

# IAB Agenda

- **Smart Card Alliance Introduction** (*Randy Vanderhoof, SCA*)
- **Keynote: Credentialing and Security** (*COL Hensley, JTF-GNO*)
- **Transportation Worker Identification Card (TWIC) Update** (*John Schwartz, DHS*)
- **Winter Storm Exercise: Results and Next Steps** (*Lemar Jones, PFPA & Craig Wilson, DHS*)
- **GSA Approved Products List Status** (*Dave Temoshok, GSA*)
- **NIST Update on Standards** (*Hildy Ferraiolo, NIST*)
- **Single Enrollment Process for Shared Service Provider Program** (*Michel Kareis, GSA*)
- **IAB Chairman Remarks** (*Mike Butler, IAB*)



# SP 800-73-1 Content

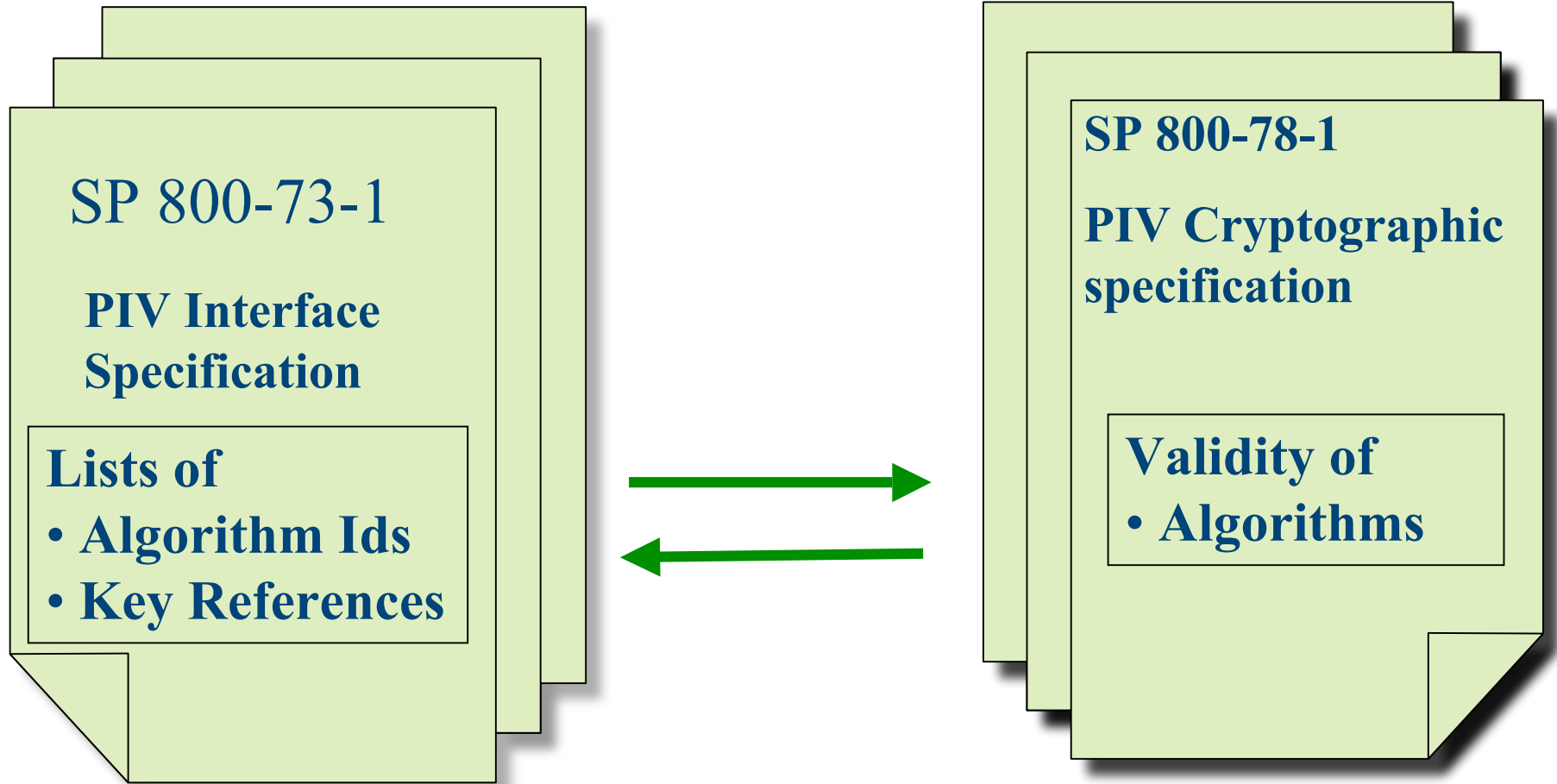
---

SP 800-73-1 *Interfaces for PIV* Specifies:

- PIV Data Model
- Transitional Interface
- End-Point Interface  
(Card Edge and Client API)

