

BeID SDK Card Data

Document History

| Date | EIDMW Version | Description |
|------------|---------------|--|
| | | Legacy |
| 12/08/2022 | 5.1.8 | Added extra fields for the card A, EU and EU+ mentions |

This document contains the list of item names that can be used to collect data from the card when using the eIDSDK 5.1

Please read the “RSA Security Inc. Public-Key Cryptography Standards (PKCS)” document first, to understand the pkcs11 API. This document can be found in the doc folder (pkcs11-base-v2.40.pdf).

1 Introduction

The eID MW 5.1 SDK consists actually of a pkcs11 implementation (presented as a C library).

In order to use the SDK for creating signatures with the eID card, request the certificates, etc., one simply has to follow the pkcs11 API.

1.1 Card Data

The data stored on the card is presented to the developer as pkcs11 'objects'.

1.1.1 Certificates

The certificates can be retrieved by searching for objects which have their CKA_CLASS attribute set to CKO_CERTIFICATE

The following certificates can be found on the eID card v1.5:

- “Authentication”
- “Signature”
- “CA”
- “Root”

1.1.2 Card data

The identity and address data can be retrieved by searching for objects which have their CKA_CLASS attribute set to CKO_DATA.

When CKA_CLASS is not specified, no card data (object with CKA_CLASS equal to CKO_DATA) will be returned. This behaviour is implemented in this way because we do not want to read all data files e.g. when a webbrowser requests all items on the eID card (only to retrieve the certificates).

1.1.2.1 The files (unparsed)

You can retrieve the unparsed files by looking for objects which have their CKA_LABEL attribute set to one of the following:

| CKA_CLASS | CKA_LABEL | |
|-----------|----------------|------------------------------------|
| CKO_DATA | DATA_FILE | the identity data file |
| CKO_DATA | ADDRESS_FILE | the address file |
| CKO_DATA | PHOTO_FILE | the photo |
| CKO_DATA | SIGN_DATA_FILE | the signature of the identity file |

| | | |
|----------|-------------------|---|
| CKO_DATA | SIGN_ADDRESS_FILE | the signature of the address file |
| CKO_DATA | BASIC_KEY_FILE | The public basic key Only available on applet v1.8 cards |

Please note that no signature checks are performed by the eID SDK 5.1 when retrieving card data; it is up to the developer to check if the signature files match the corresponding files.

For more info about the files, please refer to the 'Belgian_electronic_identity_card_content.pdf' document.

1.1.2.2 Parsed Data

You can also retrieve parsed data that was contained within one of the above files:

Parsed data from the data file will have their CKA_LABEL attribute set to one of the following:

(All values are UTF-8 encoded, unless otherwise specified)

▲ parsed data from the identity file:

| CKA_CLASS | CKA_LABEL | |
|-----------|----------------------------------|--|
| CKO_DATA | card_number | |
| CKO_DATA | chip_number | |
| CKO_DATA | validity_begin_date | the card validity begin date |
| CKO_DATA | validity_end_date | the card validity end date |
| CKO_DATA | issuing_municipality | the card delivery municipality |
| CKO_DATA | national_number | |
| CKO_DATA | surname | |
| CKO_DATA | firstnames | |
| CKO_DATA | first_letter_of_third_given_name | |
| CKO_DATA | nationality | |
| CKO_DATA | location_of_birth | |
| CKO_DATA | date_of_birth | Birth date, encoded as (see below) |
| CKO_DATA | gender | M: man / F/V/W: woman |
| CKO_DATA | nobility | noble condition |
| CKO_DATA | document_type | type of document, for list of values, see below |
| CKO_DATA | special_status | 0: No status 2: Extended minority |
| CKO_DATA | photo_hash | hash of the photo file |
| CKO_DATA | duplicata | |
| CKO_DATA | special_organization | 1: SHAPE 2: NATO |
| CKO_DATA | member_of_family | (this is a boolean value) |
| CKO_DATA | date_and_country_of_protection | |
| CKO_DATA | work_permit_mention | |
| CKO_DATA | employer_vat_1 | |
| CKO_DATA | employer_vat_2 | |
| CKO_DATA | regional_file_number | |
| CKO_DATA | basic_key_hash | SHA384 hash of the public basic key Only available on applet v1.8 cards |

| | | |
|----------|-------------------|--|
| CKO_DATA | brexit_mention_1 | |
| CKO_DATA | brexit_mention_2 | |
| CKO_DATA | cardA_mention_1 | |
| CKO_DATA | cardA_mention_2 | |
| CKO_DATA | cardEU_start_date | |

"Date_Of_Birth": Birth date, encoded as
DD mmmm YYYY (Dutch and French card)
or DD.mmm.YYYY (German card)

| Birth months | | | | | | | | | | | | |
|--------------|-----|-----|------|-----|-----|------|------|------|------|-----|-----|-----|
| French | JAN | FEV | MARS | AVR | MAI | JUIN | JUIL | AOUT | SEPT | OCT | NOV | DEC |
| Dutch | JAN | FEB | MAAR | APR | MEI | JUN | JUL | AUG | SEP | OKT | NOV | DEC |
| German | JAN | FEB | MÄR | APR | MAI | JUN | JUL | AUG | SEP | OKT | NOV | DEZ |

