

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

## **Chapter 1 – Smart Card Government Standards**

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

### **Chapter 1 – Smart Card Government Standards**

#### **1. Introduction**

- 1.1 This chapter defines the GS for ID-documents, based on Smart Cards.
- 1.2 In the following sections, the specifications of the different components of the Government Smart Card (GSC) system are described.
- 1.3 An application system incorporating Smart Cards and PKI should include several coordinated components, as follows:
  - 1.3.1 The relevant government application.
  - 1.3.2 The ID-document based on a PKI SC.
  - 1.3.3 Interface Devices (IFD' s)
  - 1.3.4 The interfaces between the Smart Card, the IFD and the application.
- 1.4 The GS defines in this chapter, in an obligatory manner, the following components:
  - 1.4.1 The ID-document based on a PKI SC.
  - 1.4.2 The interfaces between the Smart Card, the IFD and the application.
- 1.5 The interfaces include the following levels:
  - 1.5.1 Physical specifications of the SC.

1.5.2 Power-supply Interface.

1.5.3 Electronic Communication Interface.

1.5.4 Operating System Interface (Data structures, commands and services).

1.5.5 Data Base Interface.

1.5.6 Data Security Interface.

1.5.7 Application Interface.

1.6 The GS actually defines the **interface** between the GSC, and the IFD and the application existing behind the IFD.

1.7 In that sense, conformance to the standards applies to the SC, the IFD and the applications that communicate with the SC. That is, both the SC and the IFD are required to conform to the same standards, defining the physical characteristics, the logical characteristics and the communication characteristics, between the SC and the IFD.

1.8 Adaptation to Disable Persons: IFD' s installed in public places, will enable convenient usage by the public as a whole. Proper arrangements should be made for use by Disabled Persons, as much as possible, including installation of the IFD in a position and in height suitable for convenient access.

## 2. Type of the Smart Card

2.1 Each ministry or agency, will make the decision concerning the type of the SC that is most suitable for the relevant application, i.e.: Contact SC, Contactless SC, Hybrid SC or Dual-Interface SC.

2.2 In order to enable reading all the relevant Smart Cards, the government ministries and agencies, will install the infrastructure needed for that, meaning, both contact and contactless IFD' s, subject to the following conditions:

2.2.1 SC IFD' s for Logical Access, connected to workstations that are connected to communication networks, as well as to portable computers, will be Contact Smart Cards IFD' s.

2.2.2 SC IFD' s for Physical Access, connected to Access Control Systems, will be, as a general rule, Contactless SC IFD' s. At the entrance points to government facilities, or in other designated places, there will also be installed Contact Smart Cards IFD' s.

2.3 It will be possible to add to the SC, mainly for physical access requirements, a magnetic stripe according to ISO/IEC standards, as defined in the GS.

2.4 In the case that a Dual-Interface Smart Card or a Hybrid Smart Card is selected for implementation, the requirements from both the contact and contactless interfaces, as defined in the GS, will be applied accordingly.

### 3. **Government Smart Card (GSC)**

#### 3.1 **General Directions**

3.1.1 The GSC will support the following relevant standards.

3.1.2 In addition to that, the GSC will be adapted to the specific requirements of the State of Israel and the Government of Israel, as listed in the following sections, accordingly.

#### 3.2 **Physical Dimensions**

3.2.1 The GSC will be in the physical dimensions, as specified in ISO/IEC 7810 section 5, of an ID-1 card.

3.2.2 The basic dimensions are:

3.2.2.1 Width: 85.6 mm.

3.2.2.2 Height: 53.98 mm.

3.2.2.3 Thickness: 0.76 mm.

#### 3.3 **Structure of the Smart Card and its materials**

3.3.1 The GS adopts section 6 and section 7 of ISO/IEC 7810.

3.3.2 The GS does not define the type of the specific materials used. Each ministry will specify its' requirements, in terms of the life span necessary and other functional specifications. The materials of the smart card will be proposed by the manufacturer, according to the above specifications.

