## Table of contents

1. Overview ........................................................................................................................................... 3

2. Detailed features and typical use cases ............................................................................................. 4
   2.1. Platform security .......................................................................................................................... 4
   2.2. Platform cryptography .................................................................................................................. 4
   2.3. Identification ............................................................................................................................... 4
   2.4. Authentication .............................................................................................................................. 5
       2.4.1. User authentication ............................................................................................................. 5
       2.4.2. Device authentication ......................................................................................................... 5
       2.4.3. Role Authentication ........................................................................................................... 6
   2.5. Digital Signature ......................................................................................................................... 7
   2.6. Data Storage ............................................................................................................................... 8
   2.7. Encryption/Decryption .................................................................................................................. 8
   2.8. Certificate Verification ............................................................................................................... 9
       2.8.1. Certificate format .............................................................................................................. 9
       2.8.2. Verification process ......................................................................................................... 9

3. Technical characteristics ..................................................................................................................... 12
   3.1. ID-One™ IAS v1 features .......................................................................................................... 12
   3.2. ID-One™ IAS v2 features .......................................................................................................... 13
1. Overview

ID-One™ IAS is Oberthur Technologies offer targeted at providing secure identification of online counterparts, and confidentiality tools for exchanges between them. It provides the following electronic services:

- Authentication by PIN of the card holder or the administrator (security officer)
- Authenticating remote administrator by cryptographic mechanism (symmetrical and asymmetrical)
- Mutual authentication of remote machines or servers using encryption tools (symmetrical and/or asymmetrical)
- Protection of data exchange integrity, confidentiality and authenticity;
- Import, export and generation of signature key, authentication key, ciphering/deciphering key
- Digital signature of emails and PDF documents
- Anonymity and non-traceability in contactless mode
- Protection against physical and intrusive attacks

In order to enable an easy and fast deployment of services based on ID-One™ IAS, Oberthur Technologies offers also a software suite including:

- The AWP suite, including a middleware compliant with PKCS#11, CSP, Minidriver standards which interfaces ID-One™ IAS v1 card with Computer-based applications such as Outlook, Adobe, or any Corporate applications
  ID-One™ IAS-ECC v1 is also interoperable with all IAS-ECC compatible third party middleware.
- A Software Development Kit for applets development and loading on the ID-One™ Cosmo platform

This product is compliant with the European specifications IAS-ECC for Electronic Citizen Card. ID-One™ IAS now exists in 2 versions ID-One™ IAS v1 and ID-One™ IAS v2 in line with GIXEL work. Both are based on Oberthur Technologies latest JavaCard™ platforms which are certified according to the Common Criteria specifications to the assurance level 5 augmented, also know as EAL5+. 
2. Detailed features and typical use cases

2.1. Platform Security

Thanks to the compliance with the requirements of a secure signature creation device (SSCD) as defined in European Directive 1999/93/EC (Annex III), ID-One™ IAS is therefore the perfect tool to be used for “advanced” and “qualified” digital signatures.

The security assessment conducted in accordance with Common Criteria has validated the compatibility with secure signature creation device protection profiles type 2 – Signature key Import (CEN/CWA 14169-2) and RSA and EC Key generation type 3 (CEN/CWA 14169-3).

The ID-One™ Cosmo v7 is an Open platforms certified CC EAL5+ and which hosts ID-One™ IAS application certified CC EAL4+. The certificate includes an application loading mechanisms. As a result even if a non-evaluated applet is loaded, the security of the ID-One™ IAS application is not compromised and its CC certificate remains valid.

2.2. Platform cryptography

ID-One™ IAS applications support PKI algorithms which allow strong authentication, Digital Signatures creation and strong encryption/decryption use-cases.

ID-One™ IAS v1 supports RSA (up to 2048bits keys), ID-One™ IAS v2 supports RSA (up to 2048bits keys) and Elliptic Curves (up to 521bits keys).

