare Management

For years, governments have been promoting the use of public transportation because it offers several major advantages over using cars. These include a reduction in carbon dioxide and other emissions, a more efficient use of road or rail space per traveler, and a reduction in parking and traffic-related congestion. For these reasons and more, it is expected that the use of public transportation will continue to increase.

1.1. Advantages of Electronic Ticketing Systems

In the initial analysis and investment phase, it is worthwhile to consider how the Public Transportation Operator (PTO) can benefit from implementing an electronic ticketing system.

From the perspective of the PTO, some possible benefits of introducing an electronic ticketing scheme are as follows:

- Reducing operating costs, as a result of reducing the number of disposable tickets and mechanical parts in readers and vending systems
- Increasing ease of use by automating ticket vending and payment handling
- Integrating different transportation modes and transportation operators into a single-ticket system, thereby allowing interoperable travel products and revenue settlement based on actual service instead of statistical averages
- Introducing physical barriers (gates) in previously open transportation systems, which will simultaneously increase traveler safety and reduce fraud
- Increasing the throughput of existing gated systems; one way of accomplishing this is to migrate from magnetic stripe-based technology to contactless smart cards
- Maximizing revenue, through the use of differentiated fare policies that enable automatic fare modification, such as peak / off-peak tariffs
- Making it easier to replace lost or stolen tickets
- Increasing the control over a ticket’s life cycle, thus reducing fraud

Each PTO will prioritize these benefits differently. Some PTOs, for example, will benefit from new retail channels; other PTOs will likely benefit more from fraud reduction and increased safety mechanisms. Additionally, the attractiveness of integrating PTOs will vary, as will each PTO’s approach to governmental regulations. Different regulatory environments may, for example, have different requirements regarding how much cardholder-specific data can be stored and how that data should be protected—both on the card itself and in back offices.

Because the business requirements of an electronic ticketing system vary so widely, so do the technical solutions. Generally, these systems use dedicated integrated circuit cards. The technology used for these cards, the card readers, and the backend systems varies widely and includes the following distinctions: memory cards versus smart cards, symmetric versus asymmetric cryptography, proprietary versus open standards, and more.

Furthermore, there is a trend in the market suggesting that PTOs should consider moving away from just playing the transportation operator role. Instead, they are being asked to become overall door-to-door mobility providers.
All of these regulatory, business, and technological pressures have changed the landscape for electronic ticketing schemes throughout the world. These schemes vary in scale—from a single city or transportation mode, to entire countries with integrated transportation modes—which requires a solution that is robust enough to deliver solutions for all environments. The problem, however, is that these different schemes rarely interoperate, and it seems unlikely that they ever will.

1.2. Interoperability between e-Ticketing Schemes

Currently, Electronic Fare Management systems cater to the need of each PT network independently, and this market has been dominated by city- or region-wide fare management solutions.

Since this traditional approach was not designed from the beginning with a wider regional or national interoperability in mind, it has become increasingly difficult to achieve mutual acceptance of fare products or transportation cards between networks.

From the traveler’s point of view, interoperability between e-ticketing schemes is possible at several levels:

- **Card level**: This means either that the same card technology is accepted by different PTOs or that a particular PTO accepts different card technologies. For example, in the UK public transportation national scheme, both memory cards and smart cards must be supported. However, PTOs’ cards differ based on the applications present. This means that a traveler who has a card from one PTO should be able to load another application on the same card (provided that this application is available for this card technology) and subsequently buy an appropriate travel product for another PTO.

- **Application level**: In this scenario, the same application is used by different PTOs, but the products differ from scheme to scheme. This is true of some public transportation networks in some regions, including certain regions of Germany and France. A traveler with a card from one scheme is able to load products from another scheme directly onto the same card.

- **Product level**: This arrangement assumes that the same product, such as an electronic ticket, can be used with different PTOs. This requires clearing and settlement of fares among the different Application Providers, which can either be done centrally or on a party-by-party basis. An example of a scheme that requires interoperable products is the Dutch national public transportation ticketing system.

It is clear that achieving any form of interoperability between schemes requires either technical (card level) or business (product level) agreements between PTOs. Because of the reasons outlined above, such agreements may be difficult to reach, but it is important to note that, from the perspective of the card holder, full interoperability might not be necessary. Consider the following example.

Let us define a traveler’s “home network” as the most frequently visited region and the “visitor network” as a region visited only periodically. No doubt, this traveler would welcome the opportunity to use one product inside the home network without having to worry about which PTO is used. Additionally, it would obviously be preferable to be able to use the same travel card on the visitor network.
However, while this would be considered the ideal situation, our traveler would likely be willing to load a temporary travel product application while traveling on the visitor network. In other words, although our traveler requires *product interoperability* within the home network, only *card interoperability* is necessary between the home network and a visitor network.