#### 3.4 **SC characteristics**

The GS adopts section 8 of ISO/IEC 7810, relating to the following characteristics (in brackets are the sub-sections numbers in ISO/IEC 7810):

3.4.1 Bending stiffness (8.1.1).

3.4.2 Flammability (8.1.2): The card will conform to section 5.2 of ISO/IEC 7813, which states the following: The cards "shall be self-extinguishable within 5 seconds and shall not burn more than 25 mm (0.98 in) after removal from flame".

3.4.3 Toxicity (8.1.3).

3.4.4 Resistance to chemicals (8.1.4).

3.4.5 Card dimensional stability and warpage with temperature and humidity (8.1.5).

3.4.6 Light (8.1.6).

3.4.7 Durability (8.1.7): Life span of the card is not defined in the GS. It will be based on a contract signed between the issuer of the card (which is the government ministry/agency), and the producer of the card, according to the requirements of the government ministry/agency.

3.4.8 Delamination.

3.4.9 Adhesion or blocking (8.1.9).

3.4.10 Light transmittance (8.1.10).

3.4.11 Overall card warpage (card type ID-1, unembossed cards) (8.1.11).

3.4.12 Card warpage (card type ID-1, embossed cards) (8.1.12).

### 3.5 **Special Characteristics**

The GS adopts section 9 of ISO/IEC 7810, relating to the following special characteristics (in brackets are the sub-sections numbers in ISO/IEC 7810):

- 3.5.1 Cards with magnetic stripe (9.1).
- 3.5.2 Special characteristics relating to contact smart cards (9.3): See section 3.6 below.

### 3.6 **Physical Characteristics for Contact Smart Cards**

In addition to section 3.2 – 3.5 above, the GS adopts the BS ISO/IEC 7816-1 for contact smart cards, including the following extra characteristics (in brackets are the sub-sections numbers in ISO/IEC 7816-1):

- 3.6.1 Ultra-violet light (4.2.1).
- 3.6.2 X-rays (4.2.2).
- 3.6.3 Surface profile of contacts (4.2.3).
- 3.6.4 Mechanical strength (of cards and contacts) (4.2.4).
- 3.6.5 Electrical resistance (of contacts) (4.2.5).
- 3.6.6 Electromagnetic interfaces [between magnetic stripe and integrated circuit(s)] (4.2.6).
- 3.6.7 Static electricity (4.2.7).
- 3.6.8 Operating temperature (4.2.8).
- 3.6.9 Bending properties (4.2.9).
- 3.6.10 Torsion properties (4.2.10).

### 3.7 **Physical Characteristics for Contactless Smart Cards**

In addition to section 3.2 – 3.5 above, the GS adopts the BS ISO/IEC 14443-1 for contactless smart cards, relating to the following characteristics (in brackets are the sub-sections numbers in ISO/IEC 14443-1):

- 3.7.1 Ultra-violet light (4.3.1).
- 3.7.2 X-rays (4.3.2).
- 3.7.3 Dynamic bending stress (4.3.3).
- 3.7.4 Dynamic torsional stress (4.3.4).
- 3.7.5 Altering magnetic fields (4.3.5).
- 3.7.6 Altering electric field (4.3.6).
- 3.7.7 Static electricity (4.3.7).
- 3.7.8 Static magnetic field (4.3.8).
- 3.7.9 Operating temperature (4.3.9).

### 3.8 **Recommendations for Security Means for the GSC**

- 3.8.1 The GSC will be classified as belonging to one of two security levels, according to the estimated damage that might be caused as a result of its forgery:
  - 3.8.1.1 GSC used as a National ID-documentation – Level “A”.
  - 3.8.1.2 GSC not used as a National ID-documentation – Level “B”.
- 3.8.2 GSC of level A shall have the possibility of authentication without any instruments in a high level of certainty. The printing on the card shall reach the edge of the card and will penetrate to the depth of the card. The printing shall include at least three visible security means:
  - 3.8.2.1 OVI printing, that changes its color when the angle of visibility changes.
  - 3.8.2.2 Rainbow printing.
  - 3.8.2.3 Micro-text.
- 3.8.3 GSC of level A shall include at least one invisible mean that can be verified using simple instruments (such as a UV lamp) whereas this mean will be different from one card to the other and related to the details of the cardholder.