The key benefit of Elliptic Curves is that with a much smaller key, Elliptic Curves provide the same cryptographic strength. i.e. 192 EC is equivalent to 2048 RSA. For demanding use-cases mandating the use of RSA keys longer than 2048, we highly recommend our customer to use the EC keys above 192, e.g. 256, 384 or 512 or even 521.

In the following sections, we will refer to ID-One™ IAS for generic features supported by both versions of Oberthur Technologies IAS applications, and we will namely refer to ID-One™ IAS v1 and ID-One™ IAS v2 for features only supported by one of the IAS application.

2.3. Identification

Identification is required everyday when citizens and government interact on a named basis. An example could be the necessary “identity step” for a requester to get access to his personal information records e.g. tax, vehicle registration, and payment status for local government services... In our case, identify a person, over the Internet, consists in retrieving his personal credentials from his/her smart card.
2.4. Authentication

Authentication consists in proving a claimed identity. Three different authentication processes are available in ID-One™ IAS card:

- User authentication
- Device authentication
- Role authentication

2.4.1. User authentication

User authentication consists in proving the identity of the cardholder to the card. ID-One™ IAS supports knowledge based authentication which relies on something the cardholder knows, i.e. a password or a PIN. Authentication is considered to be achieved when it has been established that the PIN or Password, stored in the card, matches the PIN or Password provided by the cardholder.

In addition, ID-One™ IAS v2 supports a certified Biometric PIN, where the card verifies that the holder is who he claims he is. This mechanism is called “Match-on-Card” as it is the card itself that compares the card holder fingerprint with the fingerprint(s) stored in the card. This version 2 can for example stored all 10 fingerprints of a card holder and the new algorithm embedded in this card is capable of comparing a given fingerprint against all recorded fingerprints in less than 1 second. This mechanism is called “1/n” Match on Card. Of course “1/1” match-on-card is still supported with performances below 100ms for a positive match.

2.4.2. Device authentication

Device authentication consists in proving the identity of the cardholder to an external entity (e.g. host computer system) or proving to the card the identity of an external identity (e.g. card management system).

ID-One™ IAS supports three device authentication schemes: symmetric, asymmetric and device authentication, as detailed below:

Symmetric authentication scheme: ID-One™ IAS implements the mutual authentication scheme using symmetric keys as shown in the e-sign-K document.

A successful authentication mandates that the customer card and the external entity share the same secret key. Actually 2 keys are used for improved security:

- \( K_{\text{ENC}} \), for confidentiality (i.e. message encryption)
- \( K_{\text{MAC}} \) for integrity protection (i.e. message authentication code MAC)

Asymmetric authentication scheme: Asymmetric authentication employs a pair of keys, both are generated in one operation and while the two are related, one cannot be computed from the other. One key is kept secret – the private key – and the other can be given to anyone – the public key. The maths associated with this scheme makes it so that...
anything encrypted with one key can only be decrypted with the other key. Let’s assume Alice holds the public key of Bob. Alice will be able to authenticate Bob following an asymmetric authentication protocol that can be described with three steps:

1. Alice sends a piece of information to Bob (usually called a challenge),
2. Bob signs this information with its private key and returns the result to Alice,
3. Alice verifies the signature with Bob’s public key.

Note: prior to asymmetric authentication protocol, Bob usually sends his public key to the Alice via his certificate (which Alice can verify).

ID-One™ IAS supports:

- RSA private and public key pairs (up to 2048 bits) which can be either:
  - Generated externally and loaded in the card when enrolling a user
  - Generated by the card (OBKG), only the public part leaves the card
- External authentication scheme
  - An external device authenticates to ID-One™ IAS card
- Internal authentication scheme
  - ID-One™ IAS card authenticates to an external device

**Device authentication with privacy protection:** In order to avoid the card disclosing private information, such as identity, ID-One™ IAS can require establishment of a secure channel session before any other operation. To do so, the process starts with an unauthenticated Diffie-Hellman key exchange which allows two entities to exchange a secret key over an unsecure medium without any prior secret; then the external entity authentication occurs thanks to asymmetric authentication scheme.

