



# Electrosoft

**Fueling Customer Success Through Outstanding Value and Trust!**

## **PIV Card Test Requirements & Conformance (SP 800-85A-4) Update**

*Presented By: Jason Mohler (Supporting NIST)*

*March 3, 2015*

Electrosoft Services, Inc.  
1893 Metro Center Drive  
Suite 228  
Reston, VA 20190

Web: <http://www.electrosoft-inc.com>  
Email: [info@electrosoft-inc.com](mailto:info@electrosoft-inc.com)  
Tel: (703) 437-9451  
FAX: (703) 437-9452

- **Background**
- **Version numbering**
- **Key changes to the existing version**
- **Publication process timeline**

- **The document's focus is conformance testing to NIST SP 800-73-4 Parts 1, 2, and 3**
- **SP 800-85A contains the test requirements and test procedures for testing smart card middleware as well as the card application.**
- **Testing supports the interoperability goals of FIPS 201-2**
- **Last updated July 2010 for NIST SP 800-73-3—6 months after the finalization of SP 800-73-3**



# Version Numbering

## “WHAT HAPPENED TO SPECIAL PUBLICATION 800-85A REVISION 3?”

*Revision numbers between NIST Special Publications 800-73 and 800-85A were misaligned from the start because the initial publication of SP 800-85A did not occur until after the publication of SP 800-73, Revision 1. When SP 800-73, Revision 2 and Revision 3 were published, SP 800-85A was updated to Revision 1 and Revision 2, respectively. This revision numbering mismatch created ongoing uncertainty and confusion regarding which revision of SP 800-85A was consistent with which revision of SP 800-73. To reduce this uncertainty going forward, revision number 3 has been skipped for SP 800-85A, and this version of SP 800-85A has been given revision number 4 (SP 800-85A-4) since this version is consistent with the updates to SP 800-73, Revision 4. Future revisions of SPs 800-73 and 800-85A will maintain the revision number consistency.*



# Key changes to the existing version

## Added

- **2 new testable interfaces (Secure Messaging, Virtual Contact Interface)**
  - Behavior on the new interfaces is very similar to the existing interfaces
    - VCI closely mirrors the contact interface
    - SM closely mirrors the contactless interface
- **New command behavior and return codes in SP 800-73-4**
- **PIN/PUK value conformance checking**
  - Previously only checked length
- **One new middleware command**
  - (pivEstablishSecureMessaging)
  - SM leverages GENERAL AUTHENTICATE at the card command level
- **OCC and pairing code added to VERIFY card command**
- **Test Assertions Section approximately 35% longer than the previous revision**



# Key changes to the existing version

**Removed three appendices to make the document more manageable**

- **Appendix containing a sample test report**
- **Appendix that mapped DTRs to test assertions**
  - **Similar information is already present in the test assertion sections**
- **Informative appendix on middleware implementation considerations**



# Publication Timeframe

- **Tied to the final publication of SP 800-73-4**
- **Updated in parallel with the development of SP 800-73-4**
- **Currently up-to-date with the 2<sup>nd</sup> public draft of SP 800-73-4**
- **Remaining updates are related to the comment resolutions for the 2<sup>nd</sup> public draft of SP 800-73-4**
- **The plan is to release SP 800-85A-4 for public comment when SP 800-73-4 is published as a final or shortly thereafter**



# Questions