- 3.8.4 GSC of level A shall include at least one invisible mean that can be verified using special laboratory instruments whereas this mean will be different from one card to the other and related to the details of the cardholder.
- 3.8.5 GSC of level A shall be based upon a chip belonging to an updated technology generation that includes built-in structured security means, both physical and logical, in the operating system and the applications:
- 3.8.5.1 Full Transaction Protection – the ability to fully cope with attacks based on the termination of processes before their correct completion.
- 3.8.5.2 The ability to identify stresses, such as clock frequency or power voltage, out of the correct range.
- 3.8.5.3 Security against DPA.
- 3.8.5.4 Verification of the non-volatile memory using checksum.
- 3.8.5.5 Security against Timing Analysis, both in the operating system and in the different applications.
- 3.8.5.6 Physical security on the chip against being checked by different analytical instruments.
- 3.8.6 A detailed description on the security means listed in section 3.8.5 above, will be delivered by the supplier to the ordering ministry/agency, together with describing the significance of each item, such as, raising transaction time or decrease in performance. A supplier that will attach existing validation and evaluation by national or government agencies, his proposal will be accredited accordingly.
- 3.8.7 GSC of level B will be printed with at least one security measure that is verifiable without special instruments and is a laminate of the formal symbol of the

State of Israel. The design of the symbol and its size will be identical between all government ministries.

3.8.8 GSC of level B that its forgery will cause a serious and long-range damage will include **at least** one invisible security mean verifiable by simple instruments (such as a UV lamp).

3.8.9 GSC of level B will include physical and logical security means according to the application and the decision of the ordering ministry.

#### 4. Power and Communication Interface Characteristics

##### 4.1 Contact GSC

4.1.1 Dimensions and location of the contacts:  
The GS adopts all of BS ISO/IEC 7816-2.

4.1.2 Electronic signals and transmission protocols

4.1.2.1 The GS adopts the BS ISO/IEC 7816-3, in the following constraints and selection of alternatives as listed below (in brackets are the sub-sections numbers in ISO/IEC 7816-3).

4.1.2.2 The GSC will operate in 5 V, under class A (4.2).

4.1.2.3 VCC (4.3.2): This contact will operate under class A (5 V).

4.1.2.4 I/O: As defined in the BS (4.3.3).

4.1.2.5 CLK: As defined in the BS (4.3.4).

4.1.2.6 RST: As defined in the BS (4.3.5).

4.1.2.7 VPP: This contact will operate under class A as defined in the BS (4.3.6).

4.1.3 Card operating procedures (5): As defined in the BS, under class A (5 volt).

4.1.4 Answer-to-Reset (6): As defined in the BS. The GSC will support parameter T (6.7), in one of two alternatives: T=0 or T=1.

4.1.5 Protocol and parameters selection (7): As defined in the BS.

4.1.6 Support of protocol T=0 (8): As defined in the BS.

4.1.7 Support of protocol T=1 (9): As defined in the BS.

## 4.2 Contacless GSC

### 4.2.1 Radio frequency power and signal interface:

4.2.1.1 The GS adopts the BS ISO/IEC 14443-2. The communication signal interface will be according to type B, as defined in section 7 and section 9 of the BS.

4.2.1.2 Section 8 of the BS which relates to communication signal interface of type A will not be valid in the GS.

4.2.1.3 PICC minimal coupling zone: Will be as defined in section 10 of the BS.

### 4.2.2 Initialization and anticollision

4.2.2.1 The GS adopts the BS 14443-3.

4.2.2.2 The GS will support only communication signal interface type B. As a consequence, only section 7 in the BS is valid, whilst section 6 in the BS is not valid in the GS.

