Security Policy
for

DAL C3 Applet Suite
on
Axalto Cyberflex Access 64Kv1
Smart Card Chip

FIPS 140-2 Level 3

Version 1.01
November 12, 2004

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

CONTENTS

1 INTRODUCTION 4
1.1 Scope 4
1.2 Dependencies 4
1.3 Terminology 4
1.4 Acronyms 5
2 MODULE OVERVIEW 6
3 SECURITY LEVELS 6
4 CRYPTOGRAPHIC MODULE SPECIFICATION 6
4.1 Operational Environment 8
4.2 Module Interfaces 8
4.2.1 Physical Interface Description 8
4.2.2 Electrical Interface Description 9
4.2.3 Logical Interface Description 10
5 FIPS-APPROVED MODE OF OPERATION 11
6 MODULE CRYPTOGRAPHIC FUNCTIONS 11
7 SELF TESTS 12
7.1 Power Up Self Tests 12
7.2 Conditional Tests 13
8 ROLES & SERVICES 13
8.1 Roles 13
8.1.1 Crypto Officer/Issuer (CO/Issuer) 14
8.1.2 Crypto Officer/Administrator (CO/Admin) 14
8.1.3 Card Holder 14
8.2 Module Services (per role) 14
8.2.1 Crypto Officer/Issuer Services 15
8.2.2 Crypto Officer/Administrator Services 18
8.2.3 Card holder Services 18
8.2.4 Unauthenticated Services (NO ROLE) 19
8.2.5 Relationship between Roles and Services per applet 21
9 CRITICAL SECURITY PARAMETERS 22
9.1 Crytographic Keys 22
9.2 Public Keys 23
9.3 Other CSPS 23
10 SECURITY RULES 24

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

10.1 Identification & Authentication Security Rules 24
10.1.1 Card holder Identification And Authentication 24
10.1.2 Crypto Officer/Issuer Identification And Authentication 24
10.1.3 Crypto Officer/Administrator Identification And Authentication 24
10.2 Physical Security Rules 24
10.3 Key Management Security Policy 24
10.3.1 Cryptographic Key Generation 24
10.3.2 Cryptographic Key Entry 25
10.3.3 Cryptographic Key Storage 25
10.3.4 Cryptographic Key Destruction 25
10.4 Strength of Authentication 25
10.4.1 Triple DES keys 25
10.4.2 CO/Admin PIN and User PIN 26
10.5 Mitigation of Attacks Security Policy 26

11 SECURITY POLICY CHECK LIST TABLES 27

11.1 Roles & Required Authentication 27
11.2 Strength of authentication Mechanisms 27
Access Rights within Services 28
11.3 Mitigation of Other Attacks 29

12 REFERENCES 29

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

1 INTRODUCTION

1.1 Scope

This document defines a FIPS level 3 Security Policy for the DAL C3 Applet Suite on Axalto Cyberflex Access 64Kv1 Smart Card Chip, hereafter referred to as the DAL C3 module. A description of the basic security requirements for the Axalto Cyberflex Access 64Kv1 Smart Card Chip is included along with the DAL C3 Applet Suite and a description of how each security requirement is achieved.

1.2 Dependencies

The DAL C3 module relies on an independent FIPS evaluation of the underlying cryptographic algorithms and security functions implemented on the Axalto Cyberflex Access 64Kv1 Smart Card Chip. This underlying hardware module provides its own Security Policy (and related documents).

1.3 Terminology

In this document the DAL C3 module may sometimes be referred to as the *module* or *cryptographic module*. References to the underlying Axalto Cyberflex Access 64Kv1 module (or its Security Policy or related documents) appear as *base module* or *base cryptographic module.*

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

1.4 ACRONYMS

Acronym	Definition
ACR	Access Control Rule
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASC	Applet Security Controller
ATR	Answer To Reset
CAD	Card Acceptance Device
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CSP	Critical Security Parameter
CSC	Card Security Controller
DES	Data Encryption Standard
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
GC	Generic Container
GP	Global Platform (Open Platform)
JCRE	Java Card ™ Runtime Environment
MAC	Message Authentication Code
OP	Open Platform
PIN	Personal Identification Number
RAM	Random Access Memory
ROM	Read only Memory
SD	Security Domain
SC	Secure Channel
TDES	Triple DES (112 -bit length keys)
XAUT	External Authentication

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

2 MODULE OVERVIEW

The DAL C3 module contains an implementation of the Open Platform (OP) Version 2.0.1 specification, which defines a secure infrastructure for post-issuance programmable smart card chips. OP Compliant modules have a life cycle defined by the OP specification. Transitions between different life cycle states have well defined sequences of operation. PINS and keys that have been securely loaded at card issuance authenticate the roles of the Crypto Officer/Issuer, Crypto Officer/Administrator and Card Holder.

3 SECURITY LEVELS

The DAL C3 module meets the overall requirements applicable to Level 3 security of FIPS 140-2. The individual security requirements specific for FIPS 140-2 meet the level specification indicated in the Table 2.

Table 2 - Security Requirements Specific to FIPS 140-2

Security Requirements Section	*Level*
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self Tests	3
Design Assurance	3
Mitigation of other attacks	3

4 CRYPTOGRAPHIC MODULE SPECIFICATION

The DAL C3 module is mounted in an ID-1 class smart card body that adheres to ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The “cryptographic boundary” for the DAL C3 module with respect to the FIPS 140-2 validation is the “module edge”. The module consists of the chip (ICC), the contact faceplate, and the micro-electronic connectors between the chip and contact pad, all contained within an epoxy substrate. The module is constructed so as to provide the tamper evidence required in the FIPS 140-2 physical Level 3 validation.

