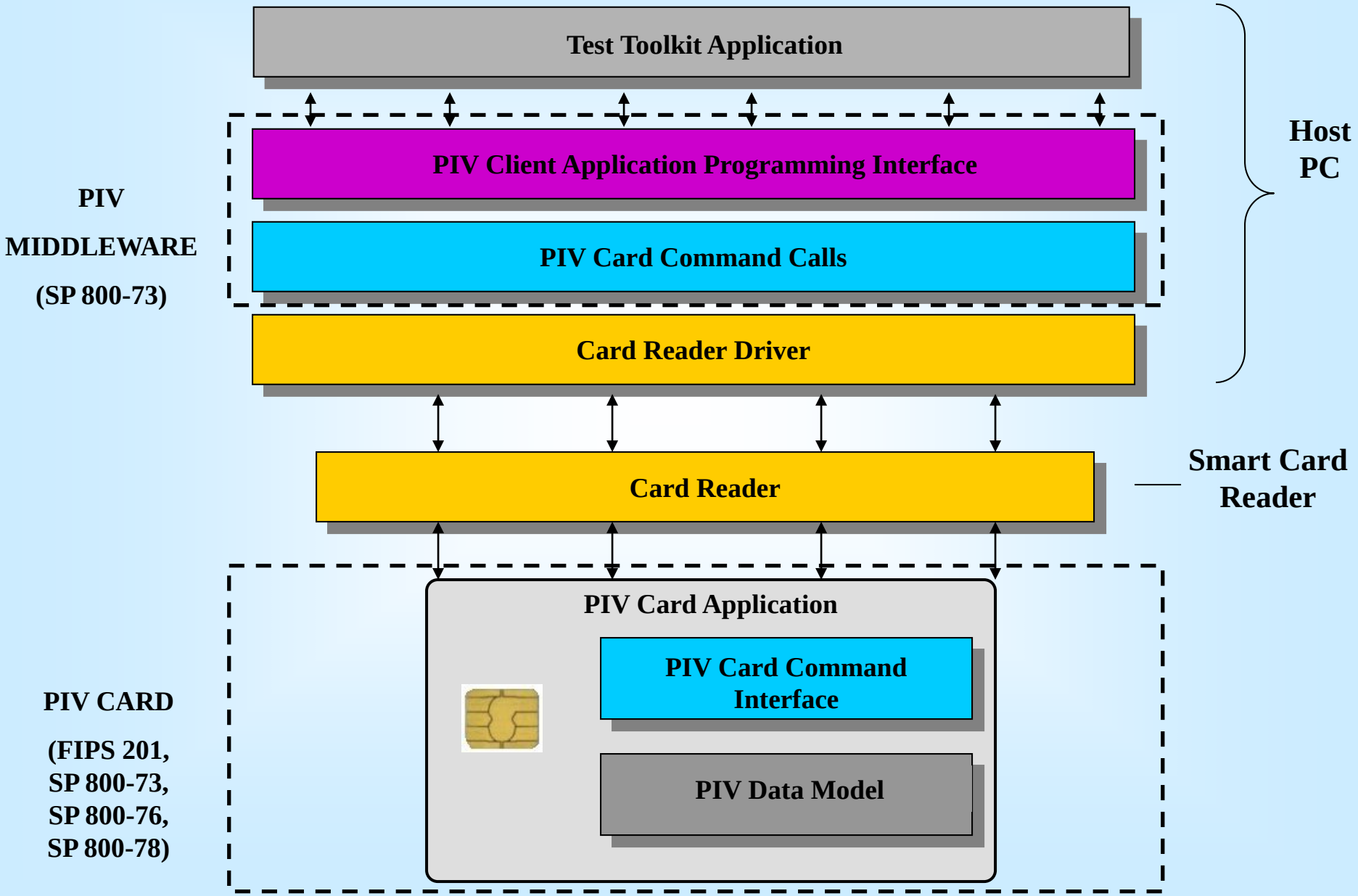
PIV Data Model Testing

Ketan Mehta
mehta_ketan@nist.gov
March 3, 2006

Agenda

- PIV Test Environment
- Test Methodology
- Test Areas
- Schedule

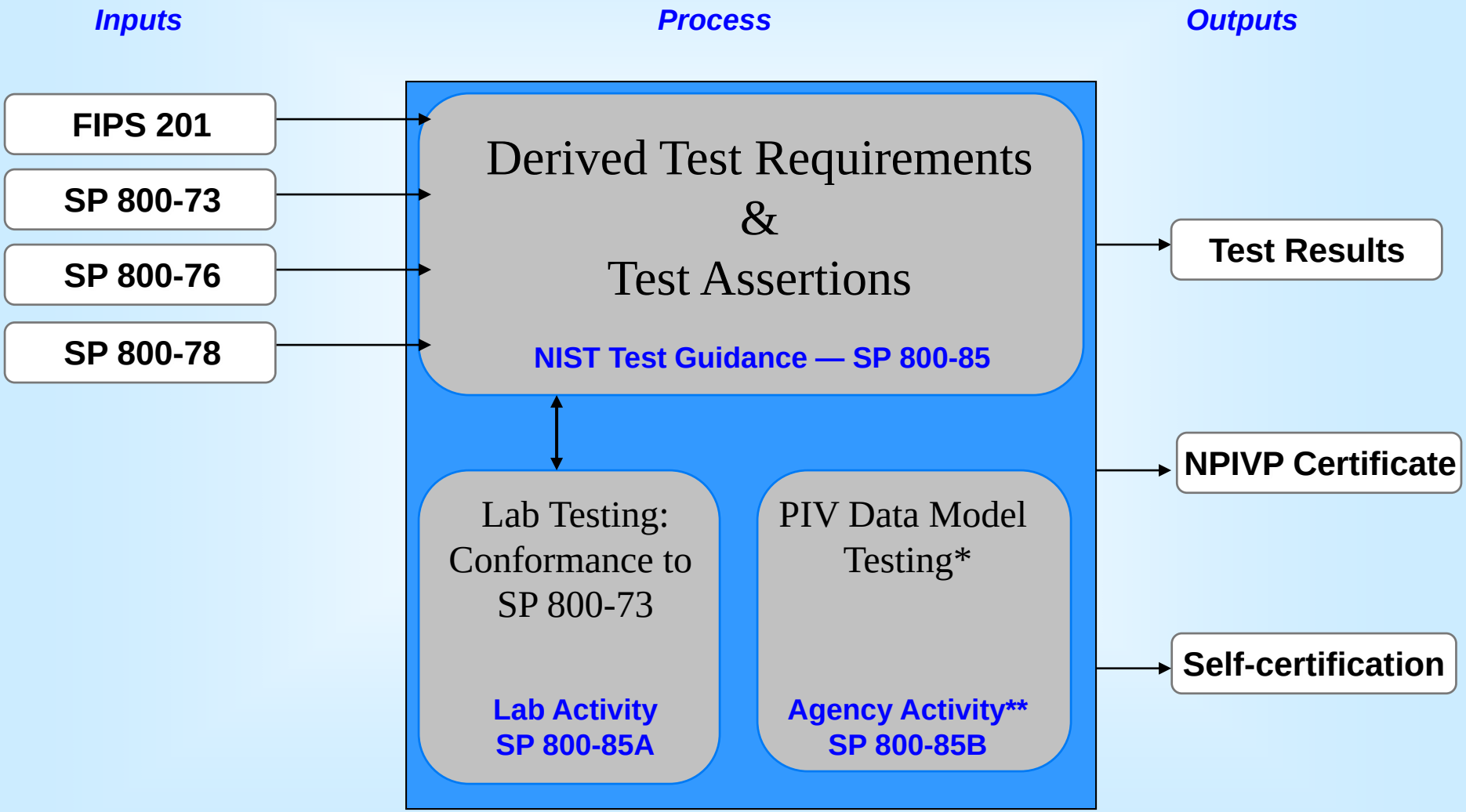
PIV Test Environment



Agenda

- PIV Test Environment
- Test Methodology
- Test Areas
- Schedule

PIV Test Methodology



* Conformance to FIPS 201, SP 800-76, and SP 800-78
** The process is currently being defined

Agenda

- PIV Test Environment
- Test Methodology
- Test Areas
- Schedule

Test Areas

- CHUID Data Object
- Security Object
- Biometric Data Object
- PKI Keys and Certificates