### 4.2.3 Answer to Select and Transmission Protocol

4.2.3.1 The GS supports the BS ISO/IEC 14443-4.

4.2.3.2 Since the GS only supports type B communication signal interface, section 5 of the BS is not valid.

4.2.3.3 Half-Duplex Transmission Protocol: As defined in section 8 of the BS.

## 5. Basic data structure on the SC

### 5.1 General

5.1.1 The GS adopts the basic data structure defined in section 5 of the BS ISO/IEC 7816-4.

5.1.2 The GSC will have a mandatory MF (master-file).

5.1.3 The GSC will support the following files categories:

5.1.3.1 DF – Dedicated File.

5.1.3.2 EF – Elementary File.

5.1.4 Data and common data items, will be organized in a basic data structure of DF and EF (and not in SCQL data structure), in order to be as wide as possible common base.

5.1.5 Listed below are relevant sub-sections (designated in brackets) of the BS.

## 5.2 File referencing methods (5.1.2)

5.2.1 The GS will support implicit file referencing.

5.2.2 In addition, all four alternatives mentioned in the GS will be possible:

5.2.2.1 Referencing by file identifier.

5.2.2.2 Referencing by path.

5.2.2.3 Referencing by short EF identifier.

5.2.2.4 Referencing by DF name.

## 5.3 Elementary file structures

5.3.1 The GSC will support **both** structures of EF' s:

5.3.1.1 Transparent structure, i.e., as seen at the interface as a sequence of data units.

5.3.1.2 Record structure, i.e., as seen at the interface as a sequence of individually identifiable records.

5.3.2 The GSC will support all **four** types of methods for EF data structure:

5.3.2.1 Transparent EF.

5.3.2.2 Linear EF with records of fixed size.

5.3.2.3 Linear file with records of variable size.

5.3.2.4 Cyclic EF with records of fixed size.

5.3.3 Data items, including common data items, will be as described in Annex 1.10.

5.3.4 Specific data items for government applications could be in any one of the above possible data structures.

#### 5.4 **Data referencing methods**

The following methods will be possible:

5.4.1 Record referencing, by record identifier.

5.4.2 Record referencing, by record number.

5.4.3 Data unit referencing, within an EF with transparent structure.

5.4.4 Data unit referencing, within an EF with a record structure.

5.4.5 Data object referencing.

#### 5.5 **File control information (5.1.5)**

The GSC will support the three (3) templates mentioned in section 5.1.5:

5.5.1 File Control Parameters (FCP template).

5.5.2 File Management Data (FMD template).

5.5.3 File Control Information (FCI template), which will be grouped according to ISO/IEC 7816-4.

5.6 **Security Architecture of the card (5.2)**: See section 15 below which discusses data security, and in particular sub-section 15.2.

5.7 **APDU message structure (5.3)**: The GSC will support the APDU message structure (An Application Protocol Data Unit) as defined in section 5.3 of the BS. See also section 15 below and in particular sub-section 15.2.3.

5.8 **Coding Conventions for command headers, data fields and response trailers (5.4):**

The GSC will support the codes defined in section 5.4 of the BS.

5.9 **Logical channels (5.5):** A GSC may support the concept of logical channels, as defined in section 5.5 of the BS. Since in the BS, support of logical channels is optional, so is the support in the GS optional. It is left optional according to the specifications of the application of each ministry/agency. If a ministry/agency decides to implement this option, it will be done according to the BS.

5.10 **Secure messaging (5.6, 5.7):** See section 15 below, which discusses data security and in particular sub-section 15.2.4.

6. **Support of Interindustry commands**

6.1 The GS adopts the structure of the basic interindustry commands as defined in ISO/IEC 7816-4, sections 6 and 7. Implementation of these interindustry commands will be done in full compliance with the BS, including all the options of each command.