The DAL C3 module is a single chip implementation of a cryptographic module. The base module is the Axalto Cyberflex Access 64Kv1 Module, Axalto HW P/N M512LACC1, HardMask 5 V1, SoftMask 4 V1. Figure 1 shows a physical view of the module configured into a smart card. The figure shows only the module contact faceplate. The chip is located directly under the faceplate within the dashed outline shown.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

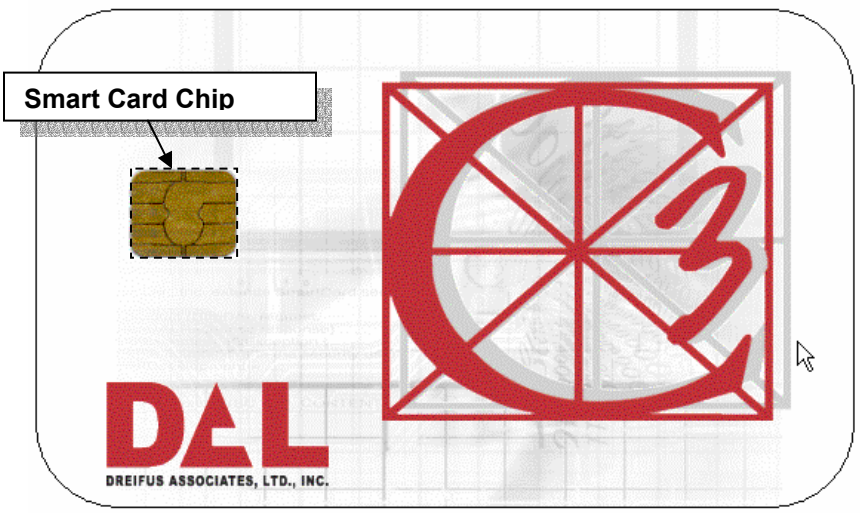

Figure 1. Physical View of the Cryptographic Module

The DAL C3 module consists of the following elements:

- Infineon SLE66CX640P, 8 bit micro controller. This IC is a standard, production-quality IC.
- System firmware is installed in Read Only Memory (ROM) as part of the chip manufacturing process (known as the Hard Mask) and in Electrically Erasable, Programmable Read Only Memory (EEPROM) for system option and additional customized software (known as the Soft Mask). The firmware is then designated: HardMask 5 V1; SoftMask 4 V1. These HardMask and SoftMask numbers are returned in the Answer To Reset (ATR) character string following the issuing of a RESET signal to the module (the ATR is: 3B 75 12 00 00 29 **05 01 04 01**).
- The DAL C3 Applets are loaded into the EEPROM of the module:

  The Applet version can be determined by a call to the GSCv2.1 command GET PROPERTIES. The applet version field is 4 bytes in length (Only the first two bytes are used for version information. The last two bytes contain build number information) The field is the second value returned from the call.

  - Access Control Applet Version 1.0
  - GSC Service Applet 1.0

- Critical Security Parameters are stored in the EEPROM as part of the module personalization operation.

The chip is encased in hard opaque epoxy-resin such that any attempt to gain physical access to the components would critically damage the module with a high probability of making the module unusable (the module will not function).

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

4.1 Operational Environment

The DAL C3 module has a limited operational environment consisting of a Java Virtual Machine operating on an Axalto Cyberflex Access 64Kv1 chip. The module does not support loading or execution of un-validated code.

4.2 Module Interfaces

4.2.1 Physical Interface Description

The DAL C3 module supports eight contacts that lead to pins on the chip. Only five of these contacts are used. The location of the contacts complies with ISO/IEC 7816-2 standard. Minimum contact surface area is 1.7 mm by 2.0 mm.

Contact dimensions are standard credit card compliant as per ISO/IEC 7816-1 standard:

Table 3 - Smart Card Chip Contact Area

Dimensions	*Value*
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

4.2.2 Electrical Interface Description

4.2.2.1 Specific Electrical Functions of Chip Contacts

Table 4 - Functional Specifications of Chip Contacts

Contact	*Function*
C1	Vcc supply voltage 3 to 5V +/-0.5 V
C2	RST (Reset)
C3	CLK (Clock)
C4	Not Connected to the chip
C5	GND (Ground)
C6	Not Connected to the chip
C7	I/O bi-directional line
C8	Not Connected to the chip

4.2.2.2 ICC SUPPLY CURRENT

- Maximum Value: 10mA at 5Mhz
- Typical Value: 3mA at 5Mhz

4.2.2.3 CHIP STRUCTURE

Chip Structure and ICC electrical contacts defined by ISO/IEC 7816-1&2

4.2.2.4 ELECTRICAL SIGNALING

Electrical signaling between “card acceptance device” (CAD) and the smart card chip is defined by ISO/IEC 7816-3.

4.2.2.5 MODULE SECURITY AND KEY ACCESS COMMAND SET

Module security and key access command set defined by the following specifications:

- ISO/IEC 7816-4.
- Global Platform – Open Platform – Card Specification v2.0.1 – 7 April 2000.
- Government Smart Card Interoperability Specification – Version 2.1 – 16 July 2003.

4.2.2.6 CAD TO MODULE COMMUNICATIONS PROTOCOLS

Card Accepting Device (CAD) to module communication protocols is defined by ISO/IEC 7816-3 & 4. This is based on a standardized, half-duplex character transmission, ISO 7816 protocol. Both protocols T=0 and T=1 are supported.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

4.2.2.7 EMI/EMC

The base cryptographic module has been tested to meet the EMI/EMC requirements specified by FCC Part 15, Subpart B, Class B. The cryptographic module is not used for radio communications.

4.2.3 Logical Interface Description

The I/O port (C7) of the platform (refer to Table 4) provides the following logical interfaces:

- Data In (I/O bidirectional line)
- Data Out (I/O bidirectional line)
- Control In (CLK, RST, and I/O bidirectional line)
- Status Out (I/O bidirectional line)

Synchronization timing controls provided in part by way of the platform CLK clock input, manages the separation of these logical interfaces that use the same physical port.