**Supplemental Access Control (SAC):** The SAC is a protocol design to agree on a shared secret key as to secure communications between the document and Inspection System. It is based on a password (which can take the form of the MRZ or a specific Card Access Number) and Diffie-Hellman cryptographic algorithm.

### 2.4.3. Role Authentication

Role authentication consists in authenticating an external entity to the card in order to associate to it a specific role (e.g. access rights). ID-One™ IAS supports two role authentication mechanisms: symmetric and asymmetric:

**Symmetric role authentication:** the process is similar to symmetric authentication scheme with the difference that a role is associated with symmetric key set stored in the card. A successfully authentication provides to the external entity all the access rights associated with the role.
Asymmetric role authentication: the process is similar to asymmetric authentication scheme with the difference that a role is associated with the public key that the external entity sends to the card. A successful authentication provides to the external entity all the access rights associated with the role.

2.5. Digital Signature

Handmade signatures are reputed unique per person and the expression of a positive consent of the signer over the content of a given document. Main applications of signature are related to official/legal or trade documents.

The same principles apply to the electronic world, where electronic signatures are done using the private key of the signer in the following manner:

1. A condensed version of the document (called Hash) is produced by the Client Application (e.g. Microsoft Outlook or Adobe PDF).
2. This hash is sent to ID-One™ IAS card and encrypted with the private key of the signer. The result is sent back to the Client Application and represents the digital signature of the signer for this document.
3. Clear email/document + digital signature + signer certificate (which include the signer’s public key) are concatenated in one message.
4. The Client Application of the recipient can validate the document by using the public key of the sender to verify the signature (decrypting the digital signature and comparing the result with the hash of the email/document). The Client Application will either provide you the document or will inform you that it failed to recognize the signer’s identity or signature.

ID-One™ IAS supports the step 2 above with 2 public key algorithms:
ID-One™ IAS v1 supports RSA (up to 2048bits keys),
ID-One™ IAS v2 supports RSA (up to 2048bits keys) and Elliptic Curves (up to 521bits keys).

2.6. Data Storage

ID-One™ IAS implements a full ISO 7816-4 file systems allowing to manage securely all the data needed for authentication or other purpose.

The ISO 7816-4 norm is specifying a standard way for smart card to handle data. Instead of being handled internally in a proprietary way, these data are put in files, within a tree-based file structure.

Each file within the file structure is identified through its File Identifier (coded on two bytes). Files can be of different types. Within the multiple file types defined by the ISO 7816-4 standard, the ID-One™ IAS applet supports the following types:

- **Dedicated files** (DF). These files are like directories on a PC. They can hold other files.
- **Binary files** (also called transparent files). These files are non structured files, used to hold raw binary data from and to the smart card terminal.

2.7. Encryption/Decryption

Encryption is the conversion of data into a form (called a cipher text) which cannot be easily understood by anyone who would intercept the message. Decryption is the process of converting encrypted data back into its original form (plaintext), so it can be understood by the authorized person.

ID-One™ IAS supports both symmetric and asymmetric encryption/decryption.

**Symmetric encryption/decryption**: the same key is shared between sender and receiver; a message encrypt by a symmetric key can only be decrypted by the same key.

ID-One™ IAS supports symmetric encryption/decryption:

- ID-One™ IAS supports TDES keys (key length: 128 and 192 bits)
- ID-One™ IAS v2 supports, in addition, AES (key length: 128, 192, 256 bits)

**Asymmetric encryption/decryption**: this process employs a pair of keys, a private key (kept secret) and a public key (can be given to anyone). A message encrypted with one key can only be decrypted with the other key.

ID-One™ IAS supports asymmetric encryption/decryption:

- ID-One™ IAS v1 supports RSA keys (key length: up to 2048 bits)
- ID-One™ IAS v2 supports in addition Elliptic Curves (key length: 160, 192, 224, 256, 320, 384, 512, 521 bits)
2.8. Certificate Verification

Trusting the external entity public key is the main requirement to validate before starting asymmetric authentication and signature verification processes.