6.2 The BS does not require support of all the commands, and even suggests several profiles of support. Accordingly, the GS does not require that all commands will be supported. The basic demand is to support profile "O" according to Annex E of the BS. A ministry designing to narrow that group of commands, will be required to request an exception to the GS, as outlined in section 0.10 in chapter 0 of the GS.

6.3 For applications of ID-documents, a specific group of commands will be selected, after the Detailed Design phase.

6.4 For application of Computerized Documents for Access and Identification in Government Ministries (TAMUZ), a specific group of commands will be selected, after the Detailed Design phase of the project.

7. **Support of Historical Bytes**

7.1 The GS adopts the definitions of the historical bytes as defined in section 8 of ISO/IEC 7816-4.

7.2 The information carried by the historical bytes will also be found in an ATR file, for redundancy reasons.

7.3 The data objects that will be included in the historical bytes are:

7.3.1 A mandatory category indicator.

7.3.2 Optional data objects (8.3):

7.3.2.1 Country/issuer indicator (8.3.1).

7.3.2.2 Card service data (8.3.2).

7.3.2.3 Initial access data (8.3.3).

7.3.2.4 Card issuer's data (8.3.4).

7.3.2.5 Pre-Issuing data (8.3.5).

7.3.2.6 Card capabilities (8.3.6).

7.3.3 A conditional status indicator.

## 8. **Support of Application – independent card services**

8.1 The GS adopts the support of application-independent card services, as defined in section 9 in ISO/IEC 7816-4.

8.2 The services that will be supported are (in brackets is the sub-section number in the BS):

8.2.1 Card identification service (9.2).

8.2.2 Application selection service (9.3):

8.2.2.1 The GSC will enable implicit application selection by the “application identifier” that will be present in the card identification data and in the ATR file.

8.2.2.2 The GSC will enable direct application selection (9.3.2).

8.2.3 Data object retrieval service (9.4).

8.2.4 File selection service (9.5).

8.2.5 File I/O service (9.6).

## 9. **Support of Numbering system and registration procedures for application identifiers:**

- 9.1 The GS adopts the numbering and registration systems as defined in the ISO/IEC 7816-5 that was also published as IS-4400. Following is a reference to the sub-sections in the standard (designated in brackets).
- 9.2 The objects defined in the BS will be found at the following places, for redundancy reasons (5.4):
- 9.2.1 Historical bytes of the ATR.
- 9.2.2 DIR file.
- 9.2.3 ATR file.
- 9.3 Retrieval of the application identifier may be read from any of the following (6.2):
- 9.3.1 DIR file.
- 9.3.2 ATR file.
- 9.3.3 Historical bytes.
- 9.4 The GS will support application selection in any of the following (6.3):
- 9.4.1 Direct application selection with AID (6.3.1).
- 9.4.2 Selection by the use of a DIR file or an ATR file (6.3.2).
- 9.5 Implicit application selection is actually not recommended for multi-application cards, but the GS will support this option anyway, for future development (6.3.3).

## 10. Support of Interindustry data Elements

- 10.1 The GS supports the interindustry data elements defined in ISO/IEC 7816-6.
- 10.2 The GS will support all types of Data Retrieval as defined in section 5 of the BS.
- 10.3 The GS will support all of the specific DE's, IDO's, and data objects, as defined in section 6,7,8 of the BS.
- 10.4 The GS will support the Interindustry templates defined in Annex A of the BS.
- 10.5 Common data items

- 10.5.1 The common data items, according to the BS, are listed and described in Annex 1.10.
- 10.5.2 It is not mandatory to include all of the items defined as “common” in each GSC, except for those explicitly noted. Nevertheless, if a data item appears on a GSC, they will be in the format defined in the GS.
- 10.5.3 Common data items are not necessarily accessible in the same manner by different users. The decision on the accessibility to the data and the ability to read the data by different users will be taken by the issuing ministries, according to the authorizations and the access mechanisms that will be defined in the application.

