SRPc

Secure Remote Payment Council

OPEN SECURE PAYMENTS STANDARD (OSPS)

SOCIETAL COST BENEFITS FOR OSPS FRAMEWORK – A WHITE PAPER

January, 2018

As the payments world continues its evolutionary path supporting increased transaction volumes in the online and mobile environments, the fundamental payment system architecture will prove to be limiting and woefully inadequate. The current payment infrastructure has not kept pace with these changing needs. Incremental, layered improvements such as PCI, EMV®, tokenization, 3D-secure and other techniques are not keeping up with the needs of today's environment.

EMV implementation in the US has hampered both issuers and merchants. Much of its original design was meant to ameliorate poor and expensive telecommunication access, which was substantially less developed than today. With this constraint gone, we should leverage the ability of the chip to handle variety and complexity, allowing new interaction models that use encryption and peer-to-peer models, instead of the fixed, command and control infrastructure that is prevalent in the marketplace today.

Furthermore EMVCo, the organization that manages the EMV Specifications and related testing processes, provides no implementation governance. EMVCo is governed by six global brands rather than an independent body where there is equal ownership (e.g., X9, ANSI, ISO, etc.). EMVCo does not get involved in how the specifications are implemented, to the detriment of global interoperability and ubiquity. Current implementations of payment technologies continue to stifle innovation as a result of this lack of governance.

The solution lies in the adoption of an open industry standards for payment security. Open Secure Payments Standard (OSPS) is the response to an industry call for a flexible and secure framework to support multiple environments and payment types, providing an alternative implementation path for protecting sensitive data other than that which is currently promoted in the market place.

New Paradigm

OSPS provides new ways of securing the traditional payments business, focusing on protection of data. The OSPS framework supports interoperability while leveraging the existing payment infrastructure and expanding stakeholder options. The framework operates in a backward-compatible mode with EMV, supporting the co-existence of EMV Personally Identifiable Information (PII) and Personal Account Number (PAN) data with the OSPS self-protecting card data. But the key differentiator in the framework lies in the multiplicity of transaction message routing options it supports. For example, BINs can ride on the existing rails or alternative and/or direct routing can also use Uniform Resource Locator (URL) tags, Routing Transit Number (RTN), or mobile phone numbers to access the issuer for authorization. The framework also enables direct routing capabilities to access any processor or debit network for authorization based on the preferred transaction address.

Societal Cost/Benefits Tenets

The major cost/benefits of an open standards approach to payment security is its ability to provide flexibility and choice where healthy competition is fostered by continued differentiation and innovation.

- OSPS defines a technical model using an open systems approach for merchants, networks, processors, and issuers to have flexibility to use an open systems approach reducing many of the constraints of legacy infrastructure and restrictive business rules. OSPS will not prevent payment stakeholders from exercising their option to leverage the existing infrastructure and business constraints.
- OSPS leverages the latest technology that innovators are using, specifically peer-to-peer access models. This will encourage easier participation by Internet innovators for Internet payments. These new business and value propositions are simpler and no longer constrained by legacy processes founded on older, less-sophisticated systems.
- OSPS eschews the use of a PAN as a routing token. Instead OSPS, through peer-to-peer access and encryption among merchants, issuers, and designated third party processor agents allows these parties to define how the card/device and the cardholder are identified and authenticated.
- OSPS supports enhanced security, enabling issuer choice. This model works effectively, as evidenced by OAUTH which has been successful as the most used application protocol supporting content exchange between Internet content and social media providers.
- OSPS offers consumer protection benefits as the technology removes consumer identification data from the authorization transaction.
- OSPS simplicity is non-threatening in itself, open and flexible.
- OSPS is not, nor will ever be, binding to anyone. It is a participation standard, representing an attractive set of ideas.

Major Benefits

Open standards foster innovation, encourage competition and promote commoditization. Compatible with existing EMV specifications, the OSPS framework is superior for the following reasons:

- OSPS provides ways to standardize the industry for increased security and protection of PII data. The framework accommodates more flexible rules, simplified technology implementations, broader pricing options, and cardholder benefits.
- OSPS encourages innovation and competition, providing new ways to engage and compete for this business, resulting in lower costs to end users.
- OSPS frees stakeholders from excessive costs associated with proprietary or closed specifications. Innovators, developers, and manufacturers are not saddled with the burden of meeting requirements they have no influence over, promulgated by entities with vested interests.

A comparative assessment of the EMV standard vs. the OSPS framework further highlights the societal benefits of an open standard.

