PRODUCT INFORMATION BULLETIN

ID-One PIV® v2.3.2
The electronic Identity card compliant with US specifications
Table of contents

1. Foreword ......................................................................................... 3

2. Introduction to PIV cards features .................................................. 4
   2.1. On-Card Fingerprint Verification ................................................. 4
   2.2. Key History Support ................................................................ 4
   2.3. Full Crypto Support ................................................................ 4
   2.4. AES Based Secure Messaging ..................................................... 4
   2.5. Iris Image Container ................................................................. 4
   2.6. Dynamic PIN Policy ................................................................. 4
   2.7. Extended Length APDUs ........................................................... 5
   2.8. Flexible Containers .................................................................. 5
   2.9. Additional keys......................................................................... 5
   2.10. Binary Files Support ................................................................. 5
   2.11. Key Usage control .................................................................. 5
   2.12. Multiple Cardholder Verification Methods .................................. 5
   2.13. Control Contactless Functionality ............................................ 6
   2.14. ID-One PIV Awards Won: ......................................................... 6

3. PIV Certifications............................................................................. 6
   3.1. FIPS 201 Compliance Certification .............................................. 6
   3.2. FIPS 140-2 Compliance Certification ........................................... 7

4. Card body ........................................................................................ 7
   4.1. Magnetic Strip .......................................................................... 7
   4.2. Hybrid cards ........................................................................... 7
   4.3. Printing and Visual security features ......................................... 7

5. Technical characteristics ................................................................. 9
   5.1. ID-One PIV® v2.3.2 application features ..................................... 9
   5.2. ID-One™ Cosmo V7.0 platform features .................................... 10
1. Foreword

Oberthur Technologies is the most successful provider of high security credential cards for nationally recognized identification programs such as the Department of Defense Common Access Card, The Department of Homeland Security Transportation Worker Identification Credential, and most of the US Federal Government Agencies. Oberthur Technologies has been the leader in providing Personal Identification Verification (PIV) cards worldwide and our implementation serves as the baseline in the Smart Card industry.

- Oberthur Technologies’ PIV card is satisfactorily in use by over 103 federal government agencies. Our market share continues to grow beyond 95% as some of the PIV customers move to Oberthur from competitors given our PIV cards and services offered are superior to the competition.

- Oberthur Technologies PIV card is widely used by several large private enterprises such as Lockheed Martin, Northrop Grumman, Booz Allen Hamilton, AMTRAK for their PIV based Employee ID cards amongst many others.

Having successfully delivered PIV cards and services for such a large market segment, Oberthur Technologies has gathered invaluable experience in the process and has applied them in establishing infrastructure and procedures best suited for PIV solutions. If chosen, Oberthur Technologies will apply this expertise to ensure that our client’s PIV based deployment is a success.

- Oberthur Technologies was first to have a FIPS 201 validated PIV cards back in 2006. Oberthur Technologies was first to have a PIV card validated for the latest PIV specifications in 2009.

- Oberthur Technologies was first to offer a PIV card that supports ALL PIV crypto (including Elliptic Curve Cryptography).

- First PIV card to support On-Card fingerprint comparison; that could be used as an alternative to PIN for performing Cardholder verification.

- First PIV card to market that supports Key History mechanism for storing retired key management keys, and associated certificates.

- Oberthur is the ONLY provider with both the PIV Card and PIV Centralized Bureau Service on the General Services Administration Approved Products List (GSA APL).

With the clear demonstration of technology leadership, our client can rest assured to get the best technology in the market and will rely on a partner that will keep our client ahead of the technology curve.

With a track record of over 150 years in the high security business, over USD $ 1.3 Billion dollars in yearly sales, combined expertise described above assures our client that by choosing Oberthur Technologies, our client would be relying on a low risk, highly qualified partner.
2. Introduction to PIV cards features

Following is the description of the proposed PIV cards from Oberthur Technologies. The ID-One PIV card has been specifically designed by Oberthur to offer a fully validated PIV End Point card for US Federal Agencies as well as extend its usage outside of the US Federal community for PIV based implementations to benefit from this standard. Following are some of the key ID-One PIV features, some of them are on top of FIPS 201 current minimum requirements (SP 800-73-3).