## **11. Support of Interindustry Commands for Structured Card Query Language (SCQL)**

- 11.1 The GS adopts the interindustry commands for SCQL, as defined in ISO/IEC 7816-7, and as defined below.
- 11.2 Support of SCQL database according to section 5 of the BS:
  - 11.2.1 A GSC may include a SCQL database, as described in the BS, together with a hierarchical file structure, including DF’ s and EF’ s of different types.
  - 11.2.2 The decision whether to actually implement the SCQL database is with the issuing ministry. It is not a mandatory condition, but, if implemented, should be according to the BS.
  - 11.2.3 Common data items will not be in SCQL but in a basic structure of DF’ s and EF’ s, to be as widely common as possible.
- 11.3 SCQL Commands: The GSC will support the commands listed in sections 6,7,8,9 of the BS, in case a

government ministry/agency decides to implement the SCQL, in the manner listed in section 6 above.

## 12. The operating system (OS) of the GSC

- 12.1 General: The requirements from the OS relate to its conformance to the BS that defines the services, the data structure and the security features.
- 12.2 Portability: The OS could operate on more than one single chip of different chip producers.
- 12.3 Support of system commands: The OS will support the system commands defined in ISO/IEC 7816-4 (Interindustry commands for interchange) both for contact and contactless cards. The manner of support will be as described in section 6 above.
- 12.4 Support of different services: The OS will support, apart from the above, all of the following BS, as far as the OS level is concerned:
- 12.4.1 ISO/IEC 7816-7 (Interindustry commands for SCQL): Support of this BS is optional, in the manner defined in section 11 above.
  - 12.4.2 ISO/IEC 7816-8 (Security related interindustry commands): As described in section 15.3 below.
  - 12.4.3 ISO/IEC 7816-9 (Additional interindustry commands and security attributes): Since this BS was not finally published, supporting it is optional. When it will be finally published, it will be mandatory in the GS, in the manner described in section 11 above.
  - 12.4.4 ISO/IEC 7816-11 (Framework for dynamic handling of multiple application in integrated circuit cards): Since this BS was not finally published, supporting it is optional. When it will be finally published, it will be mandatory in the GS, in the manner described in section 11 above.

## 13. Visual appearance of the GSC

The government documents based on smart cards, will be issued keeping the following rules:

13.1 Uniform usage of the functional zones of an ID-1 (or TD-1) type card, including headers, data zone, photo zone and other zones.

13.2 The State symbol will be in the header zone of the ID-1 (TD-1) card, in a uniform size and form, in all documents.

#### 14. **Interface Devices (IFD) for reading/writing**

14.1 General: All the standards that are in effect regarding the interface between the SC and the IFD and the application will apply to both the card and the IFD, as described in this GS.

14.2 Assuring reading ability from all types of cards:  
See section 2.2 above.

14.3 Support of transmission protocols: A government IFD (GIFD) will support transmission protocol according to parameter T=0 and transmission protocol according to parameter T=1, as defined in ISO/IEC 7816-3, in particular sections 6,7,8 and 9.

#### 14.4 GIFD for Contact GSC

14.4.1 A GIFD of a contact type will support reading any contact GSC that conforms to the specifications in the GS.

14.4.2 A contact GIFD, may be in one of the following technologies:

14.4.2.1 Friction.

14.4.2.2 Zero insertion force.

14.4.2.3 Landing contacts.

14.5 GIFD for Contactless Smart Card: A GIFD of contactless type will support reading any contactless GSC conforming to the specifications in the GS.

14.6 Keypad for pin-code: A GIFD may include a keypad for pin-code entry, where necessary.

14.7 Response for identifying forged documents of non-authentic documents or a document that was attempted at

changing it's data illegally: Each Government ministry/agency should define the mode of action to be taken in case one of the above mentioned cases is detected, while a SC is introduced to the IFD.