Electrical (physical) contact and data link layer contact is established between the smart card chip and the CAD by the CAD issuing a RESET signal to the smart card chip which then responds with an "Answer To Reset (ATR)" containing the version numbers of the hard and soft masks contained on the smart card chip. From this point on, the card functions as a "slave" processor to implement and respond to the CAD's "master" commands. The card adheres to a well defined set of state transitions. Within each state, a specific set of commands is accessible.

The details of these commands are defined in the DAL C3 Applets Technical Specification, GSC-ISv2.1 Specification and Open Platform 2.0.1 Specification. Additional commands are defined in the vendor documentation.

This interface is also known as a Virtual Card Edge Interface (VCEI) defined in the GSC-ISv2.1 Specification. The specification defines a default set of interoperable APDU level commands for both virtual machine and file system smart cards. The DAL C3 Applets reside on a virtual machine card and the VCEI consist of two providers and a shared library:

- Access Control Applet
  - Manages PINs
  - Provides Symmetric Key services
  - Manages access rights for all Generic Containers (GC) and PKI objects

- GSC Service Applet
  - Provides Generic Container service
  - Provides PKI service

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

Each of these providers (Applets) offers additional commands that the card will support, in addition to those commands provided by the basic resident (ROM-stored) software on the card. The GSC service provider provides containers for most types of data, services that act upon the containers and PKI services all at the VCEI. The Access control service provider manages PINs, provides symmetric and asymmetric key services and manages access rights for all GC and PKI objects at the VCEI.

5 FIPS-APPROVED MODE OF OPERATION

The following specific actions are required on the part of the Crypto Officer/Issuer along with a restriction within the module usage environment to ensure the module operates in FIPS-approved mode.

1. The CO/Issuer must instantiate all card applets to require a PIN for all Sign operations.
2. The CO/Issuer must instantiate all container applets to require External Authenticate or GP secure channel for all write operations.
3. The CO/Issuer must set the PIN Policies for the CO/Admin and Card Holder to have a minimum length of six bytes (characters).
4. The CO/Issuer must set the incorrect PIN counter to three failed attempts before locking the card.
5. End user environments must use the RSA public key $\mathbf{K_{PUBSM}}$ to wrap and pass a TDES session key $K_{sessionwrap}$ used to encrypt PIN material entered into the card.

In the FIPS140-2 level 3 mode of operation the Access Control Applet is instantiated with a PIN Protection Policy parameter set to 1. This instantiation forces the applets to only accept a PIN that has been encrypted using a TDES session key as defined in item 5 above. The operator can perform a GET ACR command to verify the PIN Protection Policy and retrieve the public $\mathbf{K_{PUBSM}}$ key.

An operator can use the Get PIN Policy and Get ACR command to verify that the access control rules are configured as described in this section

For key zeroization purposes, CO/Issuer may use a Put Key command with a key length parameter of zero to overwrite the RSA private keys or symmetric keys with zeros.

6 MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of the DAL C3 module is to provide a FIPS validated module for applets that may in turn provide cryptographic services to end-user applications. Cryptographic keys and CSPs (PINs) represent the roles involved in controlling the card. A variety of FIPS 140-2 validated algorithms are used in the DAL C3 module to provide cryptographic services; these include:

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

- TDES, (double-length TDES keys, $\mathbf{K_{ENC}}$ & $\mathbf{K_{MAC}}$): This algorithm uses the CO\Issuers $\mathbf{K_{ENC}}$ key to provide a secure channel and the CO\Issuer $\mathbf{K_{MAC}}$ key to MAC (integrity-protect) data sent within the secure channel. (OPv2.0.1 section 11.1)
- TDES: (double-length TDES key, $\mathbf{K_{KEK}}$) This algorithm uses the CO\Issuer $\mathbf{K_{KEK}}$ key to encrypt TDES keys that will use the PUT KEY command to place the key(s) into the module. (OPv2.0.1 section 11.1)
- TDES: (double-length TDES keys, GSC $\mathbf{K_{xauth}}$, GSC $\mathbf{K_{iauth}}$) This algorithm uses the GSC $\mathbf{K_{xauth}}$ key to authenticate a client application to the module and uses the GSC $\mathbf{K_{iauth}}$ key to authenticate the module to the application. (GSCv2.1, sections 5.3.5.2 and 5.3.5.3)
- RSA PKCS1 (1024bit GSC $\mathbf{K_{SIGN}}$): Used to sign data. . (GSCv2.1 section 5.3.6.1)
- RSA PKCS1 (1024bit DAL $\mathbf{K_{SM}}$): Used to unwrap symmetric (TDES) session keys $K_{\mathbf{sessionwrap}}$ used to pass encrypted PIN material into the module.
- SHA-1 Hashing.

Details of cryptographic functions are shown in this table:

Type	Algorithm	FIPS-Approved	Certificate
Public Key	RSA (key size: 1024)	Yes (FIPS 186-2)	Vendor affirmed
Symmetric Key	TDES (CBC), 2 keys TDES, TDES MAC	Yes (FIPS 46-3)	125 Vendor affirmed
Digest	SHA-1	Yes (FIPS 180-1)	108
RNG	DRNG (ANSI X9.31)	Yes (FIPS 186-2)	Vendor affirmed
	NDRNG (HARDWARE RNG)	No	

Table 5. Module Cryptographic Functions

7 SELF TESTS

7.1 POWER UP SELF TESTS

The DAL module performs the required set of self-tests at power-up time. When the module is inserted into a smart card reader and power is applied to the module (contact) interface, a "Reset" signal is sent from the reader to the module. The module then performs a series of GO/NO-GO tests before it responds (as specified by ISO/IEC 7816) with an Answer To Reset (ATR) packet of information. These tests include:

- RAM functional test & clearing at Reset
- DRNG and NDRNG functional test
- EEPROM Firmware integrity check
- Algorithm (known answer) tests for:
    - CRC16,

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

- DES (ECB & CBC mode encrypt/decrypt), for legacy systems, not available for use.
- TDES (ECB & CBC mode encrypt/decrypt)
- SHA-1 Hashing
- RSA PKCS1 encrypt/decrypt, sign and verify
- DRNG

If any of these tests fail, the module will respond with an ATR and a status indication of self-test error. Then, the module will go mute.

