

|         |  |                 |                          |
|---------|--|-----------------|--------------------------|
| Cert. # | Product name   | Vendor          | Issue date / update date |
| 42      | HID Global ActivID Applet Suite v2.7.4 on Gemalto TopDL v2.1 | HID Global, Inc | 7/7/2017                 |

| Tested Features  |             |                        |                      |                      |               |               |               |                  |                  |                |                |
|--|-------------|------------------------|----------------------|----------------------|---------------|---------------|---------------|------------------|------------------|----------------|----------------|
| Algorithm Description →<br>Tested combinations of key and algorithm                                  |             | 3 Key Triple DES - ECB | RSA 1024 bit modulus | RSA 2048 bit modulus | AES-128 - ECB | AES-192 - ECB | AES-256 - ECB | ECC: Curve P-256 | ECC: Curve P-384 | Cipher Suite 2 | Cipher Suite 7 |
| Key ↓  | Algorithm → | 00/03                  | 06                   | 07                   | 08            | 0A            | 0C            | 11               | 14               | 27             | 2E             |
| PIV Secure Messaging key (04)  |             |                        |                      |                      |               |               |               |                  |                  | x              | x              |
| PIV Authentication key (9A)  |             |                        |                      | ✓                    |               |               |               | x                |                  |                |                |
| PIV Card Application Administration key (9B)   |             | x                      |                      |                      | x             | x             | x             |                  |                  |                |                |
| Digital signature key (9C)   |             |                        |                      | ✓                    |               |               |               | x                | x                |                |                |
| Key management key (9D)  |             |                        |                      | ✓                    |               |               |               | x                | x                |                |                |
| Retired Key management keys (80-95)  |             |                        | x                    | ✓                    |               |               |               | x                | x                |                |                |
| Card Authentication key (9E)   |             |                        |                      |                      |               |               |               |                  |                  |                |                |
| Asymmetric   |             |                        |                      | ✓                    |               |               |               | x                |                  |                |                |
| Symmetric  |             | x                      |                      |                      | x             | x             | x             |                  |                  |                |                |
| Maximum number of retired keys tested  |             |                        |                      |                      |               |               |               |                  |                  |                | 5              |
| On-card key history function tested?   |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Off-card key history function tested?  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Secure Messaging tested?   |             |                        |                      |                      |               |               |               |                  |                  |                | Yes            |
| Crypto Suites tested?  |             |                        |                      |                      |               |               |               |                  |                  |                | CS2            |
| Intermediate CVC Tested?   |             |                        |                      |                      |               |               |               |                  |                  |                | Yes            |
| Use of Local PIN tested?   |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Use of Global PIN tested?  |             |                        |                      |                      |               |               |               |                  |                  |                | x              |
| Local PIN Preferred tested?  |             |                        |                      |                      |               |               |               |                  |                  |                | x              |
| Global PIN Preferred tested?   |             |                        |                      |                      |               |               |               |                  |                  |                | x              |
| Use of OCC tested?   |             |                        |                      |                      |               |               |               |                  |                  |                | x              |
| VCI tested with pairing code?  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| VCI tested without pairing code?   |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| <b>Mandatory and conditional data objects tested</b>   |             |                        |                      |                      |               |               |               |                  |                  |                |                |
| Card Capability Container  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Card Holder Unique Identifier  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| X.509 Certificate for PIV Authentication   |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| X.509 Certificate for Card Authentication  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| X.509 Certificate for Digital Signature  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| X.509 Certificate for Key Management   |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Cardholder Fingerprints  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Cardholder Facial Image  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Security Object  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| <b>Optional containers tested</b>  |             |                        |                      |                      |               |               |               |                  |                  |                |                |
| Printed Information  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Discovery Object   |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Key History Object   |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Retired X.509 Certificates for Key Management  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Cardholder Iris Images   |             |                        |                      |                      |               |               |               |                  |                  |                | x              |
| Biometric Information Templates Group Template   |             |                        |                      |                      |               |               |               |                  |                  |                | x              |
| Secure Messaging Certificate Signer  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| Pairing Code Reference Data Container  |             |                        |                      |                      |               |               |               |                  |                  |                | ✓              |
| <b>Notes</b>   |             |                        |                      |                      |               |               |               |                  |                  |                |                |
| ✓ indicates the feature has been tested.<br>x indicates the feature is not supported by the product. |             |                        |                      |                      |               |               |               |                  |                  |                |                |