2.1. On-Card Fingerprint Verification
ID-One PIV application includes an optional Secure Fingerprint On-Card Comparison application (On-Card Matcher). A native implementation that provides the ability to perform cardholder authentication based on fingerprint verification performed inside the card that is available in combination with or in place of the Cardholder PIN. Unlike other implementations that are designed to work with proprietary fingerprint capture devices, Oberthur’s implementation aligns with International Standards such as ISO/IEC 19794-2 enabling it to work independent of the fingerprint device vendors. Oberthur Technologies On-Card Fingerprint Verification algorithm is validated by NIST to comply with the PIV interoperability specifications. Oberthur Technologies On-Card matcher delivers exceptional performance in terms of speed, accuracy and interoperability. It is the fastest algorithm that passed NIST’s MINEX II phase III evaluation with an average of 0.28 seconds for a positive match. Oberthur ID-One PIV card is the ONLY PIV card (FIPS 201 validated card) to have passed NIST’s MINEX testing.

2.2. Key History Support
ID-One PIV supports key history object (as specified in SP800-73-3) with a provision to store on the card up to 20 retired management keys and associated certificates.

2.3. Full Crypto Support
ID-One PIV® is the ONLY PIV Card to support all the Cryptographic algorithms specified in PIV specifications (SP800-78-2), including 2TDEA, 3TDEA, AES, RSA, ECDSA and ECDH.

2.4. AES Based Secure Messaging
The ID-One PIV® supports AES based secure messaging protocol (‘OT-SCP03’) in both contact and contactless modes. This provides additional security for key injection. Secure channel protected with stronger key (such as AES) is needed to satisfy NIST recommendation for key loading.

2.5. Iris Image Container
ID-One PIV® supports Iris image container introduced in SP800-73-3.

2.6. Dynamic PIN Policy
ID-One PIV® application supports Discovery Object container introduced in SP 800-73-2 that contains PIN policy information. Card application behavior concerning Global PIN
can be dynamically changed by overwriting the PIN policy in the Discovery object container, either to enable or prohibit Global PIN privilege to grant access.

2.7. Extended Length APDUs
ID-One PIV® supports extended length APDUs for command exchange. Extended length provides greater flexibility and performance when handling large size data compared to command chaining usage. Up to 32 Kilo bytes of data can be exchanged in each direction within a single command. For example, entire x.509 certificate can be written to the card or from the card using a single APDU command. This eliminates need for time-consuming command chaining. Extended length usage coupled with fact that ID-One PIV 2.3.2 is based on a new generation chip that is faster, Personalization time is cut in half for most cases (Compared to previous generation PIV Cards).

2.8. Flexible Containers
To increase flexibility in customization, the ID-One PIV® application has been extended to support containers outside of FIPS 201 namespace. Any number of additional containers with up to 3-byte tag and configurable access conditions can be created. The number of containers that can be created is only limited by amount EEPROM space available on the card. Containers can store data either in proprietary SP-800-73 format or in pure ISO/IEC 7816 format. This feature for example can be used in storage of additional data outside of the PIV namespace.

2.9. Additional keys
The ID-One PIV® allows creation of additional keys with customized access conditions and roles at any time during the card’s lifecycle. This feature can be used for example in storage of expired private keys for key management purposes or for storing keys needed for protecting additional containers.

2.10. Binary Files Support
Support is provided for binary files with custom access conditions accessible using read binary and update binary APDU’s. These files can be used to store legacy Prox identification numbers (such as HID, Indala) protected with mutual Authentication if desired.

2.11. Key Usage control
The ID-One PIV® supports an optional Key Usage counter associated with each cryptographic key to limit the maximum number of uses of a given key. This counter is decremented each time the key is used. The key becomes unusable when the usage counter reaches zero. It is possible for the card administrator to disable or reinitialize this counter in post-issuance.

2.12. Multiple Cardholder Verification Methods
The ID-One PIV® card supports multiple methods to perform Cardholder Verification (CHV). Cardholder can be authenticated with:

- Local PIN Verification: In this case, authentication status is valid only for the currently selected application.
Global PIN Verification: In this case, the authentication status is made available for all the applications that may choose to use it as a substitute for the local PIN verification.

On-Card Fingerprint Verification.

Each instance of the ID-One PIV® application can be configured during personalization to support combination of available CHV methods.

2.13. Control Contactless Functionality

To provide additional protection against skimming when the cardholder is in higher risk environment such as when travelling overseas, a command to temporarily disable all PIV contactless functionality is included. The contactless functionality can be reversibly disabled at the PIV application level or at the card level (which essentially turns it into a contact only card).