14.8 Security of the IFD: Each government ministry/agency should demand in the tender means for protecting the IFD security (Tamper proof).

14.9 Selecting the IFD type and specifications: The decision regarding the IFD type will be made by the government ministry/agency that will install the IFD according to it's functional needs in different sites, as long as the IFD conforms to the specifications in the GS. The ministry could define whether the IFD will be an independent device or an integrated device, according to its needs, unless otherwise defined explicitly in the GS.

## 15. Data security

15.1 General background and guidelines for data security

15.1.1 Security means and data security on the card will be adapted to the demands, the requirements, the threats and the risks involved from using the card, according to the government ministry/agency considerations.

15.1.2 Notwithstanding that, while implementing the data security means, the ministries/agencies should follow the general approach that includes the following elements, which serve as guidelines and a sort of "Data security constitution".

15.1.3 The solution proposed for implementing smart card system data security, will be the property of the State of Israel. The producer will not use these solutions for any other use, without prior consent in writing, by the Government ministry/agency, except for specific

elements where known copyrights belong to another party.

15.1.4 Evaluation of the security mechanisms on the card

15.1.4.1 The ministry should demand in the tender that the supplier would present the details of the security mechanisms (Algorithms, methods and implementation), for evaluation and prior approval of the ministry. The algorithms and methods will be presented in the most detailed manner, as possible. Their implementation will be presented in a source code level, with full documentation.

15.1.4.2 The ministry has the right to reject a method or an implementation or a mechanism presented to it, without the supplier's appealing on that decision. The ministry does not have to give reasons for the rejection.

15.1.4.3 The implications on the rejection of security mechanisms on the whole proposal depend on the nature of the tender and its conditions and are not included in the GS. Each ministry has to define in the tender the way of handling a case of rejection and the implications on the possibility of receiving a re-fixed proposal or rejection of the whole proposal.

15.1.4.4 In the case that the ministry decides to point on a certain defect or a certain fix that is needed in the mechanism, the following procedure will apply: The fix will be done only in the product supplied to the ministry. No use will be made of that information in any other product of the supplier for any other third party, without the prior written consent of the ministry.

15.1.4.5 This section is mandatory in the GS and accordingly in a tender.

15.1.5 Evaluation of the OS

- 15.1.5.1 The supplier will have to present the operating system of the SC for evaluation. The OS will be presented in the most detailed manner, including source code with full documentation.
- 15.1.5.2 The ministry has the right to reject an OS without the suppliers' appealing on that decision. The ministry does not have to give reasons for the rejection.
- 15.1.5.3 In the case that the ministry will decide to point on a certain defect or a fix that is needed in the OS, then the following procedure will apply: The fix will be done only in the product supplied to the ministry. No use will be made of that information in any other product of the supplier for any other third party, without the prior written consent of the ministry.
- 15.1.5.4 This requirement is not a threshold condition, but a supplier that will not agree to this condition, then his proposal will be given less points when evaluated, than that of a supplier that agrees to this condition.
- 15.1.6 In the SC system supplied by the producer, there will be no "horizontal secrets". In other words, a compromise of certain data from one or more cards will not cause the compromise of the whole system.
- 15.1.7 After supplying a SC system, including the testing and installation periods, the producer, or the supplier, will not be able to make use of any secret information that will be given to them by the ministry. The definition of "secret information" will be as defined in the tender documents, in particular in the contract, in a manner that will enable them to produce identical or similar product, without prior written and explicit consent of the ministry.

15.1.8 The SC system will be designed so that the knowledge and the acquaintance with the security mechanisms will not enable any party trying to break into the system, to succeed. The system will be defined as an “open system” such that it will be possible to openly publish its structure, without compromising the system.

15.1.9 No use will be made of proprietary security mechanisms. If the ministry will decide to integrate a proprietary mechanism of its own, the supplier and the producer will not use it in any way, without the prior written consent of the ministry.