"Document_Type" : type of document, can be one of the following values:

- 1: Belgian citizen
- 6: Kids card (< 12 year)
- 7: Bootstrap card
- 8: "Habilitation / Machtigings-" card
- 11: Foreigner card type A
- 12: Foreigner card type B
- 13: Foreigner card type C
- 14: Foreigner card type D
- 15: Foreigner card type E
- 16: Foreigner card type E+
- 17: Foreigner card type F
- 18: Foreigner card type F+
- 19: Foreigner card type H
- 20: Foreigner card type I
- 21: Foreigner card type J
- 22: Foreigner card type M
- 23: Foreigner card type N
- 27: Foreigner card type K
- 28: Foreigner card type L
- 31: Foreigner card type EU
- 32: Foreigner card type EU+
- 33: Foreigner card type A
- 34: Foreigner card type B
- 35: Foreigner card type F
- 36: Foreigner card type F+

^ parsed data from the address file:

| CKA_CLASS | CKA_LABEL | |
|-----------|---------------------------|--------------------------------|
| CKO_DATA | address_street_and_number | the streetname and number |
| CKO_DATA | address_zip | the zip-code of your town/city |

| | | |
|----------|----------------------|----------------|
| CKO_DATA | address_municipality | your town/city |
|----------|----------------------|----------------|

^ the RN certificate

The certificate used to sign the photo file can be found as pkcs11 object with CKA_CLASS attribute set to CKO_DATA, and CKA_LABEL set to CERT_RN_FILE

Although the CERT_RN_FILE is a certificate, we added it to the CKO_DATA objects, as it is not used for signing or authenticating and would only slow down the applications that are searching for the signing and authentication signatures on the card.

The purpose of the CERT_RN_FILE is to check the signatures of the data files.

| CKA_CLASS | CKA_LABEL | |
|-----------|--------------|----------------|
| CKO_DATA | CERT_RN_FILE | RN Certificate |

1.1.2.3 Record data

Starting with eID applet 1.8, an option will be available to retrieve the data stored in the identity or address file on a “per record” basis. This allows users of the SDK to retrieve only exactly that data from the eID card that is needed (as opposed to the parsed data, where the SDK will retrieve and parse the entire file, even if only one or a few labels are needed). This option is especially useful when privacy concerns come into play.

Proof of validity of this data might not be available on the initial applet v1.8 eID cards, which would mean that when using this “per record” data, there is no means to check if this data is authentic. Nor is (or can) it be verified in the pkcs#11 library.

As this data is actually a copy of the parsed data, the pkcs#11 library will not return these objects in a find object request that does not specifically search for it (i.e. their CKA_LABEL attribute needs to be specified)

^ per record data from the identity file:

| CKA_CLASS | CKA_LABEL | |
|-----------|---|-------------------------------------|
| CKO_DATA | record_card_number | Only available on applet v1.8 cards |
| CKO_DATA | record_cardchip_number | Only available on applet v1.8 cards |
| CKO_DATA | record_validity_begin_date | Only available on applet v1.8 cards |
| CKO_DATA | record_validity_end_date | Only available on applet v1.8 cards |
| CKO_DATA | record_issuing_municipality | Only available on applet v1.8 cards |
| CKO_DATA | record_national_number | Only available on applet v1.8 cards |
| CKO_DATA | record_surname | Only available on applet v1.8 cards |
| CKO_DATA | record_firstnames | Only available on applet v1.8 cards |
| CKO_DATA | record_first_letter_of_third_given_name | Only available on applet v1.8 cards |
| CKO_DATA | record_nationality | Only available on applet v1.8 cards |
| CKO_DATA | record_location_of_birth | Only available on applet v1.8 cards |
| CKO_DATA | record_date_of_birth | Only available on applet v1.8 cards |
| CKO_DATA | record_gender | Only available on applet v1.8 cards |
| CKO_DATA | record_nobility | Only available on applet v1.8 cards |
| CKO_DATA | record_document_type | Only available on applet v1.8 cards |
| CKO_DATA | record_special_status | Only available on applet v1.8 cards |
| CKO_DATA | record_photo_hash | Only available on applet v1.8 cards |
| CKO_DATA | record_duplicata | Only available on applet v1.8 cards |
| CKO_DATA | record_special_organization | Only available on applet v1.8 cards |

| | | |
|----------|---------------------------------------|-------------------------------------|
| CKO_DATA | record_member_of_family | Only available on applet v1.8 cards |
| CKO_DATA | record_date_and_country_of_protection | Only available on applet v1.8 cards |
| CKO_DATA | record_work_permit_mention | Only available on applet v1.8 cards |
| CKO_DATA | record_employer_vat_1 | Only available on applet v1.8 cards |
| CKO_DATA | record_employer_vat_2 | Only available on applet v1.8 cards |
| CKO_DATA | record_regional_file_number | Only available on applet v1.8 cards |
| CKO_DATA | record_basic_key_hash | Only available on applet v1.8 cards |
| CKO_DATA | record_brexit_mention_1 | Only available on applet v1.8 cards |
| CKO_DATA | record_brexit_mention_2 | Only available on applet v1.8 cards |
| CKO_DATA | record_cardA_mention_1 | Only available on applet v1.8 cards |
| CKO_DATA | record_cardA_mention_2 | Only available on applet v1.8 cards |
| CKO_DATA | record_cardEU_start_date | Only available on applet v1.8 cards |