No data of any type is transmitted from the module to the reader while the self-tests are being performed.

7.2 CONDITIONAL TESTS

RSA Key generation:

- A pair wise consistency check is performed during key generation for both sign/verify and encrypt/decrypt.

Random Number Generator:

- HRNG: A 16 bits continuous testing is performed during each use of the Hardware non-deterministic RNG. The HRNG is used to generate seed values to feed the DRNG.
- DRNG: A 16 bit continuous test is performed during each use of the FIPS140-2 approved deterministic RNG.

Software/Firmware load test

- A TDES CBC MAC is verified each time an applet is loaded onto the Cyberflex Access 64K module.

8 ROLES & SERVICES

8.1 ROLES

The DAL C3 module uses identity-based access control in that individual operators have access to the module services. Access control rules provide services to operators who identify themselves by demonstrating knowledge of their cryptographic keys, or PINs, and presenting an operator ID.

The module defines three distinct roles that are supported by the on-card cryptographic system: the Crypto Officer/Issuer (CO/Issuer), Crypto Officer/Administrator (CO/Admin), and Card Holder.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

- Crypto Officer/Issuer is a role authenticated by demonstrating knowledge of a key set and key ID.
- Crypto Officer/Administrator is a role authenticated by knowledge of the Crypto Officer/Administrator PIN and Operator ID.
- Card Holder is a User role authenticated by knowledge of the Card Holder PIN and Operator ID.

The module ensures the authentication of off-card entities (the CO/Issuer, CO/Admin, and Card Holder) and provides them with cryptographic services according to their role.

8.1.1 CRYPTO OFFICER/ISSUER (CO/ISSUER)

The Cryptographic Officer/Issuer authenticates his role on the card by demonstrating to the Card Manager application that he possesses the knowledge of the $\mathbf{K_{ENC}}$ & $\mathbf{K_{MAC}}$ TDES key set and ID stored within the Card Manager. By successfully executing a series of commands, the Cryptographic Officer/Issuer establishes a secure channel to the Card Manager; establishment of this channel includes mutual authentication of roles between the Cryptographic Officer and the Card Manager. Once established, authorization (on the card) to access information and services is granted by the Card Manager. The Card Manager Security Domain corresponds to the Card Issuer Security Domain.

The DAL C3 module has a try counter of 10 for each key set contained on the module. The 10th consecutive failed attempt blocks the key set. The retry counts are per-key set. If the Card Manager has just one key set, blocking of the key set will block the module permanently.

8.1.2 CRYPTO OFFICER/ADMINISTRATOR (CO/ADMIN)

The Crypto Officer/Administrator role is authenticated by verification of the CO/Admin PIN and Operator ID. PIN verification is provided through the Access Control applet and has a maximum retry count of 3 before card locking occurs (See Section 5). The CO/Admin is responsible for not communicating his PIN. The CO/Admin can change the CO/Admin PIN using the CHANGE REFERENCE DATA command within a secure channel.

8.1.3 CARD HOLDER

The Card Holder (User) is responsible for ensuring the ownership of his card and for not communicating his PIN. The User is authenticated by verification of a PIN (Card Holder PIN) that the User has selected at issuance and an Operator ID. PIN verification is provided through the Access Control applet and has a maximum retry count of 3 before card locking occurs (See Section 5).

8.2 MODULE SERVICES (PER ROLE)

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

8.2.1 CRYPTO OFFICER/ISSUER SERVICES

A CO/Issuer authenticates his role to issue commands by proving knowledge of a CO/Issuer key set and using the key set to establish a secure channel. These commands include:

CHANGE REFERENCE DATA: this command is used to set the Crypto Officer/Administrator PIN (unblock PIN) and Card Holder PIN. The Operator ID parameter selects which PIN to set. The Crypto Officer/Issuer establishes the secure channel for this command, however the Card Holder enters the Card Holder PIN value to ensure its privacy. The Crypto Officer/Administrator sets the Crypto Officer/Administrator PIN similarly.

All PIN material must be encrypted using the $K_{sessionwrap}$ key the details of this are defined in the section 3.2 of the DAL C3 Applet Developers document. Below is an excerpt of the process.

The Access Control Applet employs a secure messaging protocol to facilitate secure communication of authentication material sent to the card. Compared to other secure channel mechanisms, this mechanism does not rely on any secret shared between the host and the card, still it provides high degree of privacy and resistance against re-play attacks.
Specifically, this mechanism applies to PIN values being transferred to the card by the VERIFY PIN and the CHANGE REFERENCE DATA commands.

The essence of the protocol is that the AC applet hosts a RSA key pair. During establishment of a secure messaging session using the MANAGE SESSION command, the host generates a double length 3DES key that it sends to the card, wrapped with the AC applet's public key. The 3DES key associated with the session can then be used to protect subsequent commands.

CREATE OBJECT: this GSC Service Applet command is used to create a Generic Container (GC) or a PKI object. The Access Control Rights (ACR's), defined in the GSC-ISv2.1 specification, are chosen for the object at this time.

DELETE: this Open Platform command is used to delete a single Load File (package) or an Application (applet instance) in the module.

OP EXTERNAL AUTHENTICATE: Open Platform command used by the module to authenticate the CO\Issuer, to establish a Secure Channel. A previous and successful execution of the **INITIALIZE UPDATE** command is required prior to processing this command.

GENERATE RSA KEY: this command is used to generate the defined 1024 bit RSA key pairs: $\mathbf{K_{SIGN}}$ and $\mathbf{K_{SM}}$. When generating RSA keys, the desired public

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

exponent is passed to the module. On successful key pair generation the public key is stored in the module and returned from the module.