The certificate verification allows the card to trust the public key stored in the certificate. So, asymmetric authentication and signature verification processes generally start by transporting external entity certificate into the card, so that the card can retrieve the external entity public key from the certificate and trust it after certificate verification.

2.8.1. Certificate format

ID One™ IAS supports Card Verifiable Certificate (CVC) format which is smaller and easier to analyze for smart card than X509 certificate. A CVC is a data container containing a RSA public key and information demonstrating that the public key is trustable, and it possibly contains some role assigned to the certificate owner that will grant him access to services or files on the card.

2.8.2. Verification process

A user certificate is always signed by a Certification Authority (CA). This CA also has a certificate that can itself be signed by another CA, leading to what is called a chain of trust. The top level CA has a certificate signed with its own key (Root Certificate or Self-signed Certificate). Such certificates must be loaded on the card during personalization in a secure environment.

When an external entity wants a user certificate to be verified by the card, it shall check which CA Root Certificate the card already knows. If the user certificate was not signed by a CA already known by the card, it shall present all required certificate to the card from the first one (that was signed by the CA known by the card) down to the user certificate the external entity want the card to verify.
3. Product Availability

3.1. Card Body

For the Identity markets, plastics and printing features are fully part of the security of the Cards.

Oberthur Technologies purposes a complete offer for card body:

- **Long-life plastics** like PETF, Polycarbonate
- **Printing security features** like Rainbow Printing, Guilloche Patterns, Relief design, Numismatic background, Microprint, OVI, Ultraviolet printing, printed text, color photo, handwritten signature...
- **Overlay** to protect variable printing and introduce additional security features (transparent holograms, UV)

Oberthur Technologies received from Infograph the CWA 14641 certification for « High Security Printer ».

**ID-One™ Cosmo** is available in volume with a variety of plastic support according to your requirements.

The product can be delivered with or without personalisation. In the second case, Oberthur Technologies is able to perform electrical and graphical personalisation in one of its 30 service centers.

3.2. Middleware and Minidriver IAS

- **ID-One™ IAS v2**

ID-One™ IAS v2, is fully compliant with IAS v1 and adds up the key features presented above. This product is fully compliant with the European Standard, European citizen Card and eSign-K. A common Criteria certification EAL4+ PP-SSCD on ID-One Cosmo v7.1 is targeted for May 2013.

- **Middleware & Minidriver IAS**

The current middleware and Minidriver IAS are currently compliant with ID-One™ IAS v1. The full support of ID-One™ IAS v2 for Match-On-Card and Elliptic Curves will be added during 2013 in the next release of middleware and Minidriver IAS.
3.3. ID-One™ IAS v2 Modular Software architecture

ID-One™ IAS v2 has a modular software architecture where, next to fundamental software modules of IAS, there are optional modules that can be loaded to add advanced functionalities on a per-project basis. ID-One™ IAS V2 could be tailored to fit customer requests from a functional or from a free-memory point of view. The available optional modules are:

- **SAC** protocol support. Also known as PACE (Password Authenticated Communication Establishment) which is a secure contactless communication standard for secure electronic passport reading. PACE establishes Secure Messaging based on weak passwords (a few characters), but builds strong session keys, independent of the strength of the password: 6 character passwords are sufficient.
- **Biometric Match on Card** support
- **AES** Cryptographic algorithm support
- **ECC** functionalities support
# 4. Technical characteristics

