Security Policy

for

Schlumberger Cyberflex Access 32K Smart Card with ActivCard Applets

Public Version 1.2

TABLE OF CONTENTS

1 Scope of Document

This document defines the Security Policy for the Schlumberger Cyberflex 32K with ActivCard Applets smart card. Included is a description of the basic security requirements for the Cyberflex 32K with Applets card and a qualitative description of how each security requirement is achieved.

2 Introduction

The Cyberflex 32K with Applets smart card contains an implementation of the Open Platform (OP) Version 2.0.1 specification, which defines a secure infrastructure for post-issuance programmable smart cards. The OP specification defines a life cycle for OP compliant cards. State transitions between states of the life cycle involve well defines sequences of operations. Cards which have been issued to a Cardholder are necessarily in a “SECURE” state. This means that a defined set of applications have been loaded onto the card plus a set of keys and a PIN through which the identities of the Cryptographic Officer and the Cardholder can be authenticated.

3 Security Levels

The Cyberflex 32K with Applets smart card (cryptographic module) meets the overall requirements applicable to Level 2 security of FIPS 140-1. The individual security requirements specified for FIPS 140-1 meet the level specifications indicated in the following table.

Security Requirements Section	Level
Cryptographic Module	2
Module Interfaces	2
Roles and Services	2
Finite State Machine	2
Physical Security	3
Software Security	3
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	2
Self-Tests	2

3.1 Cryptographic Module Specification

Cyberflex 32K with Applets is an ID-1 class smart card that adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The “cryptographic boundary” for the Cyberflex 32K with Applets card vis-à-vis the FIPS 140-1 validation is the “module edge”. The module is comprised of the chip (ICC), the contact faceplate, and the micro-electronic connectors between the chip and contact pad. The module is constructed so as to provide the tamper resistance and the tamper evidence required in the FIPS 140-1 physical Level 3 validation.

Cyberflex 32K with Applets is a single chip implementation of a cryptographic module.

3.2 Module Interfaces

The electrical and physical interface of the Cyberflex 32K with Applets module, as a cryptographic module, is comprised of the 8-electrical contacts from the face of the card to the chip. These contacts conform to the following specifications:

3.2.1 Physical Interface Description

The Cyberflex 32K with Applets card supports eight contacts that lead to pins on the chip. Only five of these are used. The location of the contacts complies with ISO/IEC 7816-2.

Minimum contact surface area: 1.7mm * 2.0 mm

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

Dimension	Value
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

3.2.1.1 Electrical Specifications

Specific electrical functions of the contacts:

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

ICC supply current:

- MAX: 50 mA at 5MHz
- TYP: 5 mA at 5MHz
- Card structure and ICC electrical contacts defined by ISO/IEC 7816-1&2.
- Electrical signaling between the “card acceptance device” (CAD) and the card defined by ISO/IEC 7816-3.
- Card security and key access command set defined by ISO/IEC 7816-4.
- CAD to card communication protocols defined by ISO/IEC 7816-3 & 4.

3.2.2 Logical Interface Description

Once electrical (physical) contact and data link layer contact is established between the card and the CAD, 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 Cyberflex 32K with Applets Technical Specification Document that is included as a proprietary and private extension to this Cyberflex 32K with Applets Security Policy document.

This card also provides an additional set of on-card services through the Java Card APIs. The API classes and their associated methods are also defined in the Cyberflex 32K with Applets Technical Specifications.

3.3 Roles and Services

The Cyberflex Access 32K with Applets supports two User roles, a Cardholder and an Application Operator, and one Cryptographic Officer role. See section 4 for a complete description of Roles and Services.

3.4 Finite State Machine Model

The Cyberflex 32K with Applets smart card is compliant with the ISO/IEC 7816-3,4 specifications. This means that the card communicates via Application Protocol Data Unit packets transferred from the CAD to the card, followed by a response APDU from the card back to the CAD. Within this protocol, the card functions as a pure, finite state machine. The card's system software undergoes a set of well-defined state transitions, as keys are stored on the card to establish Security Domains. Applets also progress through a set of well-defined state transitions as they are loaded, installed, and prepared for execution.

The Finite State Model for the Cyberflex 32K with Applets card is published as a separate document.