It should be noted, however, that loading (or downloading) the new application and travel product should be as easy as possible. This is where the technical challenge comes into play; this challenge is known as Application Download Interoperability and is discussed in [6].

Finally, when it comes to enabling interoperability, it is possible to use existing identification mechanisms together with a back office registration. Examples of these include a contactless bankcard or a mobile phone. In either approach, the GlobalPlatform specifications play an enabling role.
SECTION 2: Current Challenges for Public Transportation

2.1. **Looking for Ticketing Interoperability and Intermodality**

One of the main challenges for public transportation authorities is to provide a seamless travel experience for their passengers. The desire for interoperability and intermodality is driven by three different but complementary interests:

- The need to enable passengers to travel across and between different transportation networks—including those built, organized, and operated by different authorities. This, in turn, must enable travelers to use the same transportation smart card to access different public transportation networks.
- The desire of governmental authorities to discourage more polluting forms of transportation by promoting green mobility. To accomplish this, urban passengers should have seamless access via their transportation smart card to other green mobility services, such as “park and ride” or city bike rental.
- The need to enable door-to-door long-distance travel. This will occur by enabling access to long-distance travel options at both departure and destination locations.

The recent consultation launched by the UK Department for Transport [8] illustrates that transitioning from a large number of distinct Fare Management systems to an interoperable, nationwide system will not be straightforward. This is especially true where interoperability was not a primary driver in developing a particular local Fare Management system.

2.2. **Enabling Competitive Procurement**

Despite the efforts required, most PTOs are willing to migrate to an Interoperable Fare Management system that relies on open standards. This is particularly true for smart media, for which PTOs have placed recurrent orders and expect to benefit from standard components leveraged by a wide variety of competing organizations.

Relying on open standards-based products is also the most effective way to enable suppliers to deliver products that address larger markets. Considering that the largest public transportation networks never order more than a few hundred thousand cards per year, open standards reduce their development cost and offer them a longer term protection of their investment. Furthermore, it is expected that relying on open standards for smart cards will pave the way to open and competitive procurement, and thus, price reductions.

2.3. **Managing Privacy Requirements**

Facing public concerns about the pervasive and intangible nature of these new communication means, governments often try to anticipate and manage privacy risks by passing ad-hoc regulations. The European Commission’s [“Recommendation on the implementation of privacy and data protection principles in applications supported by radio frequency identification”](#) is a recent example of such an initiative, which recommends that end users receive full control over both the activation and deactivation states of contactless devices.
Over-the-air (OTA) transactions make e-tickets vulnerable to illegitimate access without the user’s knowledge. Many system designers concentrate on security aspects related to the protection of on-ticket entitlement, which leads to a focus on preventing fraud that results from spoofing, skimming, or cloning attacks. This approach exposes a serious flaw: failing to understand how anonymous Unique Identifications (UIDs) or worthless information (such as the emission date) can impact privacy—even when the owner’s identity is not exposed along with this seemingly benign information. In actuality, if this benign information is repeatedly exposed at different locations, malicious readers could spot the e-ticket owner at different places and thus profile and trace movements. This already happens today in areas with Wi-Fi hotspots. As a result, such “benign” privacy risks are not acceptable and may require appropriate measures to prevent illegitimate tracking activities. For this reason, several countries have legally mandated that transportation services implement anonymous usage as a basic feature in all implementations.

Today’s fare collection models often require complex attribution definitions in order to allow for detailed tariff differentiation and usage rules. Criteria like age, gender, family status, group membership, or place of residence should all be considered sensitive information that is commonly used to determine specific owner access rights. Online credentials should be exercised in full accordance with basic privacy principles, including user consent, transparency, right purpose, data limitation and confidentiality.

Without sufficient privacy protection measures, or in situations with poor implementation of platforms and applications, the risk of identity theft is extremely high. This can result in severe damage to the issuing brand, as well as the need for considerable liability reassessments on the part of manufacturers and operators.

In today’s race for rapid e-ticketing deployment, a major hurdle lies in the different and incompatible approaches to privacy implementation. In the case of multi-PTO smart media, the privacy implementation of the hosting transportation network may be incompatible with that of another network. This is an important concern, and addressing it will help to reduce disputes between operators in case of a privacy breach.

2.4. Enhancing the Security of Transportation Passes

Recent media coverage suggests that automated fare collection systems are under siege.

