cipurse™

An Open Standard for Next-Generation Transit Fare Collection

ospt™ ALLIANCE

OSPT Alliance
Prinzregenten Str. 159
D-81677 Munich
Germany

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, OSPT Alliance hereby disclaims any and all warranties and liabilities of any kind, including without limitation, warranties of non-infringement of intellectual property rights of any third party.

Information

For further information, please see OSPT Alliance Website: www.osptalliance.org or contact info@osptalliance.org.

We listen to your comments:

We are constantly striving to improve the quality of all our specifications and documentation. If you find any information that is missing or appears to be incorrect, please use the contact section to inform us. We appreciate your assistance in making this a better document.

Please be aware of that for the implementation of the CIPURSE specification into products further IPR licenses may be required:

- CIPURSE cryptography IPR can be licensed from the OSPT IP Pool GmbH. Contact: info@ospt-ip-pool.com.
- Transaction mechanism is covered by additional third party IPR, not licensable from the OSPT IP Pool. It is the responsibility of the implementer to contact the IPR owner

1 Introduction

OSPT Alliance is a vendor neutral, global association, which is helping the transit community to move toward the next generation of secure, cost-effective, and flexible fare collection solutions. It is open to companies worldwide to join as members, including vendors, integrators and PTAs.

Our charter is to define and offer an open standard for secure transit fare collection solutions, while providing industry education, creating workgroup opportunities, and supporting the development and adoption of innovative fare collection technologies, applications, and services. We are also building a global ecosystem of transit operators, transit consultants and integrators, technology solution providers, and government agencies to stimulate development and delivery of next-generation fare collection solutions.

The OSPT Alliance welcomes new members as we work together in an open forum to provide the transit industry and adjacent ecosystems with a broad range of innovative solutions.

As part of its mission, it provides CIPURSE, an open standard solution, which is independent of both the hardware and hardware provider and can be used in any ecosystem or market.

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.

2 The Evolution to Next-Generation Fare Collection Systems

Public transport is one of the fastest growing smart card markets, and is currently facing multiple pressures. Transit operators must combat growing security threats while identifying new revenue sources and enhancing fare collection. In the face of these demands, many of today' s proprietary legacy systems are limiting their options to respond in an agile and flexible manner.

Most AFC systems operating today are based on proprietary closed loop technology. That creates public transport 'islands' that offer no interoperability with either other transport systems or adjacent ecosystems. The data management on the fare media token and the interface to access the data are often completely different from one system to another. As interest in smart cities and urban mobility grows, that lack of ability to interface with applications such as ride sharing and parking will become particularly problematic.

In the past, it has been difficult to implement advanced and complex security cost efficiently within some of these proprietary systems, particularly those using simpler, lower specification fare media. This has been evidenced by several well publicized attacks on ticketing systems. As the abilities and successes of attackers grow, across all sectors, not just transit, it becomes increasingly important that fare media, which in some cases may carry high value items such as season tickets, must make use of state of the art security.

Today, transport systems are migrating to not just higher specification cards but mobile technology too that can facilitate convergence with adjacent applications such as micropayments, urban mobility and identity. These new applications demand much higher levels of security than is 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. As a result, they are coming to realize that proprietary, single-vendor technologies limit their flexibility while increasing their risk and costs. At the same time, many want their customers to be able to use their transit tickets seamlessly across different transit modalities.

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. 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 vastly improving security and providing far 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 move to mobile will make even greater demands for open, future-proof solutions for transit fare collection.

3 The Open Standards Approach

Open standards provide numerous benefits to the transport fare collection market: vendor neutrality, cross-vendor system interoperability, lower technology adoption risks, higher quality products through vendor competition, and improved market responsiveness – all resulting in lower operating costs and greater flexibility for transport system operators. Unlike systems based on proprietary technologies that can cost more to acquire, deploy and maintain, limit choices and are often 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 promotes CIPURSE, the open standard for secure transit fare collection solutions and more. The Alliance also provides industry education and working group opportunities, acting as a catalyst for promoting the development and adoption of innovative, next-generation technologies, applications and services in fare collection and adjacent ecosystems, and ensures that these solutions address the needs of all relevant communities.

The Alliance also forms 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 supports both current and future systems.

This ecosystem offers transit operators the opportunity to choose from among multiple 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 now 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 and those in adjacent ecosystems, OSPT Alliance brings together a greater assortment of vendors offering more product choices and richer capabilities than is available for proprietary systems.

4 The CIPURSE Standard

The CIPURSE open security standard addresses the need of local and regional transit authorities for future-proof fare collection systems with advanced security. It provides a platform for securing both new and legacy transit fare collection applications, and can be easily integrated into existing fare collection systems 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 and authentication system is not only superior to that used in proprietary systems but can also be implemented in low-cost silicon as well as on mobile.

Its 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 cutting-edge 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.

Furthermore, 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 providing 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 use cases. From media 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 uniquely suited for public transport and other applications needing high levels of security.

Moreover, 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 NFC mobile phones and other devices and multi-vendor support sets the stage for a truly future-proof solution.

Infrastructure migration costs are minimized as many of the needed features 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 re-use 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. For more information about how to manage integration into existing systems easily and quickly, please read the OSPT Alliance white paper Integrating CIPURSE™V2 into an Existing Automated Fare Collection System, available from the OSPT Alliance website.

The CIPURSE standard, together with its documentation and reference implementations, enables 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 a living, breathing standard, with OSPT Alliance actively engaged in advancing and developing the standard to meet ecosystem requirements. Those interested in learning more are invited to apply for an evaluators' license and CIPURSE Software Development Kit.

The CIPURSE standard is governed by an independent body, and its standards compliance testing, interoperability testing and performance testing are performed by an independent test authority.

5 Conclusion

The CIPURSE standard provides an open alternative to the proprietary solutions currently available, bringing to the public transport market 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 OSPT Alliance welcomes the participation of new members from all segments of the transport and neighboring industries—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 continue to grow and succeed.

For additional information about how using CIPURSE can benefit you or your clients, please visit the OSPT Alliance website at www.osptalliance.org or contact:

Laurent Cremer

Executive Director

OSPT Alliance

+33(0) 695 443 652

+33(0) 625 728 099 (mobile)

laurent.cremer@osptalliance.org

www.osptalliance.org

An Open Standard for Next-Generation
Transit Fare Collection