

**Israeli Government Standard (GS) for the Implementation of
National ID-Documents based on PKI Smart Cards (SC)**

**Annex 1.10 – Definitions of Common Elements –
Smart Card**

1. **List of data entities**

The GS adopts the list of data entities (objects) according to table 8 in the BS.

2. **List of interindustry templates and common data items**

Following is a list of interindustry templates that group the data entities (objects) for the GS (compatible to Annex A of ISO/IEC 7816-6):

2.1 **Common Application Template of Data Items –
tag ‘61’**

No'	TAG	Data Item
1	4F	Application Identifier (AID)
2	50	Application Label

2.2 **Common Cardholder Related Data Items – tag ‘65**

No'	TAG	Data Item
1	5F2C	Cardholder Nationality (Citizenship)
2	68	ID number (for an Israeli)
3	68	Identification Number (for a foreigner: Could be the Travel document number or another number)
4	5F20	Cardholder Full name (Latin)
5	6B	Cardholder Full name (Hebrew)
5		Cardholder Full Name (Arabic)
6	5F2B	Cardholder Date of Birth (Gregorian)
7	5F35	Sex

No'	TAG	Data Item
8	5F42	Address
9	5F40	Cardholder portrait image
10	5F2E	Cardholder biometrics data (Reserved 1 KB)
11	7F21	Cardholder digital certificate
12	5F49	Cardholder Public Key
13	5F48	Cardholder Private key
14	5F4A	Public Key of Certification Authority

Comment: It is not mandatory to include in the GSC all the common data items described above, but rather according to the needs and requirements and existence. For example: Arabic names will be available only for citizens or residents that their Arabic names exist in the database of the ministries. Furthermore, a digital photograph and biometrics will be included in the card according to the considerations of the ministries. It is possible to use more than one type of biometrics.

2.3

Common Card Data Items – tag ‘66’

No'	TAG	Data Element
1	5F28	Country Code
2	45	Card issuer's data
3	47	Card capabilities
4	46	Pre-issuing data: Version number of the card
5	5F34	Cars sequence number
6	5F26	Card effective date (Gregorian). <u>Optional:</u> Card effective date (Hebrew).
7	59	Card expiration date (Gregorian). <u>Optional:</u> Card expiration date (Hebrew).

2.4 Common Authentication Data – tag ‘67’: As defined in the BS.

2.5 Common Application Related Data – tag ‘6E’: As defined in the BS.

3. Data structure on the smart card

3.1 General

3.1.1 In order to enable interoperability and compatibility while reading the GSC, there is a need for a definition of the schema of the database and the general data structure of the card.

3.1.2 The data structure on the card will support both SCQL and a basic data structure of dedicated files (DF) and elementary data files (EF).

3.1.3 The common data items will be in the form of DF and EF, and not in SCQL.

3.1.4 Note: The following definitions are not detailed in the application level and the software implementation.

3.2 Master File directory

3.2.1 The Master File directory is mandatory.

3.2.2 DIR: the directory file will be as defined in ISO/IEC 7816-4 section 9.4, in ISO/IEC 7816-5 section 6.3.2 and in IS 4400. The directory will include several DF’ s as the number of the implementation on the card.

3.2.3 EF PIN #1: The mater PIN file, which can be applied on the whole card.

3.3 DF on the card - general

3.3.1 DF1: It will consist of the following data segments:

- 3.3.1.1 Common Cardholder Related
Data Items – tag '65'.
- 3.3.1.2 Common Card Data Items – tag
'66'.
- 3.3.1.3 Common Authentication Data –
tag '67'.
- 3.3.2 **DF2:** Application data of the ID national
card (“TELEM”) – Ministry of the Interior.
- 3.3.3 **DF3:** Application data of Working Permit
for foreign workers – Ministry of the Interior.
- 3.3.4 **DF4:** Application data of Driving license -
Ministry of Transportation.
- 3.3.5 **DF5:** application data of “BASEL” project
– Israeli Police.

3.4 **DF (TAMUZ) – definitions**

Following is the proposed data structure for the application of the
computerized card for access and identification in government
ministries (TAMUZ):

- 3.4.1 EF: Token info, including the unique serial
number of the card.
- 3.4.2 EF: Objects' data on the card.
- 3.4.3 EF: Objects data for authentication,
including pointers to the files where the PIN codes are
found.
- 3.4.4 PIN-CODE #2 for digital signature only.
- 3.4.5 RSA private key (#1).
- 3.4.6 RSA private key (#2).
- 3.4.7 Digital certificate #1, for identification and
authentication.
- 3.4.8 Digital certificate #2, for digital signature
and non-repudiation.
- 3.4.9 **“Access data”, needed for physical access
control.**

3.4.10 Other reserved areas and zones, for future addition of different data items, including data that will be written after the first personalization phase.

3.5 **Definition of the structure and data in the digital certificate:** See chapter 2 in the GS.