The signature verification public key $\mathbf{K_{PUBSIGN}}$ may be signed by an external CA and made available in a certificate by using the $\mathbf{K_{PUBSIGN}}$ key returned from the module.

The $\mathbf{K_{PUBSM}}$ public key stored in the module and retrieved by a **GET ACR** command is used to wrap a TDES session key $\mathbf{K_{sessionwrap}}$ generated by the client, for the purpose of secure messaging, based on ISO7816-4. The $\mathbf{K_{sessionwrap}}$ session key is then used to encrypt PIN material to be sent to the module for PIN verification purposes. This process requires the successful execution of the **MANAGE SESSION** command.

GET CHALLENGE: this GSC-ISv2.1 command causes the module to generate an 8-byte challenge.

GET DATA: this Open Platform command is used to retrieve a single, specified data object from the Card Manager. Card Manager data objects are define in the OPv2.0.1 specification.

GET STATUS: this Open Platform command is used to retrieve Card Manager, Executable Load File and Application related life cycle status information according to a given search criteria.

INITIALIZE UPDATE: this Open Platform command is used to initiate a Secure Channel with the Card Manager. Card and host session data are exchanged, and session keys ($\mathbf{K_{enc}}$ & $\mathbf{K_{mac}}$) generated by the card. The Secure Channel is considered open upon completion of a successful **EXTERNAL AUTHENTICATE** command that must immediately follow the **INITIALIZE UPDATE** command.

INSTALL: this Open Platform command is used to install an application or a Security Domain and requires the invocation of several different module functions. The command is used to instruct a Security Domain or the Card Manager as to which installation step it shall perform during an application installation process.

LOAD: this Open Platform command is used to load the byte-codes of a Load File (package).

MANAGE SESSION: Opens or closes a secure session for passing TDES encrypted PINs to the module. The module issues a random challenge to preclude replay attacks. The response includes a TDES session key that is wrapped in the RSA public key.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

PUT KEY: this Open Platform command is used to add or replace Security Domain key sets.

DAL PUT KEY – this command is used to load the GSC $\mathbf{K_{xauth,}}$ & $\mathbf{K_{iauth}}$ TDES keys and the $\mathbf{K_{SIGN}}$ & $\mathbf{K_{SM}}$ RSA keys. A **PUT KEY** command with a key zeroization parameter (key length of zero) will zeroize the keys. The command P1 parameter (the key version number) determines which key is being loaded onto the module.

The K_{xauth} and K_{iauth} are static TDES keys that are utilized by the defined GSC-ISv2.1 commands EXTERNAL AUTH and INTERNAL AUTH. The keys must be encrypted using the TDES K_{KEK} key prior to using the PUT KEY command.

The $\mathbf{K_{SIGN}}$ and $\mathbf{K_{SM}}$ are RSA keys that can be put in the module utilizing the PUT KEY command. When the keys are put into the module using the PUT KEY command the CO/Issuer must establish a secure channel first. The format of the keys follows the DAL C3 Applet Developers document, section 3.5.4.

The modulus and public exponent of a RSA private key are loaded by 2 repeated PUT KEY commands, once for each of the 2 components. The components are stored in any order, however all components must be stored for the key to be valid.

The CRT components of a RSA private key are loaded by 5 repeated PUT KEY commands, once for each of the 5 components. The components are stored in any order, however all components must be stored for the key to be valid.

READ BUFFER: this GSC-ISv2.1 command is used to retrieve tagged data objects from a Generic Container (GC). The access rights (ACR's) to the Generic Container are established when the object was created using the **CREATE OBJECT** command.

UPDATE BUFFER: this GSC-ISv2.1command is used to store or replace tagged data objects in a Generic Container. The access rights (ACR's) to the Generic Container are established when the object was created using the **CREATE OBJECT** command.

SET PIN POLICY: this command sets the PIN policy for the Crypto Officer/Administrator PIN or Card Holder PIN based upon the Operator ID specified. The PIN policy sets the minimum and maximum PIN lengths along with other PIN parameters.

SET STATUS – this Open Platform command modifies the life cycle state of the card or the lifecycle state of an application defined in the OPv2.0.1 specification.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

8.2.2 CRYPTO OFFICER/ADMINISTRATOR SERVICES

The following commands are available to the Crypto Officer/Administrator:

CHANGE REFERENCE DATA: This command is used by the CO/Admin to change the existing Crypto Officer/Administrator PIN to a different value or to unblock a Card Holder PIN that was previously blocked because the Card Holder entered their PIN incorrectly three times. The Card Holder is again able to authenticate using the Card Holder PIN after a successful unblock of the PIN. The Operator ID selects which PIN to modify. This command always requires the Crypto Officer/Administrator to enter the Crypto Officer/Administrator PIN.

GSC EXTERNAL AUTHENTICATE: this GSC-ISv2.1 command is used by the module to authenticate the external client application. The details are defined in section 5.1.2 and 5.3.5.2 of the NIST GSC-ISv2.1 specification.

This command is subject to a try counter with a value of 10. The value is set in byte 6 of the Instantiation Parameter for the Access Control applet. After the 10th consecutive failed attempt to use this command, the key is locked but can be re-enabled via the CO/Issuers use of the **DAL PUT KEY** command.

MANAGE SESSION: Opens or closes a secure session for passing TDES encrypted PINs to the module. The module issues a random challenge to preclude replay attacks. The response includes a TDES session key that is wrapped in the RSA public key.

VERIFY PIN: this command via the *Access Control Applet* is used to verify the Crypto Officer/Administrator PIN. The Crypto Officer/Administrator must enter the Crypto Officer/Administrator PIN and Operator ID for verification.

LOGOUT ALL: This command clears all authentication states.

INTERNAL AUTHENTICATE: this GSC-ISv2.1 command is used to perform a challenge-response authentication used for authenticating the module to the external client application. The details are defined in section 5.1.2 and 5.3.5.3 of the NIST GSC-ISv2.1 specification.