Today, all entities of the system—cards, readers, and infrastructure—are the target of concerted attacks. The results of such attacks are published on the Internet and presented in conferences, which in turn means that they are available to criminal organizations hoping to perpetuate more frauds.

Accordingly, security is a system issue. Merely having a high security evaluation level on the transportation pass itself does not mean that the whole system is secure.

The security of transportation passes should, at a minimum, involve the following requirements:

- Secure tickets (i.e. tamper resistance, inability to clone), especially when these are virtual cards in a software environment in a mobile phone
• Secure loading, activation, selection and management. Namely, only genuine applications should be recognized
• Secure communication protocols between all entities (transportation passes, mobile phones, readers, and back-ends)
• Secure trust provisioning, which requires that all keys necessary for the trust model must be created, loaded, and managed according to the highest security standards
• Security features should be based on and certified according to recognized standards (ISO, ANSI, ECMA, NIST, Common Criteria, and etc.)
• Security features should support the required privacy enhancement technologies

2.5. Taking Advantage of New Contactless Media
Multiple worldwide initiatives have focused on evaluating the usage of new contactless media for smart ticketing:

• Contactless USB dongles can provide a convenient way, once connected to a PC, to “top-up” tickets over-the-Internet (OTI)
• NFC phones enable the user to instantly load transit applications and tickets from anywhere and at anytime
• Contactless banking cards are broadly deployed by banks and can be used as smart media for transportation

PTOs view such media as an opportunity to cut media distribution costs and facilitate end user acceptance. Without forgetting the needs of local users, they tend to focus on the occasional and/or foreign travelers. Moreover, in addition to enabling PTOs to make use of new distribution channels, these new media can enhance the customer’s travel experience by removing the need to queue at ticket vending machines. New media like NFC phones will also provide an interactive interface to the end user, allowing the traveler to instantly check ticket balance, purchase tickets, view an interactive trip planner, and review traffic information.

To take advantage of this opportunity, PTOs are looking for ways to integrate the new media owned by other application providers into the existing fare systems.

2.6. Moving from Smart Ticketing to Smart Urban Mobility
Over the last decade, the main focus for PTOs interested in smart ticketing has been to provide a convenient and cost effective way to for customers to pay.

Recently, public transportation authorities have shown a desire to provide more services to passengers. This shift is a move away from the concept of a simple transportation pass to a more complete “traveler companion concept.” This model adds to the traditional transportation services by providing traffic information, timetable access, localization services, and itinerary finding services.

Those applications will be introduced over time, and each application will have a different life cycle.

As a consequence, there will likely be more than one application that PTOs must manage, but they are nonetheless looking for a standard way of developing, loading, and personalizing these applications—regardless of the type of smart media (smart card, NFC phone, USB dongle, or etc.).
SECTION 3: Benefits to the Transportation Industry of Leveraging GlobalPlatform

Having observed how regulatory, business, and technological pressures have contributed to developing modern trends in e-ticketing, the next step is to understand how GlobalPlatform technology can help transportation operators and organizations to overcome the challenges described in the previous section.

3.1. Context
Generally speaking, a “transportation application” is a software application that manages security, processes fare rules, handles transportation titles, and incorporates customer rights. It includes a way for customer profile information to be stored so that discounted tariffs can be applied, as well as a way to differentiate between different transportation products, such as single tickets, concessionary fares, and season tickets.

To incorporate future services that PTOs will offer, as well as changes in customers’ lives, transportation applications need to be capable of evolving.

There is also a clear need to be able to develop several transportation applications out of the same code package. For example, consider a situation where different PTOs have different transportation applications, such as city- and region-wide implementations. Both versions of the same application should be able to coexist on the same Secure Element while sharing the same application code to avoid wasting memory space.

In this context, there is a clear need to load, install and personalize a transportation application on a Secure Element in a standard way. This could either be done directly via a contactless connection, remotely by OTI for PC-connected media, or over a mobile wireless network for NFC phones.

Once the software code is loaded (in manufacturing or post-issuance) in a Secure Element, PTOs can create one or several personalized applications from this code.

3.2. GlobalPlatform: The Standard for Smart Card Application Management

GlobalPlatform is a cross-industry standard.

GlobalPlatform is a generic, established, and widely accepted technology among various industry sectors, including payment, government, healthcare, and telecoms. Furthermore, GlobalPlatform technology has already been endorsed for application management in the NFC ecosystem.
Fig. 3-1: GlobalPlatform supports of one or many applications from different industries

GlobalPlatform is a standard for loading, installing and personalizing applications on Secure Elements.

