

Guidelines for Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)(NIST SP 800-79-2 Draft) – Status Update

Ramaswamy Chandramouli (Mouli)

Information Technology Lab (ITL), NIST

March 4, 2015

FIPS 201-2 Associated Special Publication's Workshop

Guidelines for Authorization of PCI and DPCI – Status Update

- **Guidelines for Authorization of PCI and DPCI - Objectives**
- **Scope of the SP 800-79-2 Document**
- **Overview of Contents**
- **Publication Process Timeline**

Guidelines for Authorization of PCI and DPCI - Objectives

- Provide an assessment and authorization methodology for verifying that the following issuers:
 - (a) **PIV Card Issuers**
 - (b) **Derived PIV Credential Token Issuers**
- **ARE ADHERING TO FOLLOWING STANDARDS & IMPLEMENTATION DIRECTIVES IN**
 - *FIPS 201-2, SP 800-76-2, SP 800-156, SP 800-157, SP 800-37-1 & SP 800-79-2 itself*
 - *OMB Memorandums 05-24, 06-06 (Appendix E), 07-06, 11-11, FAR 4.1302 & Commonly Accepted Security Readiness Measures*

Guidelines for Authorization of PCI and DPCI – Objectives.. contd

- The outcome of applying the assessment and authorization methodology are:
 - (a) **Establishing the reliability of the Issuer**
 - (b) **Authorizing the Issuer (PCI or DPCI)**

SP 800- 79-2 (Guidelines for Authorization of PCI & DPCI) - Scope

- **Covers both Small & Large Organizations**
- **Issuance processes can be:**
 - **Centrally Located, Geographically Dispersed, Outsourced in varying degrees to another organization(s) or Service Provider(s)**

SP 800-79-2 – Overview of Contents

- **Controls derived from FIPS 201-2 and relevant documents (NIST Special Pubs, OMB Memos etc) for PCI & DPCI**
- **Assessment methods (Interview, Review of Documents, Observe etc)**
- **Evaluating Results of Assessment for arriving at an Authorization Decision**
- *In addition, the guidelines cover:*
 - Preparatory Tasks for Assessment that includes : Creation of Needed Roles/Responsibilities & Developing an acceptable Operations Plan, Drawing the Issuer's Authorization Boundary
 - Contents of Authorization Package

Additional Controls in SP 800-79-2

- *Issuer Controls for Derived PIV Credentials* – **Major Addition** – Controls & Assessments in Appendix G.2
- Written Policy for Identity Proofing & Registration for Citizens of Foreign Countries – DO-8
- Including the Adjudication Status in IDMS – CI-7
- Iris Image Formatting – CI-8
- Formatting of Fingerprint Template for On-card comparison – CI-9
- Representation of optional Chain-of-Trust Data – CI-10

Additional Controls in SP 800-79-2 .. Contd..1

- *If fingerprints for background investigation and PIV Card storage are collected during different visits, authentication of applicant using biometric – EI-13*
- *Credentialing Guidance based on OPM & OMB directives (Springer Memo & M-05-24) – AP-3*
- *Card Issuance only after NAC results, if FBI NCHC cannot be conducted – AP-4*
- *Termination of PIV card based on background investigation results – AP-5*

Additional Controls in SP 800-79-2 .. Contd..2

- *Coordination with Card Vendor to ensure integrity of cards in case issuer chooses to use Tactile Markers – CP-5*
- *Destruction of Cards that contain topographical defects (scratches, fading etc) – CP-6*
- *Printing of Cards corresponding to color representation specified in FIPS 201-2 Section 4.1.5 – CP-7*
- *Use of agency-approved Pseudonyms – AI-14*
- *Controls during Re-issuance, re-use of biometric data, post issuance update, PIN & verification data reset – MP-8 thru MP-15*

(Summary: 21 New Controls beside 53 DPCI Controls)

SP 800-79-2 – Publication Timeline

Milestone	Occurrence Date/ Planned Date
First Public Comment Draft	6/02/2015
Public Comment Period - Closing Date	6/30/2015
Publication of Final Document	Soon (Was Waiting for SP 800-157 Publication)

Thank you

Questions?

Ramaswamy Chandramouli (Mouli)
NIST ITL Computer Security Division
mouli@nist.gov