8.2.3 CARD HOLDER SERVICES

The following commands are available to the Card Holder:

PRIVATE SIGN – This command performs an RSA signature generation. Data decryption is not allowed in this module.

LOGOUT ALL: This command clears all authentication states.

VERIFY PIN: This command is used to verify the Card Holder PIN, or to check whether or not the PIN has been already verified.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

MANAGE SESSION: Opens or closes a secure session for passing TDES encrypted PINs to the module. The module issues a random challenge to preclude replay attacks. The response includes a TDES session key that is wrapped in the RSA public key.

8.2.4 UNAUTHENTICATED SERVICES (NO ROLE)

The following commands are available without requiring authentication.

SELECT: this command is used for selecting an application (Card Manager, Security Domain or Applet).

GET DATA: this Open Platform command is used to retrieve a single, specified data object from the Card Manager. Card Manager data objects are defined in the OPv2.0.1 specification. (see the Note for Table 6.)

GET PIN POLICY: this command returns the PIN policy for the Crypto Officer/Administrator PIN or Card Holder PIN. The Operator ID parameter determines which PIN policy is returned.

GET PIN STATE: this command returns one of four possible states for PINs. The four states are the following:

0 - Undefined. The PIN is effectively invalid.

1- Initial. The PIN must be changed before it can be used to authorize any privileged operations.

2- Normal.

3- Blocked. The PIN is blocked due to too many unsuccessful attempts.

The user must enter a proper Operator ID to retrieve the state of the PIN. No relevant security information can be obtained via this command, only the state of the PIN based on the operator.

GET PROPERTIES: this GSC-ISv2.1command is used to retrieve applet instance properties of a currently selected applet. All properties are defined in section 5.3.3.4 of the GSC-ISv2.1 specification. Some of the properties such as Applet version are used to provide middleware software the ability to configure itself properly for proper function The command does not provide key data and is mainly utilized by middleware as defined in the NIST GSC-ISv2.1 specification.

GET ACR: this GSC-ISv2.1 command is used to retrieve access control rules. All available ACR information is defined in section 5.3.3.5 of the GSC-ISv2.1 specification. The command has also been extended to retrieve the RSA $\mathbf{K_{PUBSM}}$ public key that is used in the **MANAGE SESSION** command.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

GET RESPONSE: this command is used to retrieve the response message from the immediately proceeding command.

SELECT OBJECT this GSC-ISv2.1command selects a GC or PKI object inside a GSC Service Applet instance.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

8.2.5 RELATIONSHIP BETWEEN ROLES AND SERVICES PER APPLET

Table 6 Lists available services for each application on the card and shows which role is required to use each service. X denotes a service is available within the role.

Table 6. Roles and Services per Applet.

Services / Roles	No Role	Crypto Officer / Issuer *	Crypto Officer / Admin	Card Holder
CARD MANAGER SERVICES				
DELETE		X		
EXTERNAL AUTHENTICATE		X		
GET DATA	X	X		
GET STATUS		X		
INITIALIZE UPDATE	X			
INSTALL		X		
LOAD		X		
PUT KEY		X		
SELECT	X			
SET STATUS		X		
ACCESS CONTROL APPLET SERVICES				
CHANGE REFERENCE DATA		X	X	X
GET PIN POLICY	X			
GET PIN STATE	X			
DAL PUT KEY		X		
SET PIN POLICY		X		
GSC SERVICE APPLET SERVICES				
CREATE OBJECT		X		
GET PROPERTIES	X			
GENERATE RSA KEY		X		
PRIVATE SIGN				X
DAL PUT KEY		X		
READ BUFFER	X	X[1]	X[1]	
SELECT OBJECT	X			
UPDATE BUFFER		X		
SERVICES COMMON TO ALL APPLETS				
GET ACR	X			
GET CHALLENGE	X			
GET RESPONSE	X			
GSC EXTERNAL AUTHENTICATE	X	X		
INTERNAL AUTHENTICATE	X			
LOGOUT ALL		X	X	X
MANAGE SESSION		X	X	X
DAL PUT KEY		X		
SELECT	X			
VERIFY PIN			X	X

* Crypto Officer/Issuers may use the GET DATA command within a secure channel.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

[1.] The READ BUFFER command is available outside of a Secure Channel (no security condition). However, if issued within a Secure Channel, it must follow the same security level as defined in EXTERNAL AUTHENTICATE.

9 CRITICAL SECURITY PARAMETERS

9.1 CRYTOGRAPHIC KEYS

The DAL C3 module includes the following keys:

- Initialization Key, $\mathbf{K_{init}}$ used only for the first Card Manager key-set loading,
- Crypto Officer/Issuer Security Domain keys ($\mathbf{K_{ENC}}$, $\mathbf{K_{MAC}}$, & $\mathbf{K_{KEK}}$),

A Security Domain key set is structured to contain three types of TDES keys:

> $\mathbf{K_{ENC}}$, used to generate session keys for the Crypto Officer/Issuer and encrypted mode of the secure channel,
> $\mathbf{K_{MAC}}$, used to generate session key for MAC mode of the secure channel Authentication,
> $\mathbf{K_{KEK}}$, used to encrypt keys, to be imported into the module.

Security Domains allow a number of distinct identities to be established on the Cyberflex Access 64Kv1 module. These are identities that control access to the various applets stored on the Cyberflex Access 64Kv1 module. A Security Domain represents the identity of the Crypto Officer/Issuer.

- TDES Session keys, $\mathbf{K_{enc}}$ & $\mathbf{K_{mac}}$ (keys generated from the Crypto Officer/Issuer keys set(s)) details define in OP2.0.1 section 13.1,
- GSC External Authenticate Key, K_{xauth} used to authenticate a client application to the module details define in GSCv2.1 section 5.3.5.2 & 5.1.2.1.
- GSC Internal Authenticate Key, K_{iauth} used to authenticate the module to the client application details define in GSCv2.1 section 5.3.5.3 & 5.1.2.3.
- Manage Session Key, $K_{sessionwrap}$ TDES client generated session key (passed externally from client) used to decrypt session data (secure passing of PIN material).