3.5 Physical Security

The physical security of the Cyberflex 32K with Applets module is designed to meet FIPS 140-1 level 3 requirements. From the time of its manufacture, the card is in possession of the Cryptographic Officer until it is ultimately issued to the User. From that point, the card is in the physical possession of the User.

To attack the cryptographic information contained in the module, that is to attempt to compromise this information, requires physical access to the card. To eavesdrop on normal activities of the module, while it is still in possession of either the Cryptographic Officer or of the User, will be demonstrated to be difficult or impossible due to the protocols and security mechanisms protecting access to the module's information and services. To eavesdrop on the module through extraordinary means requires physical possession of the card. In this event, the absence of the card is detected by either the Cryptographic Officer or the User and the capabilities of the card within a larger systems context can be disabled.

If the module is attacked through physical means, the attack will be evident due to the disturbance of the packaging of the card and module. The ICC is embedded within an epoxy

coating that is extremely difficult to penetrate without leaving evidence of the attack. Further, the packaging itself is resistant to penetration.

3.6 Software Security

The basic systems software of Cyberflex 32K is secure from modification due to the fact that it is stored in ROM. This systems software is written primarily in the C programming language that allows for extensive review to confirm security.

- Software security of the Cyberflex 32K with Applets card is strictly controlled by the Card Manager application

The card systems software includes an on-card Java Card Virtual Machine. Applets are secure from each other due to the fact that each runs in a "Java sandbox". The Java Card language does not contain any constructs that allow cross-sandbox communication directly; any such communication must go by way of systems software mechanisms, which allow for implementation of strict security measures. No applets or source code may be loaded onto the card after completion of the manufacturing process.

3.7 Operating System Security

This section is not applicable to this certification due to the fact that no applets or source code may be loaded onto the card after completion of the manufacturing process.

3.8 Key Management

The Cyberflex Cyberflex 32K with Applets smart card includes the following set of keys:

- Initialization Key, K_{init} used only for the first Card Manager key-set loading,
- Security Domain sets containing three types of keys:
  1. $K_{enc,auth}$ used for Cryptographic Officer authentication per OP Specification
  2. K_{mac}, used for Cryptographic Officer authentication per OP Specification
  3. K_{ek} used as Key Wrapping Key for inputting security domain key sets into the module

The module contains an ANSI X9.17 PRNG for generation of RSA key pairs.

3.9 Cryptographic Algorithms

The following algorithms are performed by the Cyberflex Access 32K with Applets.

- TDES CBC
- SHA-1
- RSA Signature (PKCS #1 compliant)

3.10 EMI/EMC

The Cyberflex Access 32K with Applets has been tested to meet the EMI/EMC requirements specified by FCC Part 15, Subpart J, Class A

3.11 Self-tests

The Cyberflex 32K with Applets card performs the required set of self-tests at power-up time. When the Cyberflex 32K with Applets card is inserted into a CAD, once power is applied to the card (contact) interface, a "Reset" signal is sent from the CAD to the card. The card 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 cleared at Reset
- EEPROM integrity check
- Algorithm (known answer) tests for:
- 3DES
- SHA-1 Hashing
- RSA signature

If any of these tests fail, the card will respond with an ATR and a status indication of self-test error. Then, the card will go mute. No data of any type is transmitted from the card to the CAD while the self-tests are being performed.

4 Roles and Services

The Cyberflex Access 32K smart card defines three distinct roles that are supported by the on-card cryptographic system: the Cryptographic Officer, the Cardholder, and Application Operator roles.

- Cryptographic Officer: established by demonstrating knowledge of a key set
- Cardholder: a User role as authenticated by knowledge of a PIN
- Application Operator: a User role as authenticated by knowledge of a TDES key

The Card Manager is the controlling application on the card. It is invoked following every card reset and initialization operation. The Cryptographic Officer establishes his identity on the card by demonstrating to the Card Manager application that he possesses the knowledge of a key set stored within the Card Manager. By successfully executing a series of commands, the Cryptographic Officer establishes a secure channel to the Card Manager; establishment of this channel includes mutual authentication of identities between the Cryptographic Officer and the Card Manager. Once established, authorization (on the card) to information and services is granted by the Card Manager.

Through on-card applets, services are provided to the cardholder based on his authenticating his identity. The cardholder authenticates his identity to the applets by proving knowledge of a Personal Identification Number (PIN) stored within the Card Manager (the Global PIN). Individual applets can have additional PINs, allowing them to do their own authentication of the cardholder.