^ per record data from the address file:

| CKA_CLASS | CKA_LABEL | |
|-----------|----------------------------------|-------------------------------------|
| CKO_DATA | record_address_street_and_number | Only available on applet v1.8 cards |
| CKO_DATA | record_address_zip | Only available on applet v1.8 cards |
| CKO_DATA | record_address_municipality | Only available on applet v1.8 cards |

1.1.2.4 Card Info

Extra information about the eID card can be found as object with CKA_CLASS attribute set to CKO_DATA, and CKA_LABEL set to:

| CKA_CLASS | CKA_LABEL | |
|-----------|-----------|-------------------------------|
| CKO_DATA | CARD_DATA | the extra card data as a file |

parsed info from this file can be found as objects with CKA_LABEL equal to:

| CKA_CLASS | CKA_LABEL | |
|-----------|-------------------------------|---|
| CKO_DATA | carddata_serialnumber | the extra card data as a file |
| CKO_DATA | carddata_comp_code | |
| CKO_DATA | carddata_os_number | |
| CKO_DATA | carddata_os_version | |
| CKO_DATA | carddata_soft_mask_number | |
| CKO_DATA | carddata_soft_mask_version | |
| CKO_DATA | carddata_appl_version | 0x11 0x00 for applet v1.1 cards 0x17 for applet v1.7 cards |
| CKO_DATA | carddata_glob_os_version | Only available on applet v1.7 cards |
| CKO_DATA | carddata_appl_int_version | |
| CKO_DATA | carddata_pkcs1_support | Only available on applet v1.7 cards |
| CKO_DATA | carddata_appl_lifecycle | Only available on applet v1.7 cards |
| CKO_DATA | carddata_pkcs15_version | Only available on applet v1.1 cards |
| CKO_DATA | carddata_key_exchange_version | |

| | | |
|----------|--------------------|-------------------|
| CKO_DATA | carddata_signature | Not yet available |
|----------|--------------------|-------------------|

The ATR of the card can also be requested by searching for objects with CKA_CLASS attribute set to CKO_DATA and CKA_LABEL set to “ATR”.

| CKA_CLASS | CKA_LABEL | |
|-----------|-----------|---------------------------------|
| CKO_DATA | ATR | the answer to reset of the card |

The personalisation versions of the card can also be requested by searching for objects with CKA_CLASS attribute set to CKO_DATA and CKA_LABEL set to:

| CKA_CLASS | CKA_LABEL | |
|-----------|----------------------------------|---|
| CKO_DATA | tokeninfo_graph_perso_version | the graphical personalisation version |
| CKO_DATA | tokeninfo_elec_perso_version | the electrical personalisation version |
| CKO_DATA | tokeninfo_elec_perso_int_version | the electrical personalisation interface version |
| CKO_DATA | perso_versions | The 4 personalisation bytes as found in the tokeninfo file on the eID card (the 3 bytes above, followed by a not yet used byte) |

1.1.2.5 Grouped Card Data

Starting from eID MW 4.0.2, the CKA_OBJECT_ID attribute has been added to the CKO_DATA object's attribute lists. This allows for searching for a group of objects with the same CKA_OBJECT_ID.

(e.g. If you are interested in finding all objects of the identity data file (and the unparsed identity file), search for object with CKA_CLASS set to CKO_DATA and with CKA_OBJECT_ID set to id.

7 Values for the CKA_OBJECT_ID attribute have been defined:

| CKA_CLASS | CKA_OBJECT_ID | |
|-----------|-------------------|--|
| CKO_DATA | id | Parsed and unparsed data from the identity data file |
| CKO_DATA | address | Parsed and unparsed data from the address data file |
| CKO_DATA | photo | The photo file |
| CKO_DATA | carddata | Parsed and unparsed data from the card data file and the ATR |
| CKO_DATA | rncert | The RN Certificate |
| CKO_DATA | sign_data_file | The signature of the identity file |
| CKO_DATA | sign_address_file | The signature of the address file |
| CKO_DATA | tokeninfo | The personalisation versions |

For “per record” data, no CKA_OBJECT_ID attribute is currently foreseen to be used, as the point of using the per record data objects is to only read the data you need. If you want all data from the id and address files, use the “id” and “address” CKA_OBJECT_ID's instead and work with either the parsed or unparsed data.