GlobalPlatform card technology [0] provides a set of specifications for smart card application download, installation, personalization, and full life cycle management. GlobalPlatform specifications are applicable for smart cards in any form factor: a contactless key fob, a Secure Element in an NFC phone, a USB dongle, and et cetera. GlobalPlatform for smart card technology is independent of the card Operating System, but it is typically developed on top of Java Card technology.

GlobalPlatform systems technology [3] provides an IT standard for the back office part for all data exchanges between actors involved in managing an application in the smart card.
GlobalPlatform is a secure and non-intrusive approach for managing transportation applications.

GlobalPlatform is application independent and is a non-intrusive technology for transportation operators. It provides a way for application owners to securely manage the operations of loading, installing, and personalizing applications through a **Security Domain** connection. This connection has several characteristics:

- Mutual authentication between off-card entities and the Security Domain
- Integrity of commands
- Confidentiality of commands (in order to protect application code and data)

![Fig. 3-2: Installation phases of a transportation application with GlobalPlatform commands](image)

GlobalPlatform secure communication protocols can be used over any proximity or remote communication link, including a contact or contactless connection with the smart card, an Http(s) connection over-the-Internet, a 3G/GSM SMS or data connection over mobile wireless networks, and more. In 2009, this technology has been enhanced [1] to allow for end-to-end communications between an application provider and the application using the network of a third party (a good example of how this has been endorsed today is a bank creating an end-to-end security communication using the OTA Platform of a Mobile operator).
Once installed and personalized, the application can be used as usual. Specifically, any ticket vendor will be able to top-up a ticket on the application, as this type of operation is managed at the application level and does not involve the GlobalPlatform open framework on the card.

Each Application Provider can independently manage its own secure communication channel with the card, provided it is given a dedicated Security Domain.

Fig. 3-4: Example of concurrent GlobalPlatform Secure communication channels with the same card
3.3. **Improving Ticketing Interoperability and Intermodality**

GlobalPlatform can enhance transportation network interoperability by allowing for the coexistence of different local transportation applications on the same media. Application coexistence will enable passengers to use the same media in a multimodal journey through different EFM systems. This will be possible without requiring any modification in the acceptance infrastructure of the visited EFM systems or any clearing interconnection between the 2 EFM systems:

- When in PT network #1, the local EFM system will select application #1 in the media and use it accordingly
- When in PT network #2, the local EFM system will select application #2 in the media and use it accordingly

Moreover, on interactive media like an NFC phone, a set of commands allows the end-user to activate or deactivate contactless applications, namely, to make them visible or not to any contactless reader. This feature provides an additional benefit: by allowing the coexistence in the same media of contactless transportation applications with conflicting RF protocols parameters, all that is required is that they are not activated at the same time.

3.4. **Relying on Standards and Open Products**

When defining e-ticketing specifications, standards offer several advantages: sustainability of systems, modularity of components, interoperability of systems, provisioning of information to travelers, cost savings, and more.

Additionally, relying on an open standard for application download opens up the possibility of having the transportation applications downloaded by various services retailers outside the PTO, such as Mobile Network Operators or Tour Operators.

From the beginning, GlobalPlatform for Card technology has been designed to provide an open framework for application interoperability and portability, as well as to provide card vendor independence. Thus, to ensure that it measures up to these expectations, GlobalPlatform technology should be used on a Secure Element that supports the following additional card standards:

- The SE must be a microprocessor IC Chip supporting standard algorithms (DES, 3DES, AES, RSA)
- ISO 7816-4 for APDU command interface
- ISO 14443 for contactless protocol communication
- ETSI OTA specifications for remote mobile network access to UICC SE (only when SE = UICC)
- Java Card Run-Time Environment or other open multi-application card OS like Multos

This may require some transportation operators to migrate away from proprietary solutions that do not support the standard ISO 14443 protocol (Type A & B) and non-standard algorithms in order to be able to manage their application in an interoperable and multi-application media.

One of the direct benefits for PTOs as they move from dedicated transportation media—or even from transportation media that is specific to one network—to
GlobalPlatform-compliant media, is that doing so will favor competitive procurement because of the selection of standard and non-vendor-specific products.