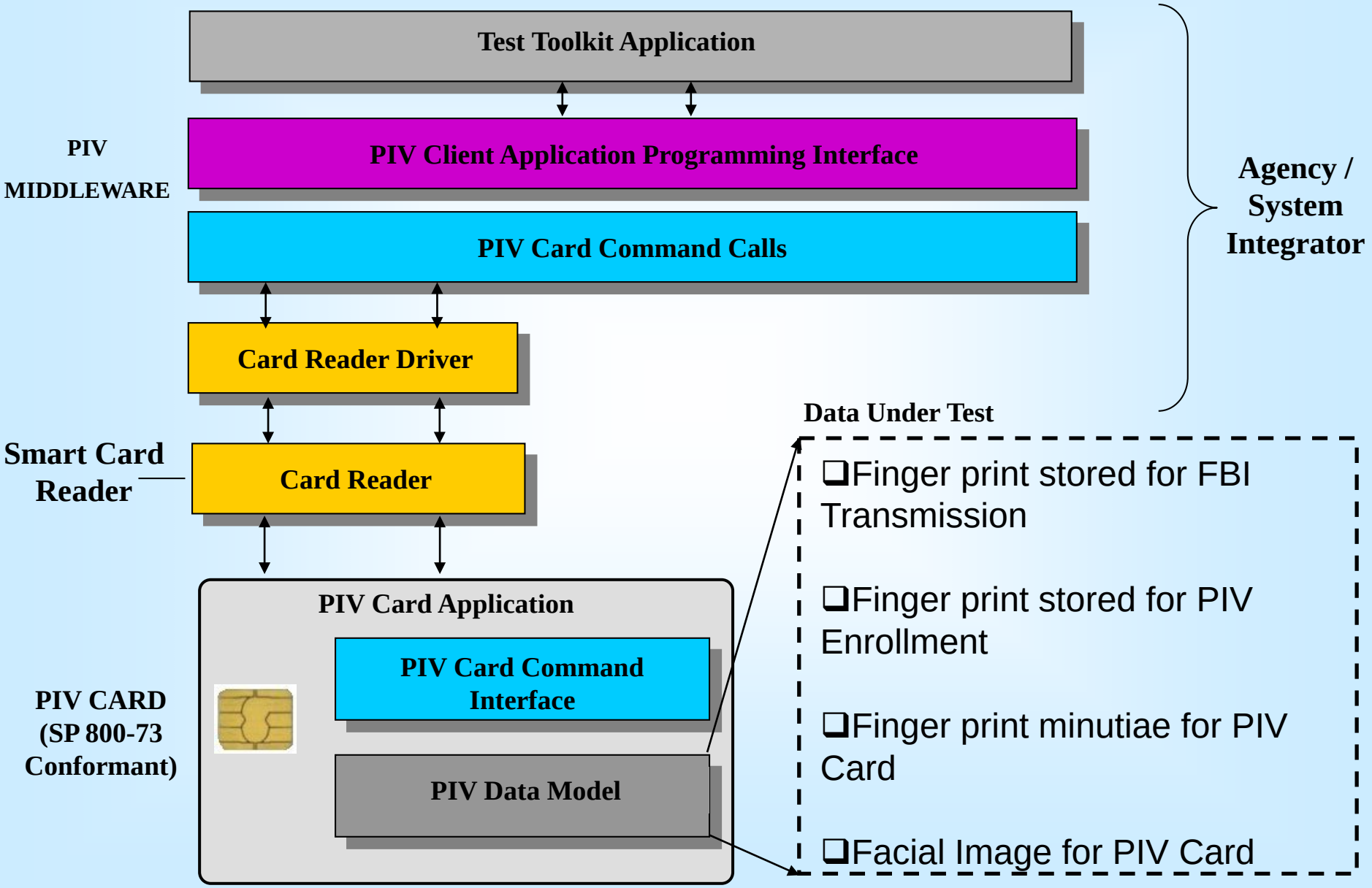
Note that all test requirements are designed to:

