

FAQs

What is the SPVA?

The SPVA is a non-profit organization that works with the multiple stakeholders of the payment value chain. Its aim is to develop an end-to-end security framework and to enhance security elements of payment solutions which protect cardholder information and defend merchants and acquirers against security breaches, while reducing fraud and lowering risk for all electronic payment stakeholders.

Why was SPVA formed?

The world of electronic commerce has changed: overall complexity has increased and payments have gone global, bringing a new set of security and regulatory challenges and making life more demanding for merchants and acquirers to implement and manage secured and cost effective payment solutions.

The multiplicity of rules makes it very difficult for all stakeholders to have a common understanding of the whole payment security value chain. Unless all aspects of security are well understood, it is not practical to expect that compliant and effective security solutions are in place to protect everyone against future risks.

The purpose of the SPVA is to ensure that every stakeholder is effective in its role so that the overall payment environment is secured.

What is the mission of the SPVA?

- To develop a common understanding of various security requirement and standards
- To increase awareness of security issues
- To provide payment solutions implementation guidelines to ensure security, durability and interoperable solutions against evolving fraudulent attack's risks
- To encourage adoption of best practices and security enhancements

What value will the SPVA bring to the market?

The SPVA members provide the key security elements among consumers, merchants and transaction acquirers and issuers. Members of the SPVA deliver a unique experience with security guidelines, ensure best practice implementation and continue to evolve security enhancements and interoperability required to reduce fraud and lower risk for all participants in card payment transactions.

The SPVA members deliver more value to their customers by enhancing security solutions that protect cardholder information and defend merchants and acquirers against security breaches.

Through education of third parties engaged in the payment system, the SPVA will increase awareness of security issues, encourage adoption of best practices and eliminate inconsistencies between standards governing disparate components and participants in the payment environment.

Why did the “Big Three” of the secure POS vendor industry decide to cooperate in this area?

Representing collective expertise in the payment systems arena, it is expected that this cooperation will accelerate widespread adoption of enhanced security guidelines. Each of the three companies already operate individually on a regular basis on issues with acquirers, processors and the card brands, as well as organizations such as the PCI Security Standards Council. All three recognize that stakeholders’ consistent adherence to standards and rules is a vital issue in the continued growth of the electronic payments industry.

Is the SPVA open to other secure point of sale payment vendors?

Yes. The SPVA is open to all vendors that develop secure POS payment systems. These vendors can become “General Members” and are eligible to be elected to serve on the Management Committee. They may vote to elect Management Committee representative from General Membership and may participate in, contribute and chair a Technical Working Group.

Is the SPVA open to other players in the payment industry?

Yes. The SPVA is open to any organizations that are not a secure POS payment developers but have products or solutions that interact with secure POS payment devices: retailers, acquirers, SW vendors, banks. These companies can become “Associate Members” and are eligible to be elected to serve on the Management Committee. They may vote to elect Management Committee representative from Associate Membership, and may participate in and contribute to Technical Working Groups.

What are Technical Working Groups?

Technical Working Groups are appointed by the Management Committee to research security topics and develop guidelines to be implemented by the alliance.

What issues will the Technical Working Groups address?

Critical issues have been identified as a first step. Each of them could be covered by a Technical Working Group such as:

1. Standardized Implementation of existing Security Standards
2. Security of Payment Device Lifecycle
3. Security Threat Analysis and Intelligence
4. End-to-End Security Transactions

What benefits should merchants expect from the SPVA's efforts?

Merchants that choose “SPVA-approved solutions” will be assured that they are providing consumers with the highest level of security currently possible and protection against future threats. They will be able to more easily comply with current industry security mandates, such as PCI, and compliance with individual card brand rules. This will reduce their risks and insure their investments against future changes to security requirements.

What benefits should the acquirers expect from the SPVA's efforts?

Acquirers that choose to deploy “SPVA-approved solutions” will significantly raise their security implementations as “SPVA-approved solutions” will require secure POS vendors to provide more proactive and comprehensive security mechanisms and tools, they will be able to more quickly respond to current and future security threats as they develop.

