



An Open Standard For Next-Generation Transit Fare Collection



The Open Standard for Public Transport (OSPT) Alliance is the outgrowth of an industry initiative launched in January 2010 by four leading technology companies— Giesecke & Devrient, Infineon Technologies, INSIDE Secure and Oberthur Technologies—to provide a new, more secure and more flexible solution for the next generation of public transportation fare collection systems.

As part of its mission, the OSPT Alliance has developed the Cipurse™ open security standard to foster the next generation of more secure, cost-effective, scalable and extensible transit fare collection systems. Cipurse addresses the demand by transit authorities for new, sophisticated fare collection systems that offer greater capabilities and convenience, such as enabling a rider to use a ticket seamlessly— in different cities, across several modes of transport or even different regions and systems—instead of having to buy different tickets each time.

This paper provides an overview of the OSPT Alliance and the Cipurse open security standard, as well as some background on the evolution of the transit fare market.

The Evolution to Next-Generation Fare Collection Systems

Public transport is one of the fastest growing smart card markets, and is currently being reshaped. Transit operators must combat growing security threats while identifying new revenue sources and enhancing fare collection, but today's proprietary systems are limiting their options.

In the past, dedicated transport schemes based on closed-loop applications were established in a number of cities throughout the world. They each employed their own proprietary fare media, creating public transport islands that were not interoperable with other transport systems. The data management on the fare media token and the interface to access the data were completely different from one system to another.

Until recently, it was difficult to cost efficiently implement advanced and complex security. Over the last decades, a widely used proprietary technology was installed in fare collection systems worldwide, which, over time, formed a legacy infrastructure. Based on a contactless memory storage device with simple mechanisms for access control that provides only a basic level of security, these proprietary systems were selected because of their broad availability and the use

of pre-integrated components – readers, cards, tickets, etc. – that assured interoperability. But since the security offered by this widely used proprietary standard was compromised in 2008, demand has increased significantly for systems with more advanced, open standards-based security.

Today, transport systems are migrating to microcontroller-based schemes that are converging with adjacent applications and technologies such as open-loop credit/debit payment cards, micropayments, multi-application cards and near field communication (NFC) mobile phones and devices. These new applications demand much higher levels of security than provided by today's transport schemes. In addition, public transport agencies have become more concerned about increasing their revenues, and are developing new business models to realize new revenue sources. However, they are coming to realize that proprietary, single-vendor technologies are limiting their flexibility while increasing their risk and costs. At the same time, they want their customers to be able to use their transit tickets seamlessly across different transit systems.

All these changes and trends clearly indicate that this market is at a turning point. A new generation of transport systems is needed and will be the foundation of transit fare collections applications for years to come. Silicon development has progressed significantly over the years. Today, even complex security algorithms such as the 128-bit advanced encryption standard (AES-128) can be implemented cost-effectively, and state-of-the-art silicon manufacturing processes enable new schemes to meet today's security demands.

There now is an opportunity to standardize important parts of the fare collection system – the data management, the media interface, the security, etc. – to allow greater flexibility, interoperability and cost-effectiveness while improving security and providing greater convenience to customers. Proprietary technologies – especially if not made widely available under fair and reasonable terms – and limited sources for smart card ICs and other vital system components will hamper this

opportunity. Furthermore, the emerging NFC technology will make further demands for open, future-proof solutions for transit fare collection.

The Open Standard Approach

Open standards drive numerous benefits to the transport fare collection market: vendor neutrality, cross-vendor system interoperability, lower technology adoption risks, higher quality, and improved market responsiveness – all resulting in lower operating costs and greater flexibility for transport system operators. Unlike systems based on proprietary technologies that cost more to acquire, deploy and maintain, limit choices and are potentially less secure, an open standard for developing secure transit fare collection solutions enables delivery of more cost-effective, highly secure, flexible, scalable and extensible solutions.

The Open Standard for Public Transport (OSPT) Alliance was formed to define Cipurse, a new open standard for secure transit fare collection solutions. The Alliance's goals also are to provide industry education and workgroup opportunities, to act as a catalyst for promoting the development and adoption of innovative, next-generation fare collection technologies, applications and services, and to ensure that these solutions address the needs of the transit fare collection community.

The Alliance also will work to establish an ecosystem of transit operators, technology suppliers, consultants and integrators, government agencies and mobile product and service providers, as well as other industry associations, to develop new, interoperable transit fare collection solutions based on open-standard security that are able to support both current and future systems.

This new ecosystem will offer transit operators the opportunity to choose from among a number of vendors, consultants and integrators to help them deploy or upgrade to a more secure and cost-effective fare collection system. Government agencies that need to evaluate bids for new or upgraded transit payment systems will have access to a much broader array of solution vendors and partners delivering a wider range of innovative, flexible, secure transit fare collection solutions. For transit system consultants and integrators, the ecosystem will bring together a greater assortment of vendors offering more product choices and richer capabilities than available with proprietary systems.