### 3.5. Fulfilling Privacy Requirements

Thanks to its strong architectural concept, GlobalPlatform offers PTOs an excellent opportunity to meet all privacy challenges in Public Transportation solutions. And, based on the requirements set forth in section 2.3, privacy should be considered as a system-wide issue that can only be addressed in transportation applications if all actors follow strict rules toward compliance with shared privacy objectives:

- Operators need to understand and express requirements that sustain privacy-friendly business models
- Chip, card, and device manufacturers must incorporate appropriate Privacy Enhancing Technologies (PET) and primitives that permit privacy-by-design implementations
- Application and system designers should enable those privacy features in such a way so as to fully comply with legal frameworks and operational requirements

Ultimately, achieving privacy in e-ticketing applications requires an impact assessment of the whole fare collection system based on the following criteria:

<table>
<thead>
<tr>
<th>PIA Criteria</th>
<th>Definition</th>
<th>GlobalPlatform Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated access</td>
<td>Only legitimate applications have access to e-tickets (loading, validation fare collection, verification)</td>
<td>GlobalPlatform cryptography and selectable security levels enable authentication of the off-card entity</td>
</tr>
<tr>
<td>Non traceability</td>
<td>Individual traveler movements are not inferable through ticketing operations</td>
<td>GlobalPlatform access protocols provide full randomization of identifiers</td>
</tr>
<tr>
<td>Non linkability</td>
<td>Individual traveler cannot be profiled through the correlation of several application(s) data</td>
<td>By fully isolating Security Domains and encryption levels, GlobalPlatform architecture keeps application spaces and communication means separated</td>
</tr>
<tr>
<td>Limited data collection and retention</td>
<td>Account data and credentials are selectively used and time-limited for the purpose (billing, statistical recording)</td>
<td>To restrict sensitive data exposure, GlobalPlatform offers application designers unique tools to manage Card and application life cycle, Security Domain association, and privileges</td>
</tr>
<tr>
<td>Non observability</td>
<td>No personal data can be catch or derived from sniffing of OTA transactions with Automated Fare Collection</td>
<td>GlobalPlatform proposes up-to-date encryption mechanisms that ensure secure communication between cards and devices</td>
</tr>
</tbody>
</table>
User awareness and confidence

<table>
<thead>
<tr>
<th>(AFC) systems</th>
<th>Appropriate symbols and messages are displayed, clear user interfaces are proposed on system and personal devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amendment C of GlobalPlatform 2.2 foresees the user-based activation/deactivation of services that are exposed on the contactless interfaces (see Fig. 3-5)</td>
<td></td>
</tr>
</tbody>
</table>

GlobalPlatform aspires to become a unique reference in portable security. As such, the current value proposition relies on worldwide adoption and certification processes supported by the organization. By conforming to universally accepted privacy principles through a set of methods and tools, integrators would gain increased confidence that their GlobalPlatform-based solution would address potential privacy issues in sensitive Public Transportation applications and allow them to flexibly adapt to future amendments in legal frameworks everywhere.

![Activation and deactivation of contactless applications by end user](image)

**Fig. 3-5: Activation and deactivation of contactless applications by end user**

### 3.6. Securing Transportation Passes

During the process of elaborating the GlobalPlatform 2.2 specification (all amendments included), modern security standards have been widely adopted to raise the bar for potential attackers. This involves the definition of new secure channels to perform the secure loading of required keys and confidential data, as well as the secure loading and management of new applications.
GlobalPlatform aims to offer PTOs the security enhancements they need to protect their own businesses and revenues. At the same time, those enhancements should include appropriate measures to prevent end-user privacy breaches. GlobalPlatform will take care to not introduce security measures that would hamper or conflict with privacy goals discussed in § 2.3 and 3.5.

By design, GlobalPlatform allows for the coexistence of several Security Domains for different application domains, such as e-Gov or payment. GlobalPlatform also facilitates security management by the platform so that applications are not impacted by a security scheme upgrade required to fulfill the usual cryptology evolution.

GlobalPlatform is working to perform a remote personalization of a transportation application over a non-trusted network, such as the Internet. This enables confidential data, such as the transportation application keys or the customer’s personal data, to be provisioned in the customer’s device. To achieve this, GlobalPlatform provides end-to-end security, through secure communications channels, between the remote application management server and the Secure Element hosting the application.

Each communication channel is secured by a Secure Channel Protocol, which provides a level of security that is independent and distinct from the security of the underlying transportation network. GlobalPlatform Secure Channel Protocols are based on state-of-the-art, field-proven algorithms like 3DES, AES or RSA.

![Fig. 3-6: End to End Secure Communication with GlobalPlatform over different connection types](image-url)
One consequence of remote application management provided by GlobalPlatform is that it is very likely that PTOs will also look to provide remote services for ticket top-up once they are able to distribute the application over-the-Internet or over NFC phones. When a remote connection will be used to top-up tickets, the application security scheme must be used if available. If not, it is also possible to use a GlobalPlatform personalization script for updating the application, thus benefiting from GlobalPlatform security.

