



GSA 800-85B TOOL CHANGE LOG

3.0.0

- Tool version added to html and pdf reports and logs.
- Automatically updates certificate 9A_06 or 9A_07 in configuration file.

3.1.0

- Automatically decompressing gzipped versions of certificate 9A_06/9A_07.
- Enable/Disabling of optional tests in certificate profile conformance category added.
- Automatically update of configuration setting USE_CASE_PIV_Authenticate key/algorithm string (9A_06/9A_07).

3.2.0

- Removed reset_retry_counter_apdu call within disconnect after each test.
- Added additional error checking for Transmit error. Error no longer affects subsequent tests.

3.3.0

- Added catching for multiple known exceptions.
- Removed unnecessary data items from Configuration tab.
- Simplified logs/results/reports path setting into single Configuration->Test Settings->Output Locations->Configuration Main Path setting.
- Added backup capability (get and save containers from card).
- Added read containers from file capability through use of Configuration->Test Settings->GET_CONTAINERS_FROM_CARD setting.

3.3.1

- Default configuration file modifiable values changed to blank.
- Reports/logs/results reset for default configuration file.

3.3.2

- Added support for 3 additional DHS OIDs which are valid of the certificate is issued prior to 2008.
- Specifically, DHS common authentication medium hw, DHS common authentication high, and DHS common card authentication.

3.3.3

- Added catching of two exceptions during LDS Security Object creation.
- Added catching of exception if a container cannot be retrieved (does not exist).

3.3.4

- Added checking of error codes in USE Case PIV Authentication Key. Output appropriate and accurate error message depending on error

3.4.0



- Added buffering of containers feature for running multiple tests.
- Added challenge vs. public key modulus check to make sure challenge does not exceed public key modulus value.

3.5.0

- Improved error reporting for biometric, certificate, and digital signature tests.
- Removed FAIL messages from results when a test has not been executed. Instead, the result is left blank.
- Added error forwarding to results and reports.

3.5.1

- Intermediate version with minor bug fixes (debug)

3.5.2

- Intermediate version with minor bug fixes (debug)

3.5.3

- Intermediate version with minor bug fixes (debug)
- Digital signature conformance Test #57 transmit failure issue addressed
- Result reporting modified heavily

3.6.0

- Report generation pdf and html consolidated to 2 files.
- Report look and feel different, as well as contents of reports.
- Completely changed reporting system from parsing XSL to java

3.7.0

- Added Expected and Actual results column to display the Expected and Actual contents of a container IF it can be read.
- Modified Exception catching to be more robust and provide more information.

3.7.1

- Added additional AP Mapping column to Reporting, read from APMapping.xml

3.7.2

- Added "EP." to precede each AP Mapping value
- Right formatted Legend
- Expanded PDF
- Changed Date to Card Manufacturer Type
- Merged IUT cell with blank cell

4.0.1

- Fixed the piv-interim indicator extension test case to allow both TRUE and FALSE values
- Added support for SP 800-78-1



4.0.2

- Minor bugfix in xml file for report generation.

4.0.3

- Bugfix in acceptance OIDs affecting CHECK_digital_signature_conformance tests #15 (CHUID), 34 (fingerprints), 53 (facial image), 65 (security object)

4.0.4

- Bugfix in retrieving certificate generation date within signed attributes.
- SP 800-78-1 indicator added to heading of reports.

4.0.5

- Bugfix in verifying signature for private/public key pair integrity tests - CHECK_certificate_profile_conformance #8, #16, #23, #33.
- Support for testing private/public key pair integrity when using EC keys for CHECK_certificate_profile_conformance #8, #16, #23, #33
- Bugfix for always authenticating to PIV Card during retrieval of data containers (i.e. sending PIN)

4.0.6

- Bugfix for pin authentication for unique case CHECK_digital_signature_conformance test #57

4.0.7

- Bugfix for compatibility with Java 1.6.0 where the 'Tests' consolidated page was not getting populated with the tests run results.
- Generates fewer shortcuts in the start menu. Added an 'Uninstall' shortcut in the start menu for this tool.

4.0.8

- Graceful handling of null pointer exceptions in CHECK_digital_signature_conformance tests #15,16 & 36.
- Shows correct tool version in reports also now.

4.0.9

- Bug fix for reading card data in the CHECK_certificate_profile_conformance tests.

5.0.1

- Updated changes for SP 800-73-2:
 - Added new discovery object and its tests.
 - Added new fields to CHUID & Printed Information.
 - Updated Security Object tests to include new object & fields.
- Bug fixes to the CHECK_digital_signature_conformance tests to get the right signing time value from PIV Authentication certificate if it is not present in the container/object's signed info.



5.0.2

- Added content checks to fields of all containers and tested in BER_TLV_Conformance tests.

5.0.3

- Added a configuration setting to enable/disable the content checks. Tests affected when this is enabled are: BER_TLV_Conformance test #1, 3, 6, & 12
- The smart card readers attached to the system now come up as a list, and the reader can be selected from it.
- Removed PUK_VALID setting from Configuration.
- Added PIN Fail checking so that if a test fails on PIN verify, no other tests are run. A button is provided to the user to re-enable the tests.
- Added a thread to keep check on Exchange APDU with card so that test can exit gracefully if the card stops responding.
- Removed field length restriction checks on certificate, chuid asymmetric signature, fingerprint block and facial image as per 800-73-2 Tables 8,9,10 & 12. Tests affected are BER_TLV_Conformance test #3, 4, 5, 7, 8, 9, 10

5.1.0

- Formatted the summary output for logs of BER_TLV_Conformance tests (All tests under this sub group affected).
- Updated library for compatibility with Windows Vista.
- Better handling of card reader error reporting.
- Updated test requirements as per the Evaluation Program Approval Procedure ver 12.1.0 (All tests affected by this change in the Overview page and Report page.)
- Changed Install Path to enable FDCC User Mode Installation.
- Updated the report page to show all expected and actual values of the content check.
- Bug in parsing of FASCN fixed for OI & POA.

5.2.0

- Updated the CCC content verifier to generate correct logs and test CardId.
- New sample data objects included with tool.

5.2.1

- Fixed some BER-TLV related test/log info.

5.3.0

- Changed GUID to binary from numeric.
- Added check in CHUID certificate algorithm extraction to support SHA1 and SHA256.
- Added check for PIN preference from the Discovery object.
- Changed to allow all ASCII characters in content check of printed name.
- Length check removed on biometric data field.
- Length check verify changed from variable to fixed length for: discovery object elements, ORGANIZATIONAL_ID(CHUID), DUNS(CHUID)
- ECDSA issues fixed for certificate_profile tests.



6.0.0

Updated to SP800-73-3 & SP 800-78-2:

- Added Iris object, Key history Object, 20 X509 Key Management Certificate Objects.
- Added 22 tests to BER-TLV conformance tests.
- Removed CCC content check for CARD RID, Card Type and PKCS value.
- Printed Information Address affiliation line 2 is now optional.
- Removed RSA key size 4096 to support SP800-78-2.

6.1.0

- Removed Content check from Printed Info - Agency Serial number.
- Updated Printed Info BER-TLV check for Serial number& Issuer Identification to be Fixed Length of 10 & 15 respectively.

6.1.1

- Removed all card writing capability.

6.2.0

- Added 20 individual Options to select/deselect the retired key management certificates.
- Fixed Discovery Object ACR_PIN 0x40 issue.
- Fixed issue with Iris object hash in Security Object.
- Updated bouncy castle libraries to version 1.6 - 145
- Updated tool to java 1.6
- Added support for EC 384