The Cipurse Standard

The Cipurse open security standard is designed to address the need by local and regional transit authorities for future-

proof fare collection systems with more advanced security than is currently in use. It provides a platform for securing both new and legacy transit fare collection applications, and has the potential to be used within existing application frameworks around the world.

Cipurse builds upon existing, proven, open standards—the ISO 7816 smart card standard, as well as the 128-bit advanced encryption standard (AES-128) and the ISO/IEC 14443-4 protocol layer—and its advanced security concept can be implemented in low-cost silicon. Its advanced authentication scheme is resistant to most of today's electronic attacks.

Its advanced security mechanisms include a unique cryptographic protocol that encourages fast and efficient implementations with robust, inherent protection against differential power analysis (DPA) and differential fault analysis (DFA) attacks. Because the protocol is inherently resistant to these kinds of attacks and does not require dedicated hardware measures, it eliminates the need by card and chipmakers for a massive overhead of software and hardware countermeasures against these attacks. This unique advantage makes it possible to cost-efficiently guard against counterfeiting, cloning, eavesdropping, man-in-the-middle attacks and other security risks that threaten the integrity of transit fare collection systems.

In addition to these advanced security mechanisms, the Cipurse standard defines a secure messaging protocol, four minimum mandatory file types and a minimum mandatory command set to access these files. It also specifies encryption keys and access conditions. The standard is RF layer agnostic, and includes personalization and life cycle management, as well as system functionality to provide interoperability and fast adoption.

The Cipurse standard also provides a security concept and guidelines, providing an implementation "cookbook" for transit agencies, system integrators and others to develop the overall system security design. Further, technology providers are free to add functionality outside the common core to differentiate their products in the marketplace and provide stakeholders with greater choice in selecting solutions as long as they do not jeopardize interoperability of the open standard core. Because of its advanced authentication and secure messaging protocol, as well as its independent ISO 7816 command set, the Cipurse standard can address a variety of different applications. From products such as simple low-end memory chip cards, to stand-alone smart cards up to multi-application cards and NFC mobile phones, the

Cipurse standard's flexibility and interoperability makes it unique for public transport. Furthermore, addressing and expanding the low-end market of single trip or limited use tickets is easy. This scalability across transit fare form factors, support for emerging NFC mobile phones and other devices and multi-vendor support sets the stage for a truly future-proof solution.

Infrastructure migration costs will be minimized as many of the needed features (command code and AES) are already used and supported by many systems. The commonly used ISO 7816 smart card standard has existed for many years and is widely supported by microcontroller cards. Standard commands, such as Mutual Authenticate or Update Binary File, ease integration into existing application schemes. The ISO 14443-4 protocol layer used in the standard makes reuse of already implemented features possible, while accelerating integration of new functionality. AES-128 is optimized for software integration and can be added easily to any reader firmware or back-end system.

The OSPT Alliance is currently developing the initial version of the Cipurse standard, as well as documentation and reference implementations, which will enable technology suppliers to develop and deliver innovative, more secure and interoperable solutions for cards, stickers, fobs, mobile phones and other consumer devices, as well as infrastructure components for transit fare collection systems. It is planned that the Cipurse standard will be governed by an independent body, and standards compliance testing, interoperability testing and performance testing will be performed by an independent test authority.

Conclusion

The Cipurse standard provides an open alternative to the proprietary solutions currently available, bringing to the public transport market, for the first time, all the benefits that result from an open, competitive marketplace. Unlike systems based on proprietary technologies that limit choices, are potentially less secure and cost more to acquire, deploy and maintain, products that conform to the Cipurse standard will include the most advanced security technologies, support multiple applications, help ensure compatibility with legacy systems and be available in a variety of form factors. The open Cipurse standard will promote vendor neutrality, cross-vendor system interoperability, lower technology adoption risk, higher quality and improved market responsiveness, all of which result in lower operating costs and greater flexibility for transport system operators.

The success of the Cipurse standard depends on the contribution of all the stakeholders in the public transport ecosystem. The initial OSPT Alliance members welcome the participation of new members from all segments of the transport industry—component and system suppliers, integrators, transport agencies, consultants and others—to contribute their experience to OSPT and the Cipurse standard. Only by including all stakeholders in the public transport ecosystem will this initiative be successful and complete.

For additional information:

Patrick Corman
OSPT Alliance
+1-650-326-9648
info@osptalliance.org

Dr. Roland Magiera
Adviser, Transit Segment
Marketing Government Solutions
Giesecke & Devrient
+ 49 (0)89 4119 2978
roland.magiera@gi-de.com

Ramona Mache
Business Development Manager
Chip Card & Security ICs
Infineon Technologies AG
+49 (0)89 2342 6862
ramona.mache@infineon.com

Herve Roche
Marketing Manager, Payment Business Line
INSIDE Secure
+33 (0)4 42 39 63 00
hroche@insidefr.com

Nicolas Raffin
Head of Product Marketing, Payment & Transport Product Line
Card Systems Division
Oberthur Technologies
+33 1 47 85 42 33
n.raffin@oberthur.com