NEW WORLD FOR CREDIT CARD SECURITY: FROM PA-DSS TO SSF

ForenSecure’19
April 11, 2019
Joel Dubin, PCI QSA, PA-QSA, CISSP
Senior Consultant, Application Validation

-Ten years as a PA-QSA and QSA and five years in PCI for a global bank

-Reviewed credit card systems of all sizes up to major global companies

-Conducted PA-DSS assessments in U.S., Latin America, Europe and Middle East

-Scoped architectures for PCI, PA-DSS applications and P2PE
OVERVIEW

• Payment application architectures
• The payment application ecosystem
  • Who is the PCI SSC?
  • What is PA-DSS and P2PE?
• The new SSF and how it will replace PA-DSS
  • What is SSF and how does it differ from PA-DSS?
• Key dates for SSF implementation
• Highlights of the SSF requirements
• Getting ready for your first SSF and SLC assessments
PAYMENT APP (POS) ARCHITECTURE I
PAYMENT APP (POS) ARCHITECTURE II

Diagram showing the flow of data from Point-of-Sale (POS) devices to the processor through an inside merchant network and firewall, with connections to the internet.
PAYMENT APP (POS)
ARCHITECTURE III (P2PE)
WHO IS THE PCI SSC?

Payment Card Industry Security Standards Council

- Visa
- MasterCard
- American Express
- Discover
- JCB

One standard for merchants and service providers  
PCI
One standard for payment applications  
PA-DSS
One standard for P2PE solution providers  
P2PE
SUITE OF PCI STANDARDS

Hierarchy of PCI Standards

- PTS → PIN-pad Level
- PA-DSS → Application Level (Soon to be SSF)
- PCI → Network Level
- P2PE → ALL OF THE ABOVE
WHAT IS PA-DSS?
Payment Application Data Security Standard (PA-DSS)
Card industry standard for payment applications
WHAT IS THE SOFTWARE SECURITY FRAMEWORK? (SSF)

• The Software Security Framework will be replacing PA-DSS in 2020

• The traditional PA-DSS will now be split into two standards:
  – PCI Secure Software Standard
  – PCI Secure Software Life Cycle (Secure SLC) Standard

• The Software Security Framework (SSF) broadens the scope of what is considered a payment application
THE KEY TAKEAWAY ABOUT SSF – TWO STANDARDS

1) Secure Software Standard
   Traditional application testing
   All PA-DSS requirements, except Requirement 5

2) Secure Software Life Cycle (Secure SLC) Standard
   A standalone version of Requirement 5

Sort of like taking Requirement 5 out and making it a separate standard
But not exactly . . . as will be seen
WHY THE SHIFT TO SSF NOW?

• The PCI SSC sees development practices at the heart of payment application security

• SSF makes development methodology a focus in payment application reviews

• Broader than just testing of application security controls and puts formerly out-of-scope applications in scope

• Allows for using other security frameworks beyond PA-DSS
THE TWO PARTS OF SSF
PART 1: SECURE SOFTWARE STANDARD

Secure Software Standard

• Closest to, and resembles, current PA-DSS

• Like PA-DSS includes traditional review of an application:
  • Document review
  • Interviews
  • Application testing
THE TWO PARTS OF SSF
PART 1: SECURE SOFTWARE STANDARD

So What Is Different?

• Objective-based approach – No “One Size Fits All”

• Risk management rather than simple binary audit approach

• Holistic view of security controls

• Self Delta assessments if Software Life Cycle (SLC) validated
THE TWO PARTS OF SSF
PART 1: SECURE SOFTWARE STANDARD

*What Else Is Different?*

- Broader scope and definition of the term “payment application”
  - Traditional payment applications like the current PA-DSS
  - Modern payment applications that were out-of-scope for PA-DSS
    - Cloud based
    - Mobile
The Two Parts of SSF

Part 2: Secure Software Life Cycle

Secure Software Life Cycle

- Similar to current PA-DSS Requirement 5
  - Verify software development process to make sure they include security reviews throughout the life cycle

- Similar testing procedures like PA-DSS Requirement 5:
  - Document review
  - Interviews
So What Is Different?

