

Kingdom of Bahrain
Central Informatics Organisation
General Directorate of Information Technology



Smart Card
Reader' specifications

Kingdom of Bahrain
Identity Smartcard



KINGDOM OF BAHRAIN Identity SMARTCARD PROJECT

List of Abbreviations

AFIS	Automated Fingerprint Identification System
CAD	Card Acceptance Device
CIO	Central Informatics Organisation
Dpi	Dots-Per-Inch
ESD	Electrostatic Discharge
GDNPR	General Directorate of Nationalities, Passports and Residence
GDT	General Directorate of Traffic
ISO	International Standards Organisation
LCD	Liquid Crystal Display
MOL	Ministry of Labour
OS	Operating System
PCSC	Personal Computer Smart Card
RF	Radio Frequency
SAM	Security Access Module
SIM	Subscriber Identity Module
USB	Universal Serial Bus

1. The Smart card Project

The Kingdom of Bahrain Identity Smartcard Project is one of the series of projects known collectively as E-Government.

Smart cards in conjunction with new technologies offer unprecedented opportunities for modernization throughout governments and society. These emerging technologies represent the beginning of a modern information age with a nascent electronic government structure and culture which is radically changing the way governments do business and the way citizens get many of the services and goods that they need.

2. Smart Card Security

The Identity smart Card also incorporate card surface design that comply with the minimum five (5) security features specified by the Common Guidelines for Interoperable GCC National ID scheme. The card is Common Criteria EAL 4 compliance and capable of performing symmetric cryptography and the memory are "firewalled".

The IDENTITY SMART CARD is a Java Hybrid Smart card consisting of 66K EEPROM ST Micro contact and 1K EEPROM contactless mifare chip.



3. Smart Card System

The Identity smart Card System architecture is webbed enable and the multiple backend Xeon servers is supported by Legato software for clustering and mirror failover. The Smart Card Management System (SCMS) communicates through MQ using XML message format for updating of the central Database.

The Identity smart Card Personalization Management System (PMS) supports distributed printing and the operators will also quality checked the cards before issuance. The Enrollment and Issuance System (EIS) enables the operators to work online or offline for capturing of the photograph, signature and finger print. The finger print algorithm uses Sagem morpho and JPEG compression technology for both the photograph and signature before storing the data in the backend database.

4. Smart Card Readers

The smartcard will have two chips in it, a contact and contactless chip. These descriptions refer to the method of access to the chip. The majority of the data will be located in the contact portion, with only e-Purse and access control applications located in the contactless portion of the card. Each involved Ministry or Directorate will need access to specific portions of these chips depending on their intended smartcard business processes.

4.1 Contact Smartcard Reader

Name	Contact Reader
Smartcard Interface	1 Card insertion slot 1 SAM slot
Standards	Must be ISO 7816-1/2/3 compliant
Miscellaneous	Must come with drivers (preferably PCSC)

4.2 Contactless Smartcard Reader

Name	Contactless Reader
Smartcard Interface	1 SAM slot
Standards	Must be ISO 14443 type AB compliant Must support Mifare classic protocol



4.3 Mobile CAD

Mobile CADs are portable card readers with varying features such as PDA style touch screens, wireless connectivity and integrated biometrics scanners. Some models also allow for the connection of external portable devices such as barcode scanners, infrared scanners and miniature receipt printers. These devices are mainly used by inspections officials such as those at the GDT, GDNPR and MOL.

Name	Mobile CAD
CPU	200 MHz
Memory	32 MB Flash ROM 32 MB RAM
OS	Microsoft CE.NET
Display	Backlit LCD touch-panel colour display
Interfaces	<ul style="list-style-type: none">• 1 USB• 1 CF-Flash type I/type II
Smartcard interface	<ul style="list-style-type: none">• 1 Card insertion slot• 3 SAM slot• 1 SIM slot
Security	Tamper-proof housing
Standards	ISO 7816, T=0,1
Wireless connectivity	GSM/GPRS capable
Biometric scanner	Reference relevant type in Sections 2.6.1 and 2.6.2

4.4 Biometrics Scanner

Biometrics scanners will be used to provide a means of authoritative proof of identity, by matching the cardholder's fingerprints against stored records. There are two types of biometric scanners, optical and capacitance. The type that should be purchased depends purely on its intended function in the relevant business process.

Optical scanners can produce higher quality scans of the fingerprint, but also cost much more than capacitance. These scanners are mandatory for any business process that includes capturing fingerprint data for storage or for matching the fingerprint against a large database (AFIS).

Capacitance sensors are recommended to be used only for identity verification as they generally provide a lower degree of detail than optical sensors. This means that they should only be used for one-to-one matching between the cardholder and the fingerprint data stored in the smartcard chip. The majority of biometric verifications will be of this type. However, the decision to use capacitance sensors for capture will depend on the level of detail mandated by the concerned governmental agencies business processes.



4.1.1 Type 1 (Optical)

Name	Biometrics Scanner - Optical
Scanner Type	Optical
Acquisition area	21 x 21mm
Connection	USB connector
Image resolution	500 dpi
Image format	8-bit greyscale image
Compatibility	Must be Windows XP compatible
Miscellaneous	Must come with drivers Must be able to load different biometric algorithms

4.1.2 Type 2 (Capacitance)

Name	Biometrics Scanner - Capacitance
Scanner Type	Solid state capacitance sensor
Connection	USB connector
Acquisition area	12.8 x 18 mm
Area size of solid state sensor panel	256 x 360 pixels
ESD tolerance	+/- 8 kilowatts
Image resolution	500dpi
Refresh rate	15 frames/sec
Compatibility	Must be Windows XP compatible
Miscellaneous	Must come with drivers Must be able to load different biometric algorithms



5. Card Composition and Standards

The smartcard is composed of multiple layers. The inner core layers, as shown in the diagram below, comprise the basic material of the card and are designed to be resistant to tears, flexing and bending. The next layers are the layers that personalize the card with the cardholders details. The outer layers add additional security and protection in the form of holographic overlays and protective films.