2.14. ID-One PIV® Awards

There are two card models available based on ID-One PIV platform:

1. Oberthur ID-One PIV® 128k Dual Hybrid Card: This model contains a contact module along with two antennas, one for ISO 14443 contactless interface and the other for HID Prox. This card will have technical features and functionality as required by FIPS 201, and the GSA APL, in addition, will have Corporate 1000 HID Prox.

2. Oberthur ID-One PIV® 128k Dual Interface Card: This model is standard Dual interface PIV card containing a contact module along with an antenna for ISO 14443 contactless interface. This card will have technical features and functionality as required by FIPS 201, and the GSA APL.

3. PIV Certifications

3.1. FIPS 201 Compliance Certification

The Oberthur ID-One PIV® Card has been validated by NIST for FIPS 201 Compliance. The original certificate can be downloaded from the NIST web site at http://csrc.nist.gov/groups/SNS/piv/n pivp/validation_lists/PIVCardApplicationValidationList.htm

Certificates # 1 (SP-80073-1), # 18 (SP-80073-2), # 19 (SP-80073-2). Please note that although ID-One PIV implements SP-800-73-3 features, NIST labs are not yet equipped to validate compliance with SP800-73-3.
3.2. FIPS 140-2 Compliance Certification

The Latest version of Oberthur ID-One PIV® Card with the above “FIPS 201 Compliant” application is currently being validated by NIST for compliance with FIPS 140-2 requirements, this process is in the final Stages and the certificate is expected sometime this month.

Our earlier version of the PIV Card was the first PIV Card to get a FIPS 140-2 certification. It is certified with the following security levels:

<table>
<thead>
<tr>
<th>Roles, Services, and Authentication:</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Security:</td>
<td>Level 3</td>
</tr>
<tr>
<td>EMI/EMC:</td>
<td>Level 3</td>
</tr>
<tr>
<td>Design Assurance:</td>
<td>Level 3</td>
</tr>
<tr>
<td>Overall:</td>
<td>Level 2</td>
</tr>
</tbody>
</table>

The original downloaded from the NIST web site at http://csrc.nist.gov/cryptval/140-1/1401val2006.htm#668

In addition to being FIPS 140-2 certified with an overall security level 3, the Oberthur dual interface smart card was extensively tested by the National Security Agency (NSA). NSA, whose entire mission is built around security, has specifically recognized the Oberthur card for its high level of security features. It is after reading the NSA security assessment report that the U.S. Department of Defense (DOD) decided to migrate its current Common Access Card (CAC) program to use dual Interface cards.

4. Card body

Card body for our client will be a composite card made out of PET/PVC plastic and meets durability and physical characteristics requirement by the PIV specification (FIPS 201-1).

4.1. Magnetic Strip

Oberthur Technologies ID-One PIV® Dual Interface Smart Cards optionally offers a HiCo Magnetic stripe with 3 tracks and with coercively of 4000 Oe.

4.2. Hybrid cards

Oberthur Technologies ID-One PIV® Dual Hybrid Smart Cards offer genuine HID-Prox Inlay (sourced from HID) in the card body capable of storing 35-bit format data. In partnership with HID, Oberthur has established a process to procure and program HID inlays. This established process has been successfully used for several government and Non-government customers of Oberthur Technologies.

4.3. Printing and Visual security features

Oberthur Technologies is the world leader in high security printing, thereby offering the most advanced anti-counterfeiting features available today for smart ID cards.

Oberthur’s personalization facilities are Security Certified in accordance with the most stringent physical and logical procedures imposed by Visa, MasterCard and American Express. We have capabilities for producing a card with a variety of security features that are harder to counterfeit than currency. Our ID-One™ High Security Card’s durable
plastic body can include all or any combination of the multiple security features shown in Figure 1 below.

Our clients can choose between a variety of security features such as design, inks and security patches that are impossible to reproduce without advanced printing technologies available only to authorized companies. Additionally, since matching visual identification with the chip and card personalization data is critical, Oberthur has developed a robust architecture to provide accurate matching.

As shown above, the range of the visual identification options includes the following methodologies for secure background and secure personalization, any of which can be easily and economically incorporated into our clients smart ID card:

- **Guilloche**: A pattern of fine continuous lines which form a unique image that can only be recreated with the equipment, software and parameters used in creating the original design.

- **Rainbow**: A technique whereby two or more colors of ink are printed simultaneously to create a controlled merging of the colors, similar to the effect seen in a rainbow.

- **Relief Design (Medallion)**: A security background design incorporating an image generated in such a way as to create the illusion that it is embossed or debossed on the substrate surface.