- Review of payment application vendor *not* their application
  - Vendor-based vs application-based

- Risk management-based to allow flexibility based on risk-rankings

- Valid for three years, and must reassess after three years
  - Unlike annual renewals for PA-DSS and other PCI standards
SSF IMPLEMENTATION DATES

• January 2019 – PCI SSC releases SSF standard to the public
• July 2019 – Anticipated start date for SSF assessments
• July 2020 – End date for PA-DSS submissions
• Late 2022 – Retirement of PA-DSS listings (move to “Acceptable for Existing Deployments”)
SECURE SOFTWARE
CORE REQUIREMENTS

Security Objective: Minimizing the Attack Surface

• Control Objective 1: Critical Asset Identification
• Control Objective 2: Secure Defaults
• Control Objective 3: Sensitive Data Retention
SECURE SOFTWARE
CORE REQUIREMENTS

Security Objective: Software Protection Mechanisms

• Control Objective 4: Critical Asset Protection
• Control Objective 5: Authentication and Access Control
• Control Objective 6: Sensitive Data Protection
• Control Objective 7: Use of Cryptography
SECURE SOFTWARE
CORE REQUIREMENTS

Security Objective: Secure Software Operations

- Control Objective 8: Activity Tracking
- Control Objective 9: Attack Detection
SECURE SOFTWARE
CORE REQUIREMENTS

Security Objective: Secure Software Lifecycle Management

• Control Objective 10: Threat and Vulnerability Management
• Control Objective 11: Secure Software Updates
• Control Objective 12: Vendor Security Guidance
SECURE SOFTWARE CORE REQUIREMENTS

Module A – Account Data Protection

Security Objective: Account Data Protection

• Control Objective A.1: Sensitive Authentication Data
• Control Objective A.2: Cardholder Data Protection
SECURE SOFTWARE LIFECYCLE REQUIREMENTS

Security Objective: Software Security Governance

• Control Objective 1: Security Responsibility and Resources
• Control Objective 2: Software Security Policy and Strategy
SECURE SOFTWARE LIFECYCLE REQUIREMENTS

Security Objective: Secure Software Engineering

• Control Objective 3: Threat Identification and Mitigation
• Control Objective 4: Vulnerability Detection and Mitigation
Security Objective: Secure Software and Data Management

- Control Objective 5: Change Management
- Control Objective 6: Software Integrity Management
- Control Objective 7: Sensitive Data Protection
SECURE SOFTWARE LIFECYCLE REQUIREMENTS

Security Objective: Security Communications

• Control Objective 8: Vendor Security Guidance
• Control Objective 9: Stakeholder Communications
• Control Objective 10: Software Update Information
BUT DON’T PANIC – YET!

The SSC is working on a transition plan to include:

1. Assisting existing payment application vendors to move from PA-DSS to SSF
2. Develop reporting templates for the two parts of the framework
3. Transition existing PA-QSAs to be able to do SSF reviews
WORK WITH YOUR PA-QSA

In addition, we at Coalfire are working on a transition plan:

1. Work with you to discuss next steps and tailor make a transition plan
2. Make presentations to your staff and management about SSF
3. Develop assessment methodology for when we can begin assessments
4. Transition existing PA-QSAs to be able to do SSF reviews
IF SOME OF THIS SEEMS VAGUE

It’s not you.
You’re not confused.
It is vague,
because it’s still in development.
And no assessments have been done yet
to test it out in the field.
FOR MORE INFORMATION

Check the PCI SSC web site:

https://www.pcisecuritystandards.org
MY CONTACT INFORMATION

Joel Dubin, QSA, PA-QSA, CISSP
Senior Consultant
jdubin@coalfire.com
720-643-4391
QUESTIONS?