GlobalPlatform has also recently started a joint effort to define a new security certification composition model that certifies combinations of GlobalPlatform devices, GlobalPlatform applications and GlobalPlatform infrastructures.

### 3.7. Enabling the Usage of New Media in Transportation

With GlobalPlatform technology, PTOs can take full advantage of new multi-application media—like Secure Element in NFC phones, smart cards, or USB tokens—for transportation applications.

In multi-application environments, media are often not owned by the PTOs. This is the case with UICC Cards in an NFC phone, which can be used to store contactless applications from multiple business partners, but which remain the property of the Mobile Network Operator.

One consequence of using a third party SE is the need to identify SE technical capabilities and the SE owner. In an open world, the application provider should first identify the SE owner or the entity responsible for managing the SE.

- The SE owner then provides the business access rules and the card platform technical capabilities
- The card platform capabilities list is a standard XML profile [5] that describes all technical elements needed for the application provider to verify the compatibility of the transportation application

In order to cope with environments that have multiple business partners, GlobalPlatform technology defines standardized mechanisms for the manner in which the Security Domain is given to the Application Provider. The Application Provider then manages its application loading, installation and personalization in a completely confidential way vis-à-vis the SE Issuer or other Application Providers. The handover can be secured by using a Controlling Authority, the third party on-card certificate.
Fig. 3-7: Handover of Security Domain ownership by the SE Issuer to an Application Provider

Thanks to this GlobalPlatform mechanism, the Application Provider can manage its application with the same level of security as though the application were being managed on its own card.

GlobalPlatform supports a variety of business models and can be set up by the Card Issuer in the following ways to enable card content management:

- **Issuer Centric Model:**
  - Application loading and installation can only be managed by the Issuer
  - Once loaded and installed by the Card Issuer, application personalization can be managed by the Application Provider

- **Delegated Management Model:**
  - All application management operations can be performed by the Application Provider, but the Card Issuer must provide a pre-authorization token

- **Dual Management Model:**
  - Application Management operations can be freely performed by Application Providers without any preauthorization from the Issuer
  - Optionally, the Issuer can allocate a quota of memory space assigned to each Application Provider
3.8. **Benefiting from and Complying with a Cross-Industry Certification Process**

The smart media management infrastructure specified by GlobalPlatform consists of multiple components:

- The Issuer Smart Card Management System
- The Application Provider Host
- The Download Server
- Customer Media Acceptance Devices
- The Customer Medium itself

Since it is an open standard, the implementation will most likely be a multi-vendor architecture. For example, consider a situation where the customer media is implemented by different manufacturers and the components in the chain of application download are not delivered by a single vendor. With the existence of the GlobalPlatform Compliance & Certification Program, it is guaranteed that the final composite system will effectively work together.

Nowadays, certification within a single industry is usually well organized. The standardized post-issuance application download will be used by all sectors in the industry: Government, Banks, Mobile Network Operators, and Transit. This makes the importance of certification even more important.

The Compliance and Certification Program answers the following questions:

- What does the product do?
- How was this tested?
- Who performed the testing?

Required for the ‘what’ answer is a specification that is unambiguous, consistent, and as complete as possible. The published specification must provide a clear level of interoperability.

The ‘how’ answer requires a test specification that is unambiguous, consistent, and as complete as possible. To enhance the interoperability and the quality of the test suites, GlobalPlatform provides configurations that are an implementation guide of a specification for a specific market. Based on these configurations, the compliance program generates more detailed test suites that are used to verify the product compliance.

The ‘who’ question is solved by GlobalPlatform qualification of Lab Services.

The specification of the system behavior and the tests are iterative processes. Each new implementation of the standard discovers open points in either the behavior specification or the test specification. The best result is reached asymptotically. To maximize the benefit of the certification program, the transit industry should be represented in this cross-industry environment and bring test cases that are representative of the public transportation market.

To make it easier to deploy value-added services, GlobalPlatform has been working closely with other standards bodies to develop a new certification scheme for Secure Elements.
Currently, the security certification scheme for each application requires a check of both the platform and the application. Thus, if two applications are loaded, the hosting platform will be checked twice.

The new security certification model will make it possible to first certify the card platform (let us call this P1) with the transportation application. When this application is loaded within another platform P2, the issuer of platform P2 will sponsor the certification by checking the differences between P1 and P2.