How is the SPVA organized? How is it governed?

The SPVA is governed by a Management Committee consisting of five Directors made up of the three permanent members (Ingenico, Hypercom and VeriFone) and two elected Directors, one each from the ranks of the “General Members” and “Associate Members”. The two elected Directors will be chosen by their respective membership group and serve a two-year term.

The Management Committee's Board is made of Paul Rasori (VeriFone), Chairman; Christopher Coonen (Ingenico), Vice Chairman/Chief Technology Officer; T.K. Cheung (Hypercom), Secretary/Treasurer; Thomas Xu (PAX Technology, Ltd.), General Member Director; and Robert Carr (Heartland Payment Systems), Associate Member Director.

What is the benefit of being a General Member?

Through their participation and leadership on Technical Working Groups, General Members can help shape future security guidelines and acquire first-hand knowledge of current security threats as discussed in working group meetings.

What is the benefit of being an Associate Member?

Through their participation on Technical Working Groups, Associate Members can help shape future security guidelines and get first-hand knowledge of current security threats as discussed in working group meetings.

How does the SPVA relate to the work of other organizations such as the PCI Security Standards Council, EMVco or card brand rules?

A major objective of the SPVA is to foster widespread compliance to existing security standards. The SPVA members already work closely with these standard bodies and expect to offer a more unified voice to these organizations going forward.

Will the SPVA guidelines conflict with or override PCI SSC standards?

No. The intent of the SPVA is to ensure that PCI compliance is a baseline requirement of “SPVA-approved solutions”. The goal is to ensure that there is no confusion regarding implementation of PCI standards in payment appliances, and to ensure that from a payment appliance perspective we are moving beyond minimal compliance to a focus on the best security available.

What sort of issues or gaps is the SPVA trying to address?

Each of the major card brands affiliated with PCI sets its own interpretations of the PCI standards, resulting in differences in deadlines, affectivity, waivers and scope of compliance. Merchants, banks and acquirers are frequently confused by how these rules have been individually interpreted and how to rationalize overlaps and gaps among those interpretations. There is currently no entity that provides a consolidated view of these unique implementations of the standards and, as a result, individual secure POS payment device providers are asked by customers to provide their own interpretations. The SPVA wants to avoid the confusion that this current situation creates.

Additionally, there are different sets of standards for different areas—such as networks, data storage, hardware requirements and software requirements—for the most part, these are complementary but may not mesh perfectly; for example PA-DSS doesn’t encompass operating system security, PCI hardware standards only address PIN entry, and network standards disregard dial-up lines. The goal of the SPVA is to work with card brands and security organizations to smooth out these issues, ensure that customers aren’t confused by different standards and to make compliance easier and less costly

Can the SPVA describe an area in which it envisions creating enhanced standards or requirements?

The initial charter of the SPVA will create Technical Working Groups to focus on:

- common interpretation and implementation of existing industry Security Standards
- common vision and position on SEPA for POS terminals
- Security of Payment Device Lifecycle framework, by developing end-to-end lifecycle security, and
- end-to-end security framework from Terminal to Host

What is the SPVA Lab Network?

The SPVA Lab Network is a group of labs that participate with SPVA members, prospective members and the SPVA's Technical Working Groups on security evaluations of the SPVA implementation guidelines. Members of the Lab Network work together to share best practices and raise the security level within the point of sale industry.

Vendors of secure POS payment devices seeking to obtain an “SPVA-approved solution” designation will need to submit their products to an authorized SPVA laboratory, or member of the SPVA Lab Network. Upon positive completion, such vendor may submit the lab approval report to the SPVA for final approval and listing.

All members of the SPVA Lab Network must pass a rigorous set of eligibility requirements.

Will the SPVA enforce compliance requirements?

Yes. “SPVA-approved solutions” found to be out of compliance post approval will be stripped of their approval until such time the situation is properly corrected and passes third-party lab re-evaluation.

How can I stay informed of the SPVA news and current events?

Regularly visit the SPVA website at www.spva.org.