The Access Control Applet employs a secure messaging protocol to facilitate secure communication of authentication material sent to the module. Compared to other secure channel mechanisms, this mechanism does not rely on any secret shared between the host and the module, still it provides a high degree of privacy and resistance against re-play attacks.

Specifically, this mechanism applies to PIN values being transferred to the module by the VERIFY PIN and the CHANGE REFERENCE DATA commands.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

The essence of the protocol is that the AC applet hosts a RSA key pair. During establishment of a secure messaging session using the command, the host generates a double length 3DES key ($K_{sessionwrap}$) that it sends to the module, wrapped with the AC applet's public key. The $K_{sessionwrap}$ key associated with the session can then be used to protect subsequent commands.

The RSA key pair is either generated by the module using the GENERATE RSA KEY command or loaded to the card during applet pre-personalization by the PUT KEY command. The public key can be retrieved from the card by the GET ACR command.

Details can be found in ISO7816-4 (Secure Messaging) and DAL C3 Applets Developers Technical Document starting in section 3.2.

9.2 PUBLIC KEYS

Public keys can be generated on the card (GENERATE RSA KEY), or loaded onto the card (PUT KEY).

K_{SIGN} (Key pair)

- RSA Public Sign Key, **$K_{PUBSIGN}$** for signature verification operations.
- RSA Private Key for Sign operations $K_{PRIVSIGN}$

K_{SM} (Key pair)

- RSA Public Key **K_{PUBSM}** for wrapping the TDES session key ($K_{sessionwrap}$).
- RSA Private Key **K_{PRIVSM}** for unwrapping the TDES session key ($K_{sessionwrap}$)

9.3 OTHER CSPS

The DAL C3 module includes two CSPs (two Personal Identification Numbers (PINs) managed by the Access Control Applet):

- A Card Holder PIN to authenticate the Card Holder
- . A Crypto Officer/Administrator PIN used by the Crypto Officer/Administrator to unblock a blocked Card Holder PIN.

The User PIN is 6 - 125 character string that may be used to authenticate the Card Holder to the card. That is, by successfully entering a PIN sequence, a Card Holder can prove knowledge of a shared secret (the PIN) and thereby authenticate himself to the card. The CHANGE REF DATA is available to the Crypto Officer/Admin to change or unblock a PIN.

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

The Crypto Officer/Administrator PIN is 6 - 125 character string that may be used to authenticate the CHANGE REF DATA command.

10 SECURITY RULES

10.1 IDENTIFICATION & AUTHENTICATION SECURITY RULES

The module implements specific methods for authenticating the different roles. The implementation consists of the binding of an Identity-based Access Control Rule to each service that requires a role.

10.1.1 CARD HOLDER IDENTIFICATION AND AUTHENTICATION

Proving knowledge of the Card Holder PIN and Operator ID authenticates the Card Holder.

10.1.2 CRYPTO OFFICER/ISSUER IDENTIFICATION AND AUTHENTICATION

The Crypto Officer/Issuer must prove the possession of the Card Manager Key Set and Key ID to authenticate his role. The $\mathbf{K_{ENC}}$ & $\mathbf{K_{MAC}}$ keys are used to generate the $\mathbf{K_{enc}}$ & $\mathbf{K_{mac}}$ TDES session keys to authenticate the command payload. The $\mathbf{K_{KEK}}$ key is used to encrypt keys transported within the command (Initialize Update & External Authenticate commands).

10.1.3 CRYPTO OFFICER/ADMINISTRATOR IDENTIFICATION AND AUTHENTICATION

The Crypto Officer/Administrator must prove knowledge of the Crypto Officer/Administrator PIN and Operator ID to authenticate his role.

10.2 PHYSICAL SECURITY RULES

The physical security of the DAL C3 module is designed to meet FIPS 140-2 level 3 requirements. A hard opaque epoxy is used to encapsulate the module to meet level 3 requirements. From the time of its manufacture, the card is in possession of the Crypto Officer until it is ultimately issued to the end user.

10.3 KEY MANAGEMENT SECURITY POLICY

10.3.1 CRYPTOGRAPHIC KEY GENERATION

RSA key pairs may be generated using the GENERATE RSA KEY function along with a key ID. The public key is returned from the function and may be used externally from the module by being included on a digital certificate establishing the relationship between the public-key and the role of the Card Holder. The private-key, which is retained securely within the PKI Container, is used to establish the identity of the Card Holder by verifying a digital signature. The Access Control applet contains the $\mathbf{K_{SM}}$ Generated RSA key pair

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

that is used for the sole purpose of securely transporting a TDES session key $K_{sessionwrap}$ that is used to encrypt PIN material that will be passed to the module.

10.3.2 CRYPTOGRAPHIC KEY ENTRY

Security Domain Keys are input to the Card Manager in encrypted format, using the PUT KEY command within a secure channel. During this process, the keys are double encrypted (using the Session Key $\mathbf{K_{enc}}$ and the $\mathbf{K_{KEK}}$ Key).

RSA key pair CRT components may be generated off card and imported onto the card (using the PUT KEY command within the secure channel). The public-key is used externally from the module by being included on a digital certificate establishing the relationship between the public-key and the User. The certificate containing the public key may be stored on the card in a GSC container. The private-key, which is retained securely within the PKI Container, is used to establish the identity of the Card Holder by forming a digital signature.

10.3.3 CRYPTOGRAPHIC KEY STORAGE

All secret and private keys are structured to contain the following parameters:

- Key id, which is the Id of the key
- Algo Id
- Integrity Mechanisms (ECC)

The symmetric session keys reside in RAM only and become invalid when a secure channel session ends.

All keys, the Crypto Officer/Administrator PIN and Card Holder PIN are stored in plaintext format in EEPROM.