![Composition Model](image)

**Fig. 3-8: Certification by Composition model**

The certification may support functional, security, and performance checks. Minimum requirements will become very important to verify that the platform is providing the correct level of features to the application and that the application will not be a threat when loaded in the platform.

GlobalPlatform’s objective is to publish these composition rules between the application and the platform in order to facilitate the start of a new market of certified SE and compatible applications.

### 3.9. Managing Additional Services

Using GlobalPlatform technology for managing the application download process into transportation media can also allow each PTO to enrich its existing service offering by adding new applications and services on the media after its issuance.
Thanks to the GlobalPlatform framework, PTOs can benefit from standardized processes for application life cycle management (including load, install, activate, delete, and etc.) and can leverage the same technology to remotely manage their entire application portfolio independently of the communication link with the Secure Element (whether this be over a Mobile wireless network, over the Internet, or over a contactless reader).

The costs associated with setting up an application download platform can then be paid off—not only on a single ticketing application, but also on the complete portfolio of urban mobility applications that can be seamlessly deployed thanks to GlobalPlatform technology.

This will allow PTOs to play a pivotal role in rolling out new urban mobile services that will complement their ticketing applications, and, in the case of an NFC phone, even provide traffic information or a trip planner application.

Fig. 3-9: Examples of multiple urban services on a GlobalPlatform card
SECTION 4: Conclusion

From a GlobalPlatform technical perspective, loading a transportation application is similar to loading any other type of application. But, it is worthwhile to note that the transportation industry will bring new use cases that require a high level of performance for contactless transactions.

The implementation path is clearly defined:

- The remaining challenges for expanding transportation application usage on non-dedicated media are commercial and business issues. An extension is also needed in the field of the technical aspect to simplify the OTA provisioning and management with a strong compliance program, Implementation Guide, and detailed card profile.
- The technical impact for transportation operators is either to provide a Java Card applet version of their transportation application that is compliant with the GlobalPlatform personalization process, or to cooperate with an application provider to include their transportation service requirements in a Java Card applet.
- The business impact for transportation operators will likely be a bit more difficult to handle but involves the following two steps:
  - Building a business agreement with SE owners and either providing them with the application to download, or entering into a business agreement with an application provider to provide the application to download
  - Identifying and building a business agreement with a TSM to handle transportation application personalization

Ultimately, there are many benefits to PTOs that leverage GlobalPlatform technology when implementing an Electronic Fare Management system. These benefits result from a standardized answer to many of the PTO’s expectations, such as greater interoperability, open procurement for customer media, seamless deployment of new services, and acceptance of contactless media.
APPENDIX A: References and Standards Bodies

<table>
<thead>
<tr>
<th>Standard / Specification</th>
<th>Description</th>
<th>Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlobalPlatform Card v 2.2</td>
<td>Card specification from GlobalPlatform.</td>
<td>[0]</td>
</tr>
<tr>
<td>GlobalPlatform Confidential Card Content Management – Card Specification v2.2 – Amendment A v1.0</td>
<td>Defines a mechanism for an Application Provider to confidentially manage its own application when using a third party communications network.</td>
<td>[1]</td>
</tr>
<tr>
<td>UICC Configuration v1.0</td>
<td>An implementation guide for deploying GlobalPlatform Card Specification v2.2 within the mobile services sector and managing the secure delivery of new services over-the-air. It outlines the behavior of each and every actor involved in a UICC implementation, how they should be represented, and a summary of their roles and responsibilities in a variety of business models.</td>
<td>[2]</td>
</tr>
<tr>
<td>GlobalPlatform Messaging Specification v1.0</td>
<td>Specifies the data exchange between actors involved in the card and application customization process</td>
<td>[3]</td>
</tr>
<tr>
<td>ISO 24014-1 – Interoperable Fare Management System – Part 1: Architecture</td>
<td>Provides the basis, on a national and international level, for the development of Interoperable Fare Management Systems (IFMSs) that are multi-operator, multi-service, and public service transportation (including subways). The objective of ISO 24014-1:2007 is to define a reference functional architecture for IFMSs and identify the requirements that are relevant in order to ensure interoperability between several actors in the context of the use of electronic tickets.</td>
<td>[4]</td>
</tr>
<tr>
<td>GlobalPlatform Systems Profiles</td>
<td>In conjunction with the Systems Scripting Specification, this specification specifies in XML all the information required for the card customization process, including data preparation and personalization.</td>
<td>[5]</td>
</tr>
</tbody>
</table>
## APPENDIX B: Publications