- **UV (Ultraviolet Ink)**: Ink visible only when exposed to UV light.

- **Hologram**: A generic or customized three-dimensional image, impossible to reproduce.

- **Special Patented Inks**: Inks formulated to be detected using special equipment only.
5. Technical characteristics

5.1. ID-One PIV® v2.3.2 application features

<table>
<thead>
<tr>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>• EEPROM Size 128K (144K).</td>
</tr>
<tr>
<td>• NIST Specification Compliance: SP-800-73-3 (note it is backward compatible with SP 800-73-2, SP 800-73-1)</td>
</tr>
<tr>
<td>• Supports for All PIV Cryptographic Algorithms (as specified in SP800-78-2 for ECDSA, ECDH, RSA, AES, 3DES for all key lengths).</td>
</tr>
<tr>
<td>• Supports key history mechanism, up to 20 retired certificates and keys can be stored on the card.</td>
</tr>
<tr>
<td>• Supports Extended Length APDU for fast data access.</td>
</tr>
<tr>
<td>• Supports On-Card Fingerprint Comparison functionality (NIST MINEX II validated, the Only PIV card to do so)</td>
</tr>
<tr>
<td>• Secure Channel Support using OT-SCP03 Protocol (AES Based, the Only PIV card to do so)</td>
</tr>
<tr>
<td>• Supports IRIS Image Container as specified in SP-800-73-3</td>
</tr>
<tr>
<td>• PIN Discovery Object With Dynamic Policy</td>
</tr>
<tr>
<td>• Supports Binary Files With custom access conditions</td>
</tr>
<tr>
<td>• Additional Custom Data Containers with custom access conditions</td>
</tr>
<tr>
<td>• Support For Additional Keys: Up to 256 keys can be created on the card with custom access conditions</td>
</tr>
<tr>
<td>• Functionality to disable Contactless access at a Card and applet level.</td>
</tr>
</tbody>
</table>

Please note that although ID-One PIV® implements SP-800-73-3 features, NIST labs are not yet equipped to test compliance with SP800-73-3. We are actively involved in that process.
### 5.2. ID-One™ Cosmo V7.0 platform features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEPROM</td>
<td>Up to 128K of EEPROM (Total Space 144K)</td>
</tr>
<tr>
<td>Silicon Provider</td>
<td>Dual source (Same operating system works on multiple chips, this offers supplier sourcing redundancy)</td>
</tr>
</tbody>
</table>
| Communication Protocol                                                | • T=1, T=CL, type A or type B (First PIV card to support Type B, note that all the readers on the GSA APL are required to support both type A & B)  
• MIFARE Classic™ emulation (Can be activated if desired)  
• Communication Speed: Ultra fast communications (new ISO 7816-3 & 14443)  
• 625,000 bauds at 5Mhz in contact (T=0 and T=1)  
• 847,000 bauds full duplex in Contactless |
| Java Card 2.2.2                                                        | • RMI,  
• Logical Channel support  
• Garbage Collector  
• Supports new cryptographic API  
• Extended Length APDU as defined in ISO 7816 |
| Cryptographic Features                                                | • Compliant with FIPS 140-2, SP 800 78-2.  
• DES, 3 DES (2 and 3keys)  
• AES 128/192/256bits  
• RSA from 512 to 2048 bits  
• RSA key generator :1024 to 2048 bits  
• Elliptic curve DSA GFP algorithm 160/192/224/256/384/521 bits  
• ECC key generation.  
• Elliptic curves Diffie-Helman 160/192/224/256/384/521 bits  
• SHA1, SHA-256,SHA-384, SHA-512  
• True Random generator compliant to FIPS 186-2 |
| Global platform 2.1.1                                                 | • DAP RSA : to secure applet loading with PKI  
• Secure channel protocol SCP 01/SCP 02 and SCP03 (based on AES algorithm)  
• GP 2.1.1 commands : Store Data / Process Data / Extradite  
• Delegated Management |
| Security mechanisms                                                   | • Implementation of all the security mechanisms needed for Common criteria and FIPS certifications.  
• Compliant with the Security Guidelines against SPA, DPA and DFA attacks.  
• The ID-One Cosmo V7 is the 1st java card platform compliant with the NSA Suite B recommendations. |
| Biometry                                                              | • Java Card API to access On-Card fingerprint functionality. |
| Platform Certifications                                               | • FIPS 140-2 level 3  
• Common Criteria EAL5+ |