INDUSTRY INSIGHTS

Presented by
The ETA Technology Council

Mobile Payments Security
Standards Working Group

Derek Webster
CardFlight

Barbara Mitchell
Verizon

Ryan Schneider
Integrity Payment Systems

Amy Zirkle
Electronic Transactions
Association

Relevant Standards and Specifications applicable to mobile payments in the United States

Introduction

The Mobile Payments Security Standards Working Group of ETA's Mobile Payments Council developed this briefing note to provide an overview of the key security standards and specification setting bodies relevant for the provision of mobile payment service offerings. This document is to serve as an initial tool to inventory the standards and regulations that are applicable to the mobile payments ecosystem.

Employing the relevant industry standards and specifications to support delivery of mobile payments is vital. However, establishing and maintaining a current and consistent security program will ultimately serve to move beyond compliance requirements set forth by industry standards and offer heightened levels of security.

PCI-DSS

In 2004, the major payment networks – American Express, Discover Financial Services, JCB, MasterCard and Visa Inc. – jointly established the Payment Card Industry (PCI) Data Security Standard Council (DSSC). The goal was to establish technical and operational requirements for the protection of cardholder data. The standards developed by the PCI Council apply to all entities that store, process, or transmit cardholder data of these major payment networks – with accompanying requirements for those who develop software/applications or devices that are used in those transactions.[1] The PCI DSS are a well-established benchmark within the payments industry, and apply to any entity that accepts or processes card payments in the physical, online, or mobile space.

Overview

The PCI DSS embraces six key goals that together, serve as best practices for network security. Each goal includes an accompanying PCI DSS requirement that facilitates achieving each specific goal.

For more information
contact

Amy Zirkle
Director of Industry Affairs
azirkle@electran.org

ELECTRONIC TRANSACTIONS ASSOCIATION
Advancing Payments Technology

- The first goal is to establish and maintain a secure network and system. This will ensure that transactions are conducted in a robustly secure network. Per the standard, firewalls must be established to protect cardholder data. These firewalls must be effective without causing undue inconvenience to cardholders or vendors. In addition, authentication data such as personal identification numbers (PINs) and passwords must not involve defaults supplied by the vendors.
- The second goal of the PCI DSS framework is to protect cardholder information wherever it is stored. To support this goal, PCI requires that cardholder data be securely stored, with necessary steps taken to secure against hacking. When cardholder data is transmitted through public networks, that data must be encrypted effectively.
- The third goal is the establishment of a vulnerability management program. This means that systems should be protected against the activities of malicious hackers by using frequently updated anti-virus software, anti-spyware programs, and other anti-malware solutions. All applications should be free of bugs and vulnerabilities that might enable exploits through which cardholder data could be stolen or altered.
- Fourth, network administrators are required to implement strong access control measures. The PCI DSS requirement is to restrict and control access to system information and operations. Cardholder data should not be provided to a system, business or individual unless this data is required to effectively carry out a transaction. Every person who uses a computer in the system must be assigned a unique and confidential identification name or number. Cardholder data should be protected physically as well as electronically.
- The fifth goal is to ensure that networks are constantly monitored and regularly tested to determine that all security measures and processes are in place, are functioning properly, and are kept up-to-date. PCI DSS requires that tracking and monitoring all access to network resources and cardholder data. In addition, security systems and processes must be tested regularly to ensure that they are working effectively.

Finally, an information security policy should be defined, maintained, and followed at all times and by all participating entities. PCI DSS further requires that such policy addresses information security for all personnel.

PCI Security Standards

While the above paragraphs summarize the six key goals of PCI-DSS, it should be noted that the detailed guidelines published by the Council contain hundreds of specific requirements organized into twelve sections, as well as specific guidelines for the frequency and depth of auditing that is required to validate continued compliance.

There are three key areas within the PCI standards activities. These include Payment Application Data Security Standards (PA-DSS), PIN Transaction Security (PCI-PTS), and PCI standards addressing point-point encryption (PCI P2PE). Each of these standards is relevant to mobile payments.