EMV	OSPS
EMV does not protect data stored on the Chip including but not limited to the PAN.	OSPS is secure. It protects the PAN and other sensitive data.
EMV is a Proprietary Standard. It lives to serve the interests and profitability of its owners.	OSPS is an Open Standard. It lives to serve consumers and the entire payment industry.
EMV was created 25+ years ago to solve problems that no longer exist, like substandard and costly communication.	OSPS solves modern problems, like data breaches.
EMV requires certifications and limits the number of qualified laboratories.	OSPS does not derive profit by mandating certifications, nor does it artificially limit those who offer testing tools or methods.
EMV discourages innovation. More secure, less expensive security methods are not allowed.	OSPS encourages innovation, better security and least cost transaction routing.
EMV shortfalls require costly mitigation processes such as PCI.	OSPS eliminates the need for PCI because the card or payment device is able to protect itself.

Why is the Timing Right Now?

PCI compliance costs all participants in the payments ecosystem hundreds of millions of dollars annually. The global card brands control this environment. Taking sensitive PII data out of the equation remediates fraud problems with consumer identification and renders PCI unnecessary.

Payments economics have changed dramatically in the past few years. Financial institutions have seen their net revenue from payments decrease. Merchants don't believe their costs have decreased enough and continue to look for ways to reduce payments cost even further. Both agree that transaction processing costs should be reduced. New payment initiatives such as "Faster Payments" may move from P2P to POS further changing the payments business case.

The time is now to put an architecture in place that better serves the needs of emerging digital and mobile commerce environments, as well as the physical space.

The early adoption and onset of emerging technologies such as next generation tokenization and 3D-secure continue to be implemented in a manner that takes away routing choices from merchants that accept payments through those backbone technologies, for example, tokenization used in the context of in-app purchases, card-on-file and checkout through a pay button. The "standards" underlying these emerging technologies are owned by entities that implement them in a manner by placing business constraints on the use of those technologies. Such implementations violate the very principles of ubiquity and interoperability that are the fundamental tenets of the standards body. The implementation of the standards leads to proprietary implementations and essentially lack any governance or enforcement of standards adherence.

Challenges with the OSPS Approach

The introduction of new things in the marketplace has the potential to increase costs and complexity for all stakeholders in the ecosystem, thereby causing adoption problems for the OSPS framework.

Support for a broad range of encryption and tokenization options raises integration questions. For example, the current implementations of the EMVCo tokenization specification creates issues with debit routing choice. While the specifications underlying tokenization do not directly create these routing challenges, current implementations of tokenized, card-not-present transactions such as in-app, card-on-file and pay button transactions don't appear to allow such choices Similarly, card BINs, URLs, and RTNs are all separate channels. Can alternative transaction messaging be supported in the ecosystem without burdening stakeholders with significant retrofitting cost?

The cost / benefits may not be explicitly quantifiable, but we believe everyone gets some gains. While we believe the whole system would be better off, there are concerns that no single party gains enough to offset the negatives to the current situation with global brands. We believe the OSPS will challenge the proprietary payment implementations through the existing global brands by releasing the stronghold on BIN ownership by the front-facing card brand.

Spurring Adoption

The industry-wide cost/benefits of the OSPS framework are structured around an open management concept based on standards, protocols and minimum requirements to maintain interoperability. So the next question is how do we spearhead adoption?

There are a couple of examples of this construct in the market today that can serve as models. ANSI and ISO are accredited standards bodies that promote open, global standardization for specifications and requirements for the payments industry. The Internet Engineering Task Force (IETF) maintains open standards for internet engineering, but done with a light hand. The IETF attempts to foster broad consensus about how the Internet interoperates. It is a standard at the lowest level, and supports the vast diversity of the Internet at the highest level. Another example is Financial Innovation Now, an organization which endorses open standards for authentication systems.

We believe that endorsement by an accredited standards body will be key to the successful adoption of the OSPS framework. Our immediate plan is to reach out to standards groups and engage in conversations with organizations whose charter supports the development of open industry standards for security in the payments environment to determine the optimum governance structure to promote adoption.

OSPS is a way to define a more rational future. This technical framework redefines the future of payments, so that the payments industry can move in that direction on their own terms. At its core, OSPS builds consensus on the foundation of transaction message processing by embracing the use of open standards allowing all industry stakeholders a seat at the table in the decision-making. We must create an environment that is based on an open standard and then let users develop it.

The SRPc invites all interested payments industry stakeholders to participate in the development of this open standard framework. Contact us at info@SecureRemotePaymentCouncil.org for more information.

About the Secure Remote Payment Council

The Secure Remote Payment (SRPc) is a nonprofit, inter-industry trade association that supports the growth, development and market adoption of debit based internet eCommerce and mobile channel payment methods that meet or exceed the security standards for pinned based card present payments. It will accomplish this by encouraging and supporting those activities that accelerate the implementation, adoption and promotion of these payments. The SRPc's members include merchants, financial institutions, merchant processors, issuer processors, payment brand companies, payments authentication hardware providers, payments authentication software providers and payments consultants. This document does not necessarily express the views and opinions of every member of the SRPc. For additional information, visit www.secureremotepaymentcounci.camp8.org