10.3.4 CRYPTOGRAPHIC KEY DESTRUCTION

The module destroys secret and private cryptographic keys by using a PUT KEY command with a key length value of the key component set to zero. This zeroizes the key selected by the key version (P1) parameter.

10.4 STRENGTH OF AUTHENTICATION

10.4.1 TRIPLE DES KEYS

Each of the Triple DES keys used by the CO/Issuer has an effective key length of 168 bits. This results in over 3^{50} possible keys for the Triple DES keys in the CO/Issuer 3 key set which far exceeds the 1 in a million test requirement.

To try a key against the module, an attacker must send a minimum 13 byte APDU to the card, and get a resulting 2-byte response. As there is a single I/O port on the module, each Triple DES key attempt requires 15 bytes of data to be clocked in or out of the card. The maximum data rate for the module is 115Kbps through this single port. Ignoring the

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

processing time required on the module to process the triple DES key, we can compute the maximum number of attempts which could occur within a 60 second interval:

- 15 bytes of I/O at 8bits/byte = 120bits/attempt
- 120bits/attempt divided by 115,000bits/second = .001043seconds/attempt
- 60seconds/minute divided by .001043seconds/attempt = 57,526attempts/minute

As the Triple DES key space is over 3^{50} possible values, it follows that 57,526 attempts in a 60 second interval will not significantly traverse the space of possible values. As a result, the module far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

Finally, the modules try counter limits an attacker to 10 attempts per key set before locking the key set against further attempts.

10.4.2 CO/ADMIN PIN AND USER PIN

The length of the CO/Admin PIN and the User PIN is a character string of 6 to 125 characters. PINs may contain any keyboard characters including Shift-number combinations. That is, each byte of the PIN can be one of the character sets (a-z, A-Z, 0-9) yielding a minimum of 62^4 or approximately 14.7 million possible PINs. This far exceeds the 1 in a million test.

To try a PIN against the module, the attacker must send a 9 byte APDU to the card, and get a resulting 2-byte response. As there is a single I/O port on the module, this means that each PIN attempt requires 11 bytes of data to be clocked in or out of the card. The maximum data rate for the module is 115Kbps through this single port. If we ignore the processing time required on the module to check the PIN, we can compute the maximum number of PIN attempts which could occur within a 60 second interval:

- 11 bytes of I/O at 8bits/byte = 88bits/attempt
- 88bits/attempt divided by 115,000bits/second = .000765seconds/attempt
- 60seconds/minute divided by .000765seconds/attempt = 78,431attempts/minute

As the minimum length PIN results in over 14.7 million possible values, it follows that 78,431 attempts in a 60 second interval will not significantly traverse the space of possible PIN values. As a result, the module far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

Moreover, an 8 bit counter internal to the Access Control applet further limits the number of failed PIN attempts an attacker could perform by blocking the card if the counter limit (3 attempts per PIN set) is exceeded.

10.5 MITIGATION OF ATTACKS SECURITY POLICY

The DAL C3 module has been designed to mitigate the following attacks:

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

- Simple Power Analysis (SPA)
- Differential Power Analysis (DPA)

11 SECURITY POLICY CHECK LIST TABLES

11.1 ROLES & REQUIRED AUTHENTICATION

Table 7. Roles and Required Authentication

Role	*Type of Authentication*	*Authentication Data*
Crypto Officer/Issuer	TDES authentication	TDES keys (Crypto Officer Security Domain) $\mathbf{K_{ENC}}$, $\mathbf{K_{MAC}}$ & $\mathbf{K_{KEK}}$
Crypto Officer/Admin	PIN, TDES authentication	Crypto Officer/Administrator PIN K_{xauth} & K_{iauth}
User	PIN	Card Holder PIN

11.2 STRENGTH OF AUTHENTICATION MECHANISMS

Table 8. Strength of Authentication Mechanisms

Authentication Mechanism	*Strength of Mechanism*
TDES authentication	High (Far exceeds the 1 in a million test)
PIN-based authentication	High (Far exceeds the 1 in a million test)

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

ACCESS RIGHTS WITHIN SERVICES

Table 9. Access Rights Within Services

Service	*CSP*	*Type of Access (eg. Read, Write, Execute)*
Crypto Officer/Issuer		
External Authenticate (Secure Channel)	TDES CO Keys	Execute
PUT KEY	TDES CO Keys	Write
DAL PUT KEY	TDES K_{xauth} & K_{iauth} RSA $K_{PRIVSIGN}$ & K_{PRIVSM}	Write
CHANGE REFERENCE DATA (P2=00H)	Card Holder PIN Crypto Officer/Administrator PIN	Write
GENERATE RSA KEY	RSA $K_{PRIVSIGN}$ & K_{PRIVSM}	Write
Crypto Officer/Admin.		
Verify PIN	Crypto Officer/Administrator PIN	Read
CHANGE REFERENCE DATA (Change Unblock PIN)	Crypto Officer/Administrator PIN	Write
CHANGE REFERENCE DATA (Unblock PIN)	Card Holder PIN	Write
User		
Verify PIN	Card Holder PIN	Read
SIGN	RSA $K_{PRIVSIGN}$	Execute

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.

11.3 MITIGATION OF OTHER ATTACKS

Table 10. Mitigation of Other Attacks

Other Attacks	*Mitigation Mechanism*	*Specific Limitations*
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A

12 REFERENCES

1. Global Platform – Open Platform – Card Specification v2.0.1 – 7 April 2000.
2. Government Smart Card Interoperability Specification – Version 2.1 – 16 July 2003.
3. Security Policy for Schlumberger Cyberflex Access 32K Smart Card with Schlumberger PKI Applets – Version 1.07 – 6 June 2003.
4. Security Policy for Schlumberger Cyberflex Access 64K Smart Card. Revision: 2.3 (2002)

This document may be reproduced only in its original entirety (without revision).
Copyright Dreifus Associates Limited, Inc.- 2003, 2004.