Payment Application Security Standard (PA- DSS)

PA-DSS is applicable to software vendors and those who develop payment applications that store, process or transmit cardholder data and/or sensitive authentication data.[2] Most, if not all, the payment networks require merchants to use payment applications that are PA-DSS- certified. A detailed list of validated applications can be found at: ***https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement.***

In recent years, many solutions have been developed for using widely available mobile devices (e.g. iPhones, iPads, and Android devices) for payment acceptance. In their document ***"Mobile Payment Acceptance Applications and PA-DSS Frequently Asked Questions",*** the PCI-SSC defines a Mobile Payment Acceptance Application Category 3 device as "Payment application operates on any consumer electronic handheld device (e.g., smart phone, tablet, or PDA) that is not solely dedicated to payment acceptance for transaction processing". They further state that such

devices "will not be considered for PA-DSS validation until the development of appropriate advice, guidance, and/or standards to ensure that such applications are capable of supporting a merchant's PCI DSS compliance."

The PCI-SSC subsequently published ***"PCI Mobile Payment Acceptance Security Guidelines"*** in 2014 to help address the ambiguity of PA-DSS requirements when using a Category 3 solution.

PIN Transaction Security (PCI-PTS)

PCI-PTS outlines security requirements that address the management of devices that are utilized to protect cardholder PIN information, as well as other payment processing activities. PCI-PTS further establishes requirements that manufacturers can follow to ensure that the design of a device is PCI compliant. The goal is to encourage financial institutions, processors, merchants and service providers to use devices or components tested and approved by PCI DSS.[3] A list of approved PIN transaction is available from PCI.[4]

Point-to-Point Encryption Standard (P2PE)

PCI's P2PE outlines a comprehensive set of security requirements for point-to-point encryption providers to validate their encryption products, and serves as a means to reduce risk.

At present, use of the PCI P2PE standard in the United States is not mandatory. The advantage of using P2PE certified solutions is a scaled back set of requirements that the merchant must validate as part of their overall PCI-DSS program.

Additional PCI Resources

The Council also provides training to professional firms and individuals so that they can assist organizations with their compliance efforts. The Council maintains public resources such as lists of Qualified Security Assessors (QSAs), Payment Application Qualified Security Assessors (PA-QSAs), and Approved Scanning Vendors (ASVs). Large firms seeking to educate their employees can take advantage of the Internal Security Assessor (ISA) education program.

Payment Network Programs

Though not designated as specific industry standards, the two largest networks, Visa and MasterCard, offer separate programs geared toward supporting the deployment of mobile payments that conform to each of the network's rules and requirements. The goal is to expand the use and acceptance or mobile payments globally and further to ensure that payments made via a mobile device can be utilized just as easily as a traditional card swipe.

Visa Ready Program for Mobile Payments

Visa established its Visa Ready Program to assist financial institutions, merchants, and developers to build and implement solutions that meet Visa's requirements for mobile payments. The program also offers guidelines on how to secure device certification as well as approval of software that can used to initiate and accept payments on the Visa network.

The Visa Ready Program also provides access to Visa intellectual property such as Visa's mobile payment specifications, software development kits (SDK) and best practices. It speeds approval of new payment solutions globally and streamlines the process of connecting to and taking advantage of Visa capabilities.[5]

MasterCard mPOS Program

To further support the use and growth of mobile payments, MasterCard developed its Mobile Point of Sale (mPOS) program. It ensures safe, simple, and smart transactions when consumers use their debit, credit, and prepaid cards at Mobile POS.