The module insures the authentication of off-card entities and provides them with cryptographic services according to their role.

4.1 User Roles

- **Card Holder** - The Card Holder is responsible for insuring the ownership of his card and for not communicating his PIN. The Card Holder is authenticated by verification of a PIN.

- **Application Operator** – The Application Operator represents an off-card entity operating an external application requesting the services offered by the applets. The applet authenticates the Application Operator role by verifying the possession of a TDES key.

4.2 Cryptographic Officer Role

The Cryptographic Officer is responsible for managing the security configuration of the applets, and in particular executes the necessary PIN and key management operations for the applet. The Cryptographic Officer owns a Card Manager or Security Domain Key Set, and has therefore access to the services offered by the Card Manager or Security Domain. The Cryptographic Officer has also the privilege to unblock the PIN, after successive wrong PIN values have been tried. This is done by externally authenticating himself by proving the possession of a TDES key, in order to access the PIN unblock service of an ID applet instance.

4.3 Role Authentication

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

4.3.1 User Authentication

- **PIN**: the Card Holder must send a Verify PIN command to any applet to access any Applet service protected with PIN. The APDU corresponding to the applet service must be sent before the card is removed or a reset order is send to the card.
- **PIN Always**: the Card Holder must send a Verify PIN command to any applet to access any applet service protected with PIN Always
- **External Authentication (XAUT)**: The Application Operator must prove the possession of a particular 3DES key to access the GC Applet read or update service protected with External Authentication with this particular key.

4.3.2 Cryptographic Officer Authentication

- **OP Authentication**: The Cryptographic Officer must prove the possession of a Key Set composed of 3 3DES keys. Two keys are used to authenticate the command payload. A third key is used to encrypt keys transported within the APDU command.
- **External Authentication (XAUT)**: The Cryptographic Officer must prove the possession of a particular 3DES key to access the ID Applet PIN unblock service protected with External Authentication with this particular key..

4.4 Services

The applet services are invoked by external APDU commands sent to the card. The Access Control Rules(ACRs) are applied on the APDU commands.

4.4.1 ID Applet Services

The ID applet provides Card Holder Verification (CHV) services. Here are the different APDUs / Services that are provided by an ID applet instance:

- **Select**: This APDU causes the selection of the applet.
- **Install**: This APDU causes the installation of the applet.

- **Change PIN/Unblock**.
  - The Change PIN APDU is used by the cryptographic officer to set a new PIN value and recover Card Holder access.
  - the Change PIN APDU is also used by the Card Holder to set a new PIN value upon presentation of the current PIN
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.
- **Initialize update**. This APDU corresponds to the OP secure channel specification.
- **External Authenticate**. This APDU corresponds to the OP secure channel specification.
- **Verify CHV**. This APDU checks the PIN presented by the Card Holder
- **Put Key**. This APDU is used to set the XAUT key used to unblock the PIN, and must be used with the Key Wrapping Key. The APDU format is compliant with OP specification.
- **Get Challenge**. This APDU is used in combination with AC external Authenticate to perform an external authentication of the Cryptographic Officer in order to unblock the PIN.
- **AC External Authenticate**. This APDU is used in combination with a Get Challenge, this APDU is used to unblock the PIN.
- **Change PIN after First Use**. This APDU indicates that the Card Holder must change his PIN before any PIN protected service can be accessed.

Role / Authentication Method Vs. Services	None	Any Role	Crypto-graphic Officer OP Auth.	Crypto-graphic Officer XAUT	Card Holder PIN
ID Applet					
INSTALL			X		
CHANGE PIN/UNBLOCK			X	X	X
GET PROPERTIES	X	X			
INITIALIZE UPDATE	X	X			
EXTERNAL AUTHENTICATE			X		
VERIFY CHV					X
PUT KEY			X		
GET CHALLENGE	X	X			
AC EXTERNAL AUTHENTICATE				X	
CHANGE PIN AFTER FIRST USE	X	X			

Table 1 - Roles & Possible ACR Configuration for ID Applet Services
Only FIPS-modes are represented in this chart.