## 4.1. ID-One™ IAS v1 features

<table>
<thead>
<tr>
<th>Certified applet loaded in ROM on an ID-One™ Cosmo v7.0.1, JavaCard™ platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Platform certificate:</td>
</tr>
<tr>
<td>• Application certificate:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configurable activation of communication protocols (contact/contactless)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>72K / 80k / 128K EEPROM</strong></td>
</tr>
<tr>
<td>Contact Protocols: T=0, T=1, PPS from 9600 to 614 400 bauds</td>
</tr>
<tr>
<td>Speeds: 106, 212, 424, 848 kbps.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>JavaCard Virtual Machine, RTE &amp; API compliant to JC 2.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Card Management &amp; API compliant to GP 2.1.1:</strong></td>
</tr>
<tr>
<td>• SCP01, SCP02 and proprietary SCP03 based on AES support</td>
</tr>
<tr>
<td>• DAP, Delegated Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Form factors:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cards in PVC, PVC/PETF or Polycarbonate</td>
</tr>
<tr>
<td>• USB Tokens or Secure μSD</td>
</tr>
<tr>
<td>• Contactless modules or inlays</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supported algorithms:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data protection and confidentiality: 3DES-CBC (mode EDE) with double DES keys</td>
</tr>
<tr>
<td>• Data integrity protection and authenticity: ISO9797-1 algorithm</td>
</tr>
<tr>
<td>• Signature RSA PKCS#1 v1.5 with SHA-1 and SHA-256</td>
</tr>
<tr>
<td>• Hash SHA-1 or SHA-256</td>
</tr>
<tr>
<td>• RSA key generator ANSI X9-31 compliant</td>
</tr>
<tr>
<td>• RSA key 1024, 1536 and 2048 bits</td>
</tr>
<tr>
<td>• DH based on RSA 1024, 1536 and 2048 bits</td>
</tr>
<tr>
<td>• CVC certificates verification: RSA ISO9796-2 with SHA-1 and SHA-256</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Keys and Certificate management:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• RSA key import and On-board generation</td>
</tr>
<tr>
<td>• RSA keys in CRT format</td>
</tr>
<tr>
<td>• CVC certificates management</td>
</tr>
<tr>
<td>• Configurable activation of symmetric/asymmetric authentication</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-Certified extensions which can be loaded in EEPROM:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Elliptic Curve: EC DSA 160, 192, 224, 256, 320, 384, 512 and 521 bits</td>
</tr>
<tr>
<td>• AES 128, 192 and 256 bits</td>
</tr>
<tr>
<td>• Biometric Fingerprint Match-on-Card 1/1</td>
</tr>
</tbody>
</table>
4.2. ID-One™ IAS v2 features

Certified applet loaded in ROM on an ID-One™ Cosmo v7.1, JavaCard™ platform
- Platform certificate: Expected Q1 2013
- Application certificate: Expected Q4 2013

Configurable activation of communication protocols (contact/contactless)

<table>
<thead>
<tr>
<th>80k EEPROM</th>
<th>80k EEPROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Protocols: T=0, T=1,</td>
<td>Contactless Protocol: T=CL ISO 14443, Type B</td>
</tr>
<tr>
<td>PPS from 9600 to 614 400 bauds</td>
<td>Speeds: 106, 212, 424, 848 kbps.</td>
</tr>
</tbody>
</table>

JavaCard Virtual Machine, RTE & API compliant to JC 3.0.1 CE (exact same APIs than JC 2.2.2)

Card Management & API compliant to GP 2.2
- SCP02, SCP03 and proprietary SCP03
- DAP Verification and Mandated DAP Verification

Form factors:
- Cards in PVC, PVC/PETF or Polycarbonate
- Contactless modules or inlays

Supported algorithms:
- Data protection and confidentiality: 3DES-CBC (mode EDE) with double DES keys
- Data integrity protection and authenticity: ISO9797-1 algorithm
- AES 128, 192 and 256 bits
- Hash SHA-1, SHA-244, SHA-256, SHA-384, SHA-512
- RSA key generator ANSI X9-31 compliant
- RSA key 1024, 1536 and 2048 bits
- DH based on RSA 1024, 1536 and 2048 bits
- EC key 160,192,224,256,320,384,512,521 bits
- CVC certificates verification: RSA ISO9796-2 with SHA-1 and SHA-256

Keys and Certificate management:
- RSA and EC key import and On-board generation
- RSA keys in CRT format
- CVC certificates management
- Configurable activation of symmetric/asymmetric authentication

Biometrics support
- Biometric Fingerprint Match-on-Card 1/n