- Validate the format of PIV data

- Validate values in the fields

- Validate computation such as signatures or data comparison

SP 800-85B – PIV Biometrics Testing



SP 800-85B – Biometric Data Conformance

Integrated PIV Biometrics Process

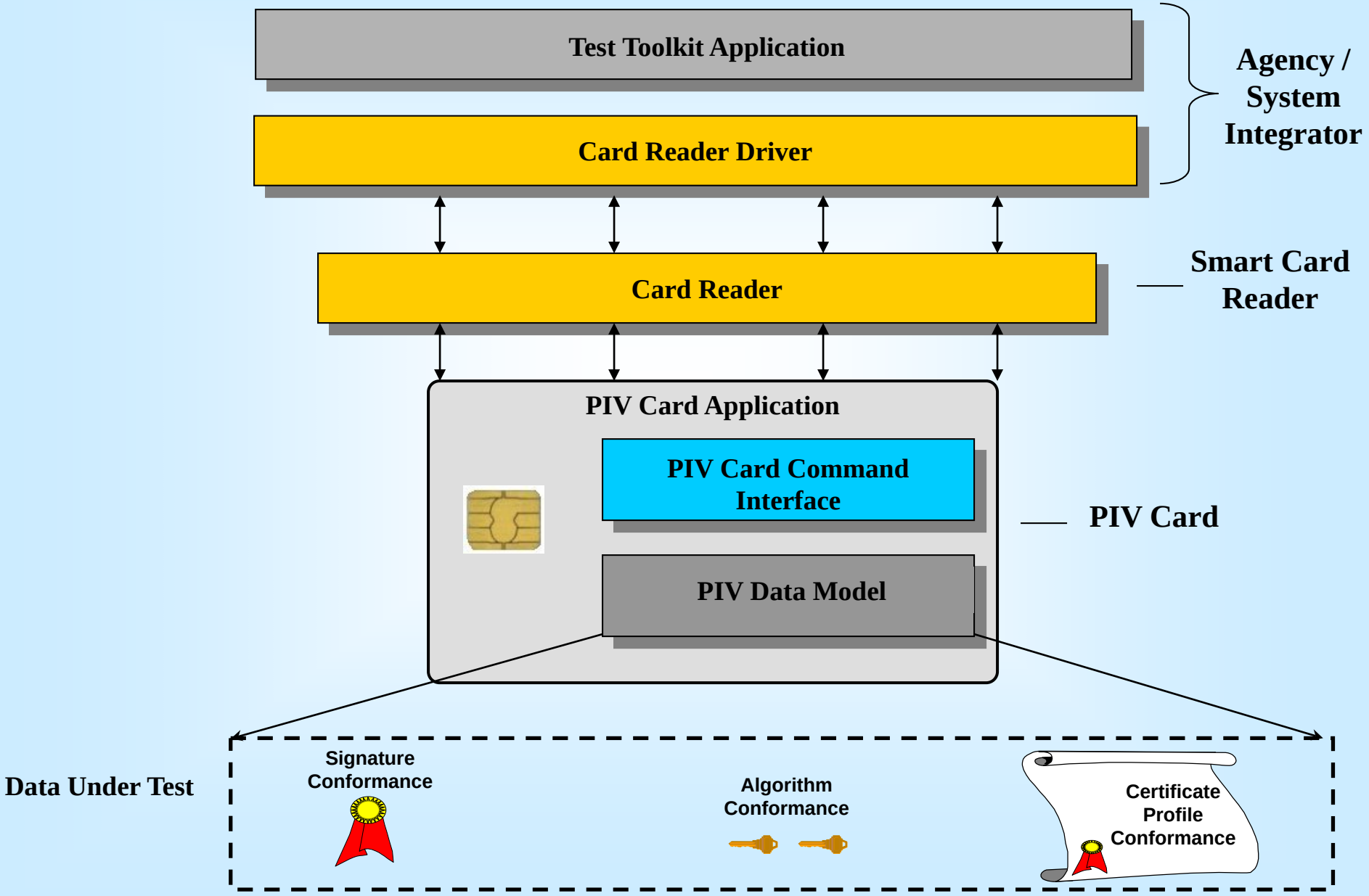
Enrollment Process
- Face Templating
- Fingerprint Templating
- CBEFF Header Generation
- PIV-Specific Enrollment Procedures

Verification Process
- Fingerprint Matching

Documentation (Fingerprint and Facial Acquisition, Equipment, Procedures)

Format Validation	Human Inspection	Performance Tests
Tested through SP 800-85B	**- Dependent on the policy requirements and procedural steps** **- External to PIV Testing**	**- Quality dependent on the MINEX04 test results** **- External to PIV testing**

SP 800-85B – PIV PKI Testing



SP 800-85B — Cryptographic Objects Conformance …Signature Conformance

- Validate signatures on all signed PIV objects
- Validate signature block format on all signed PIV objects
  - Validate encoding of Cryptographic Message Syntax external digital signature
- Validate values in certain fields of the signature block
  - Validate algorithms employed are in agreement with SP 800-78
  - Values are consistent with other data objects on the PIV Card

SP 800-85B — Cryptographic Objects Conformance …Certificate Conformance

- Validate the presence of CRL and OCSP URLs
- Validate NACI indicator field

SP 800-85B — BER-TLV Format Conformance

- The tags and lengths in various data objects should conform to specifications in Appendix A of SP 800-73.

Tentative Schedule

- Draft SP 800-85B – April 3rd
- Final SP 800-85B – April 28th