

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

**Chapter 2 – PKI standards**

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

### Chapter 2 – PKI Standards

#### 1. Introduction

This chapter defines the GS for the implementation of PKI integrated with GSC, relating to the requirements from different components of PKI.

#### 2. Components of PKI

- 2.1 The system will be based on the following central components:
  - 2.1.1 Digital Certificates, according to x.509 (ISO/IEC 9594-8).
  - 2.1.2 Management of Directories, according to X.500 (ISO/IEC 9594).
  - 2.1.3 Cryptographic Information Application on the smart card (ISO/IEC 7816-15).
  - 2.1.4 Directory management for digital Certificates Revocation List (CRL) (ISO/IEC 9594-8).
  - 2.1.5 Access protocols to the directories: DAP and LDAP (ISO/IEC 9495-5).
- 2.2 The main standard, according to which the PKI will be implemented, is ISO/IEC 9594-8. This standard will be elaborated in the following section.
- 2.3 Another key standard is ISO/IEC 7816-15. This standard is still under discussions and in a **Draft version** only. But, because of its importance, it is adopted already at this

stage in the GS, in its most current version, with necessary updates in the future, according to the requirements.

### 3. **Support of ISO/IEC 9594-8**

#### 3.1 **General and Scope**

- 3.1.1 There is a set of basic ISO/IEC standards, dealing with all aspects of the “DIRECTORY” entity and the usage of the directory for authentication.
- 3.1.2 ISO/IEC 9594 defines the manner in which the data for authentication is stored, how to access and receive this data, how that data is originally created and transferred to the directory, and what are the ways to use this data for security authentication services.
- 3.1.3 The protocol used to access and retrieval of data from the Directory is DAP (Directory Access Protocol), defined in ISO/IEC 9594-5 (X519). The GS adopts this standard and also the protocol known as “LDAP” (Light DAP).

#### 3.2 **Strong Authentication (Section 7 in the BS)**

- 3.2.1 The GS will be based on the method of “strong authentication”, as defined in section 7 of the BS.
- 3.2.2 A “Certification Authority” will carry out the creation of digital certificates.
- 3.2.3 As a general rule, the authentication framework does not rely on the usage of a certain cryptographic algorithm, as long as that algorithm has the properties described in section 7 of the BS. On the face of it, it may seem that different algorithms may be used. However, two users wishing to authenticate shall support the same cryptographic algorithm for authentication to be performed correctly. Thus, within the context of a set of related applications, the choice of a single algorithm shall serve to maximize the community of users able to authenticate and communicate securely.
- 3.2.4 According to this rule, the GS supports a single cryptographic algorithm for PKI, which is RSA.

That algorithm is described, among other places, in appendix D of the BS.

3.2.5 In order to create the digital signature of the Certificate Authority, the RSA algorithm will be used with a key of 2,048 bits.

3.2.6 In order to create the digital signature of an end user, the RSA algorithm will be used with a key of 1,024 bits.

3.2.7 Hashing: The following hashing function will be used, as defined in the BS ISO/IEC 10118-3: 1998: dedicated Hash Function 3 (SHA – 1).

3.3 Digital Certificates, the Public Key of the user and different means for management of the certificates

3.3.1 The GS adopts sections 8 – 13 of the BS.

3.3.2 In particular, the structure of the digital certificate is adopted, which is X.509 compatible, as defined in the BS.

3.3.3 Following is a table that describes the basic values that will be in the GS digital certificate:

<b>Field</b>	<b>Value</b>	<b>Comment</b>
Version	"2"	X.509 certificate version 3
SerialNumber	Certificate number	A unique serial number by each CA.
Signature	sha1With RSA 2048 Encryption	Contains the algorithm identifier for the algorithm used by the CA to sign the certificate.
Issuer	Country = IL Issuer code Issuer name	Details of the issuer.
Validity	notBefore notAfter	Validity dates.
Subject	Country = IL; Surname; givenName IdNumber; Organization; Department; Title.	Details of the cardholder.

<b>Field</b>	<b>Value</b>	<b>Comment</b>
SubjectPublic Key	RSA Encryption	Contains the public key and identifies the algorithm with which the key is used.
KeyUsage#1	Identification & authentication	An extension: For certificate number 1 for identification and authentication.
KeyUsage#2	Digital Signature & Non Repudiation	An extension: For certificate number 2 for digital signature.