

delivering
comprehensive
payment
security
experience



Critical issues have been identified. Technical Working Groups will be established to cover:

1 Standardized Implementation of Existing Security Standards. Goal is to release a common interpretation of existing security standards and publish collective implementation guidelines.

2 Security of Payment Device Lifecycle. Goal is to develop end-to-end lifecycle security guidelines to:

- ▶ Ensure security during the complete POS terminal lifecycle – from manufacture through deployment, field maintenance, application software upgrades, eventual end-of-life and removal and secure destruction
- ▶ Manage digitally-signed applications
- ▶ Provide mechanisms to track and manage devices, to ensure security compliance and respond to new threats
- ▶ Create development, manufacturing/supply chain, deployment and repair security guidelines and audit procedures

3 Security Threat Analysis and Intelligence. Goal is to provide education and resources to educate members and payment industry stakeholders regarding the current threats and ways to mitigate them.

4 End-to-End Security Transactions. Goal is to create industry encryption framework of cardholder data utilizing hardware level security module capabilities of secure payments systems to adequately secure cardholder information before it enters the application environment.

■ “SPVA-APPROVED SOLUTION”

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.

Acquirers that choose to deploy “SPVA-approved solutions” will significantly raise their security implementations. Because “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.



CONTACT
info@spva.org

WEBSITE
www.spva.org





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, making life more demanding for merchants and acquirers to implement and manage secured and cost-effective payment solutions.

Each of the major card brands affiliated with PCI sets its own interpretations of the Payment Card Industry (PCI) standards, resulting in differences in deadlines, effectivity, 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 their implementation.

This 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.

It is vital that every stakeholder is effective in its role so that the overall payment environment is secured.

PROVIDING A CONSOLIDATED VIEW

The Secure POS Vendor Alliance (SPVA or the Alliance) 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.

The initial charter of the SPVA focuses on standardized implementation of existing security standards, security of the payment device lifecycle and security threat analysis and intelligence.

A major objective of the SPVA is to foster widespread compliance with existing security standards (PCI Security Standards Council, EMVco, domestic card schemes) by making sure they are properly implemented.

The SPVA members already work closely with these standard bodies and expect to offer a more unified support to these organizations going forward, while giving visibility regarding business intelligence for merchants.

SPVA's Values

- ▶ Open
- ▶ Expert
- ▶ Sharing
- ▶ Committed
- ▶ Proactive
- ▶ Leading

MAKING GOODWILL COOPERATE

The “Big Three” of the secure POS vendor industry – Ingenico, Hypercom and VeriFone – have decided to act as a catalyst and kick off this initiative by establishing a forum for industry-wide cooperation.

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 operates 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.

SPVA structure. To drive this initiative to define and prioritize strategy and activities, the SPVA encourages all payment industry stakeholders to participate in this initiative by joining the Alliance, contributing their expertise and sharing their views.

The SPVA is governed by a Management Committee consisting of five Directors, highly experienced managers within the member organizations, comprised from the three founding members (Ingenico, Hypercom and VeriFone) and two elected members who represent secure POS vendors and organizations involved in the delivery of solutions or services for the payment industry.

These vendors and organizations can become members and all are eligible to be elected to serve on the Management Committee and contribute to Technical Working Groups.

PROVIDING VISIBILITY AND UNDERSTANDING: THE TECHNICAL WORKING GROUPS

The main contribution and guidelines the SPVA can provide to the payment industry will be achieved through the efforts of working groups focusing on key industry issues.

Each Technical Working Group works on a per-project basis bringing together specialists from each of the SPVA members’ companies. Through regular meetings, these teams liaise to develop the outputs required to design recommendations and solutions that would be impossible without such industry cooperation.

Through their participation and leadership in Technical Working Groups, the SPVA members can contribute to enriching and developing future security guidelines and acquire first-hand knowledge of current security threats.

Management Committee

- ▶ **Christophe Dolique**
(Ingenico)
Chairman
- ▶ **TK Cheung**
(Hypercom)
Vice Chairman and CTO
- ▶ **Paul Rasori**
(VeriFone)
Secretary/Treasurer