MasterCard has also developed, as part of their mPOS program, a comprehensive best practices guide to further enable and facilitate the use of mobile payments and expand its acceptance.[6]

EMVco

Established in 1999, EMVCo is now owned by Visa, MasterCard, American Express, Discover, China Union Pay and JCB. EMVCo is the payment systems entity that manages, maintains, and enhances the EMV Specifications to ensure interoperability and acceptance of EMV based payments on a worldwide basis. EMVCo has expanded its scope from EMV Chip specifications to include EMV tokenization specifications as of January 2014.[7]

EMVCo is also responsible for type approval processes, which presently include EMV Chip terminal compliance testing, as well as Common Core Definitions (CCD) and Common Payment Application (CPA) card compliance testing. These EMV Chip testing processes ensure a single terminal and card approval process at a level that will allow cross payment system interoperability through compliance with the EMV Chip specifications.

More importantly, EMVCo has developed contactless specifications that are relevant for mobile payments. Much of this work is related to addressing the critical technical infrastructure issues associated with enabling contactless payments via mobile handsets.[8]

The work of EMVCo includes defining security requirements for both chip and non-chip based mobile solutions, as well as defining global interoperability between contactless mobile payment devices and payment acceptance infrastructure from a technical perspective.[9]

In working to consider mobile payment issues, EMVCo established a baseline set of principles to guide their efforts[10]:

- A mobile device may support multiple contactless mobile payment applications from multiple financial issuers and carrying different brands.
- The user determines which payment instrument is to be used for a transaction.
- EMVCo does not mandate a particular Secure Element architecture or policy, but seeks to provide flexibility in order to allow the deployment of the most appropriate solution for a given market. This includes flexibility in the actual location of the Secure Element – as to whether it is on the handset or cloud-based.
- Where possible, EMVCo will make use of existing industry specifications rather than defining new specifications.
- EMVCo will also seek to utilize industry type approval programs for qualification of mobile devices.
- Contactless Mobile Payments must be compatible with existing EMVCo based contactless payment infrastructure.

Deploying an EMV "chip card" acceptance solution typically involves selecting a hardware supplier and software kernels that have received Level 1 and Level 2 approvals from EMVCo. In addition to using EMV approved hardware and software, the entire solution (encompassing hardware, middleware, payment gateway, processor host and card brand) must be validated and approved by a rigorous set of card brand approvals including Visa Acquirer Device Validation Toolkit (ADVT), MasterCard Terminal Integration Process (M-TIP), American Express Integrated Circuit Card Payment Specification (AEIPS), and Discover Payment Application Specification (D-PAS). Such approvals are required for each unique configuration. For example, a payment gateway that supports multiple acquirer processors will need to obtain a unique set of certification approvals for each processor that EMV transactions may pass through.

Summary

For over a decade, the PCI DSS standard has been widely recognized as the security benchmark for the payments industry. Compliance with PCI PA-DSS is a clear indicator that a payment application is mature and may be safely used to process payments. The EMV standard, widely adopted throughout Europe and in parts of the rest of the world, is gaining momentum in the United States, with adoption spurred by a liability shift that began in October 2015.

In addition to these security standards, the card brands have developed programs to speed adoption of mobile payments for merchants and customers alike. The tools available through Visa Ready Program and MasterCard's mPOS program aid developers in designing robust and compliant mobile applications.

Other standards to watch

The National Retail Federation and its technology standards organization ARTS (Association for Retail Technology Standards) are working to develop standards for retail environments. **ARTS is now collaborating with a Belgium based group** on a POS payments integration standard that will encompass mobile payment and EMV at the POS.

Cloud Security Alliance Mobile Working Group has prepared security guidance for critical areas of mobile computing with recommendations.

Footnotes

1 See PCI DSS Quick Reference Guide, Understanding the Payment Card Industry Data Security Standard Version 3.0, August 2014.

2 Ibid. pp.7.

3 Ibid.

4 https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

5 See https://technologypartner.visa.com/Mobile/

6 See http://www.mastercard.com/us/company/en/docs/MasterCard_Mobile_Point_Of_Sale_Best_Practices.pdf

7 Further details on EMV Co operation can be found at http://www.emvco.com/

8 EMV Co White Paper on Contactless Mobile Payment, Version 2.2, June 2015

9 Ibid., p. 6.

10 Ibid., p. 9.