# SP 800-73-1 Dependencies

---



# Why is a Revision necessary?

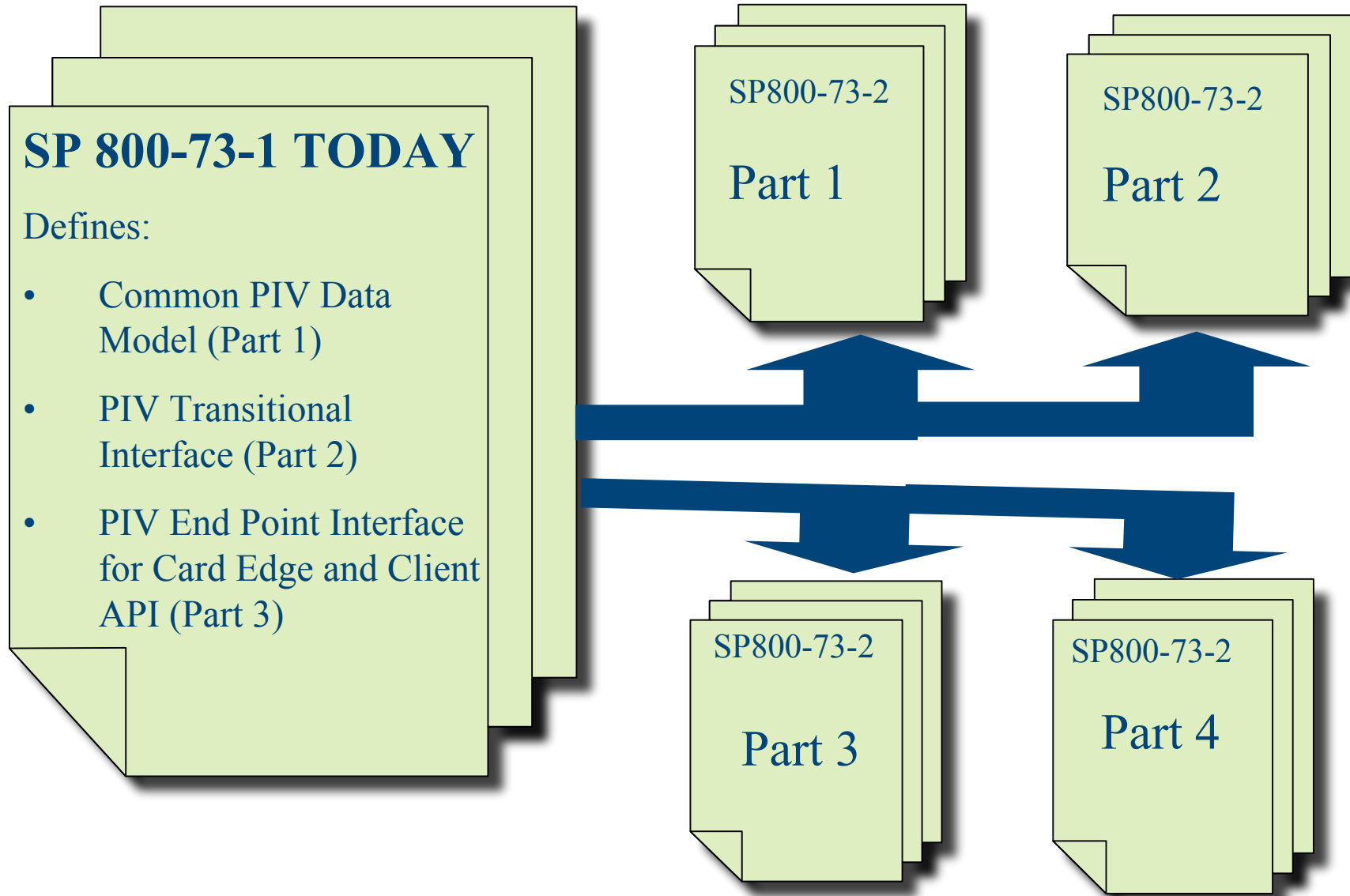
(Revised Version: SP 800-73-2)

---

- To achieve -78-1 independent
- Future sunsets of algorithms due to security threats analysis will not affect SP800-73-2
- The key reference Tables and algorithm identifiers tables have been removed and incorporated in -78-1
- Incorporate the current Errata

# SP 800-73-2 Modules/Parts

---



# Rationale for SP 800-73-2 Parts

---

- Easier adaptation to parts of 800-73-2 for multiple smart card programs
  - E.g. de-federalized PIV Card incorporating Part 2 and 3, but defining their own Part 1 (Data Model elements and AID from a different Namespaces)
- Ease of future (targeted) revisions without impact on other parts.