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
<th>Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>UITP</td>
<td>UITP Position paper: “Everybody local, everywhere” – Electronic ticketing interoperability and Fare Management cooperation.</td>
<td>[6]</td>
</tr>
<tr>
<td>IFM Project</td>
<td>D3.1 - State of the art on interoperable media and multi-application management – <a href="http://www.ifm-project.eu">www.ifm-project.eu</a></td>
<td>[7]</td>
</tr>
<tr>
<td>Department for Transport (UK)</td>
<td><a href="http://www.ifm-project.eu">Developing a strategy for smart and integrated Ticketing</a></td>
<td>[8]</td>
</tr>
</tbody>
</table>
## APPENDIX C: Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFC</td>
<td>Automated Fare Collection</td>
</tr>
<tr>
<td>EFM</td>
<td>Electronic Fare Management</td>
</tr>
<tr>
<td>IFM</td>
<td>Interoperable Fare Management [4]</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>OTA</td>
<td>Over-The-Air</td>
</tr>
<tr>
<td>OTI</td>
<td>Over-The-Internet</td>
</tr>
<tr>
<td>PET</td>
<td>Privacy Enhancing Technologies</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Assessment</td>
</tr>
<tr>
<td>PT</td>
<td>Public Transportation</td>
</tr>
<tr>
<td>PTO</td>
<td>Public Transportation Operator</td>
</tr>
<tr>
<td>SD</td>
<td>Security Domain</td>
</tr>
<tr>
<td>SE</td>
<td>Secure Element</td>
</tr>
<tr>
<td>SSD</td>
<td>Supplementary Security Domain</td>
</tr>
<tr>
<td>TA</td>
<td>Transportation Authority</td>
</tr>
<tr>
<td>TO</td>
<td>Transportation Operator</td>
</tr>
<tr>
<td>TSM</td>
<td>Trusted Service Manager</td>
</tr>
<tr>
<td>UICC</td>
<td>Universal Integrated Circuit Card</td>
</tr>
<tr>
<td>UID</td>
<td>Unique Identification</td>
</tr>
<tr>
<td>UITP</td>
<td>Union Internationale des Transports Publics (International Association of Public Transportation)</td>
</tr>
</tbody>
</table>
APPENDIX D: Definitions

Single Ticket:
A single ticket entitles the user to travel one time by public transportation—in one route direction or to one destination.

Season Ticket:
In public transportation, a season ticket allows the user to travel by public transportation an unlimited number of times within a prescribed period of time. Season tickets are typically sold for a day, week, month or year, but usage rights vary. In the most limiting instances, a season ticket may allow only for travel between two points (A to B) and even limit travel to a single operator and route (assuming that there are multiple operators competing in this area). At the other extreme, a season ticket may allow unlimited travel within a geographic area, allowing users to select any method of transportation (bus, tram, train etc.) and operating company.

Fares:
A fare is the fee that a passenger pays in order to make use of a public transportation system.

Concessionary Fares:
Concessionary fares are discounted fares that are available to people who qualify according to some specific conditions (low income, age, group membership, and etc.); these concessions may be offered for all journeys over a period of time or for individual journeys.

Smart Media:
Smart media refers to a portable object that has a contactless interface and hosts a Secure Element. Smart media can be initialized with one or more applications.

Intermodality:
Intermodality is a characteristic of a transportation system that allows at least two different operators’ transportation modes to be used in an integrated manner in a door-to-door transport chain.

(Ticketing) Interoperability:
Interoperability involves using several transportation networks that are run by different operators during a single journey. Alternatively, it can involve using the same transport mode over different transport networks. For example, one could take a regional train, followed by urban transport—all the while using the same smart media. Note that ticketing interoperability is not necessarily achieved by technical interoperability between the different EFMs; it can also be achieved by the coexistence of different ticketing applications on the same media.
## Appendix E: Table of Figures

| Fig. 3-1: GlobalPlatform supports of one or many applications from different industries | 13 |
| Fig. 3-2: Installation phases of a transportation application with GlobalPlatform commands | 14 |
| Fig. 3-3: Same GlobalPlatform script for multiple types of remote links | 15 |
| Fig. 3-4: Example of concurrent GlobalPlatform Secure communication channels with the same card | 15 |
| Fig. 3-5: Activation and deactivation of contactless applications by end user | 18 |
| Fig. 3-6: End to End Secure Communication with GlobalPlatform over different connection types | 19 |
| Fig. 3-7: Handover of Security Domain ownership by the SE Issuer to an Application Provider | 21 |
| Fig. 3-8: Certification by Composition model | 23 |
| Fig. 3-9: Examples of multiple urban services on a GlobalPlatform card | 24 |