15.2 Support of ISO/IEC 7816-4 (Interindustry commands for interchange)

15.2.1 The GSC will support the security architecture defined in ISO/IEC 7816-4 section 5.2, and all that is implicated by it, including:

15.2.1.1 Entity authentication with password.

15.2.1.2 Entity authentication with key.

15.2.1.3 Data authentication, using cryptographic checksum and digital signature: This section is mandatory.

15.2.2 The GSC will not include a data encipherment mechanism, except for random numbers creation. That does not mean that the data itself will be exposed, but rather that it will be secured without encipherment of the data itself. Access will be managed by authorizations according to the mechanisms detailed above, but without encipherment of the communication to the card and from the card in cryptographic mechanisms (except for transferring private keys in a secure

way in a symmetric type cryptographic mechanism), without encryption of the data itself.

15.2.3 The GSC will support the following data objects for authentication, as defined in ISO/IEC 7816-4, sections 5.6.3.1 and 5.6.3.2:

15.2.3.1 Cryptographic checksum data object.

15.2.3.2 Digital signature data object.

15.2.4 The GSC will support secure messaging according to ISO/IEC 7816-4 section 5.6 and 5.7, and Amendment 1: Impact of secure messaging on the structures of APDU messages. The support of secure messaging according to the above is optional, i.e., the GSC does not have to support this option, but in a GSC that this is required, it will be implemented according to the BS.

15.3 Conformance to ISO/IEC 7816-8 (Security related interindustry commands):

15.3.1 The GSC will conform to ISO/IEC 7816-8 that includes specific security commands.

15.3.2 In particular, the GSC will support the execution of digital signature, as defined in chapter 2 of the GS.

15.3.3 The minimum requirement is that the card will support digital verification on the card.

15.3.4 The ministry, according to its specifications, will decide whether to require digital signature creation on the card.

15.3.5 Except for the above requirements, it is not mandatory that the GSC will support all of the commands in the BS, except

those commands that are defined as “mandatory” in the BS itself.

15.4 Standards for digital signature: See chapter 2 of the GS.

15.5 Usage of personal Identification number (PIN):

15.5.1 Access to information that is related to privacy issues, or from any other functional reasons, will be done by a PIN CODE, known only to the card holder. The PIN DODE will be code at least 4 digits long that will be delivered to the cardholder concurrently with the issuance of the GSC. Entering the PIN CODE is not considered as “mandatory” in all the applications, but as an option of each application. The PIN CODE can serve as an authorization token for access, to all the details in the card, or to some of them, according to the design of the specific application.

15.5.2 Israeli police, using IFD’ s installed in police premises or police vehicles, will be able to read certain common data from the card, without the necessity of entering the PIN CODE by the cardholder, according to the design of the application.

16. **Tests**: The GSC has to pass the tests defined in ISO/IEC 10373 – Identification cards – Test methods, parts 1 and 3.

## 17. **Numbering system and registration procedures**

17.1 The numbering system and the registration procedures for the GSC will be according to IS-4400, which adopts and refers to the following standards:

17.1.1 ISO/IEC 7816-5: Numbering system and registration procedure for application identifiers including the 1997 Amendment A1.

17.1.2 ISO/IEC 7812-1: Numbering system.

17.1.3 ISO/IEC 7812-2: Application and registration procedures.

17.2 The General Accountant Division in the Ministry of Finance will handle of application and numbering in the government sector, in accordance with the BS, for all government ministries and agencies.

18. **Implementation of the Hebrew language:** Implementation of the Hebrew language will be done according to IS-4424 (1999): Cards with Integrated circuit(s) – The implementation of Hebrew.
19. **Quality Assurance:** Delivering components of a smart card system will be done by suppliers, including sub-contractors, that are ISO-9000 approved.
20. **Configuration Control:** The management of all the components of the software, hardware and communication that will be supplied to the government will be under the control of a computerized configuration management system. In particular, that system will include the management of all the application components, starting from the logical level down to the physical level.