# SP 800-73-2 Part 1: PIV Namespaces, Data Model and Data Types

---

SP 800-73-2  
Part 1

## SP 800-73-1 TODAY

Defines:

- **PIV Data Model (Part 1)**
- PIV Transitional Interface (Part 2)
- PIV End Point Interface for Card Edge and Client API (Part 3)

Inherits Part 1 of the current standard

- Plus (from other sections):
- Specification of the PIV card application Namespaces for AID, OID and tags
- Description of the PIV Data Types (Algorithm ID and Key references)
- Inherits Appendix A of SP 800-73-1 (Spreadsheet of Containers and inner tag elements with respective lengths requirements)

# SP 800-73-2 Part 2: The End Point Card Command Interface

---

## SP 800-73-1 TODAY

Defines:

- Common PIV Data Model (Part 1)
- PIV Transitional Interfaces (Part 2)
- **PIV End Point Interface for Card Edge and Client API (Part 3)**

SP 800-73-2

Part 2

- Inherits End-Point Card Command Interface specifications of the current standard as is.

# SP 800-73-2 Part 3: End-Point Client Application Programming Interface

---

## SP 800-73-1 TODAY

Defines:

- Common PIV Data Model (Part 1)
- PIV Transitional Interface (Part 2)
- **PIV End Point Interface for Card Edge and Client API (Part 3)**

Inherits End-Point Client API specification of the current standard as is.



SP 800-73-2

Part 3

# SP 800-73-2 Part 4: The Transitional Interfaces

---

## SP 800-73-1 TODAY

Defines:

- Common PIV Data Model (Part 1)
- **PIV Transitional Interface (Part 2)**
- PIV End Point Interface for Card Edge and Client API (Part 3)

- The Transitional Interfaces (subset of GCS-IS NISTR 6778)
- Inherits (informative) Part 2 of current standard as is.

SP 800-73-2

Part 4

# Deleted Elements of SP 800-73-2

---

- Mandatory key size and algorithm per key
  - Issuers can choose -78-1 key size and algorithms per key
- Impact: Relying systems have to prompt the card to discover on card key size and algorithm
- A cryptographic object discovery mechanism is needed

# New Elements of SP 800-73-2

## Discovery Mechanism

---

- SP 800-73-2 introduces a cryptographic object discovery mechanism
- 7816-15 (PKCS#15) – it's standards-based, well known and widely in use

# Decoupling of Object Sizes & Container Sizes

---

- SP 800-73-2 retains minimal container sizes specifications.
- Upper bound of object sizes, for selected objects, will be removed.

# SP 800-73-2 Deletions

---

- The Algorithm identifiers table and key references table will not be listed in -73-2
- SP 800-78-1 will be the source of algorithm IDs and key reference
- Implications: Future sunset of keys due to security threats analysis will not affect SP800-73-2



# NIST PIV Strategy in 2007

---

1. Respond to critical urgencies as they arise.
2. Provide application examples & advice.
3. Complete revisions already committed.
  - SP800-76-1 editorial improvements (completed)
  - SP800-78-1 and SP800-73-2 changes (in process)
  - SP800-104 (color coding)—it's *optional* (public comment period ended)
4. Other Work in Progress.

# Application Examples

---

- Card and Middleware Reference Implementation
  - updated now to SP800-73-1; will track SP800-73-2
  - Available by Mid-April 07
- Data Model toolkit (-85B) is available at  
[http://csrc.nist.gov/piv-program/dm\\_tester/index.html](http://csrc.nist.gov/piv-program/dm_tester/index.html)
- Windows Smart Card Logon with the PIV card
  - Demo CSP source code
- Linux Smart Card Logon with the PIV card
  - Demo PKCS#11 module source code
- Using the PIV card to establish secure sessions (SSL/TLS), and secure email (S/MIME)

# NIST Demonstration at the SCA Conference

---

- Visit NIST's boot Today, April 11<sup>th</sup>
- Demonstration to include:
  - Windows (Server) and Linux (Client) Smart-Card OS Logon
  - Followed by
    - SSL/TLS secure session using the PIV card
    - email (signing and encrypting) through S/MIME-enabled email client

# Other Work in Progress

---

- With NCR & FRAC, develop “skills & qualifications representation”
- Secure Biometric Match-on-Card (MOC) over contactless Interface
  - Goal: A technical feasibility demonstration
- Additional Application Demonstrations for PACS
  - CHUID, PKI and Biometrics Use-Cases

# Thank you

Program Website: <http://csrc.nist.gov/piv-program>

## Program Team:

Dr. R. Chandramouli (Mouli)  
*NIST, Director, NPIVP*  
[mouli@nist.gov](mailto:mouli@nist.gov)

William I. MacGregor  
NIST PIV Program Coordinator  
[william.macgregor@nist.gov](mailto:william.macgregor@nist.gov)

Hildegard Ferraiolo  
NIST  
[Hildegard.Ferraiolo@nist.gov](mailto:Hildegard.Ferraiolo@nist.gov)