4.4.2 PKI Applet Services

The PKI Applet provides RSA-based cryptographic services. There is one RSA private key for each PKI applet instance. The corresponding certificate is located in the attached GC instance. Here are the different APDUs / Services that are provided by a PKI applet instance:

- **Select**: This APDU causes the selection of the applet.
- **Install**: This APDU causes the installation of the applet.
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.
- **Initialize update**. This APDU follows the OP secure channel specification.
- **External Authenticate**. This APDU follows the OP secure channel specification.
- **Generate Key Pair**. This APDU is used to generate a Key Pair in the Smart Card.
- **Get Certificate**. This APDU is used to obtain the certificate corresponding to a Private Key.
- **Sign**. This APDU uses a RSA private key to sign data.
- **PIN Verify**. This APDU checks the PIN presented by the Card Holder against the current PIN.
- **Put Key**. This APDU is used to import/unwrap the Private Key. The APDU format follows OP specification..

Role / Authentication Method Vs. Services	None	Any Role	Crypto-graphic Officer OP Auth	Card Holder PIN	Card Holder PIN ALWAYS	NEVER
PKI Applet						
INSTALL			X			
GET PROPERTIES	X	X				
INITIALIZE UPDATE	X	X				
EXTERNAL AUTHENTICATE			X			
GENERATE KEY PAIR			X	X	X	X
GET CERTIFICATE	X	X		X	X	X
SIGN				X	X	X
PIN VERIFY				X	X	
PUT KEY			X			

Table 2 -Roles & Possible ACR Configuration for PKI Applet Services
Only FIPS-modes are represented in this chart.

4.4.3 GC Applet Services

The Generic Container Applet provides secure storage services. Each GC applet instance corresponds to one storage area.
Here are the different APDUs / Services that are provided by a PKI applet instance:

- **Select**: This APDU causes the selection of the applet..
- **Install**: This APDU causes the installation of the applet. .
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.
- **Initialize update**. This APDU follows the OP secure channel specification.
- **External Authenticate**. This APDU follows the OP secure channel specification.
- **Update Buffer**. This APDU is used to write or modify data elements in storage area.
- **Read Buffer**. This APDU is used to read data elements from storage area.

- **Get Challenge**. This APDU is used in combination with GC external Authenticate to perform an external authentication.
- **Put Key**. This APDU imports/unwraps the XAUT keys. The APDU format follows OP specification..
- **GC External Authenticate**. This APDU communicates the cryptogram obtained by 3DES encryption of a card challenge with the 3DES key associated to the service protected by XAUT.
- **PIN Verify**. This APDU checks the PIN presented by the Card Holder against the current PIN.

Role / Authentication Method Vs. Services	None	Any Role	Crypto-graphic Officer OP Auth.	Card Holder PIN	Card Holder PIN ALWAYS	Application Operator XAUT	A.O. or C.H. XAUT or PIN	A.O. and C.H. XAUT then PIN
GC Applet								
INSTALL			X					
GET PROPERTIES	X	X						
INITIALIZE UPDATE	X	X						
EXTERNAL AUTHENTICATE			X					
UPDATE BUFFER	X	X	X	X	X	X	X	X
READ BUFFER	X	X	X	X	X	X	X	X
GET CHALLENGE	X	X						
PUT KEY			X					
GC EXTERNAL AUTHENTICATE						X		
PIN VERIFY				X	X			

Table 3 - Roles & possible ACR configuration for GC applet services
Only FIPS-modes are represented in this chart.

5 Security Rules

5.1 Applet environment

- The applets must be installed within a FIPS 140-1 certified smart card.
- The applets must be installed on a smart card platform offering Java Card and Open Platform (or Global Platform) services.
- The Card Holder must take the necessary measures to insure that the terminal and/or the Card Acceptance Device are controlled by a valid role: Card Holder, Application Operator or Cryptographic Officer.

5.2 Content Management

- The management of the life cycle of the applets – load, install, delete, personalize keys, shall follow the Open Platform standard.
- Applets management and key management APDU commands (such as download, install, delete, put key) are protected by OP authentication. They have their origin authenticated and their integrity verified. In particular this protects the applet byte code against tampering when downloaded at post issuance.

- The download of applets packages and the installation of applet instances may only occur during the manufacturing process.
- There may be as many instances of each applet as there are available smart card resources.

5.3 Role Authentication

- The applets shall provide the following distinct operator roles: The user role – Application Operator or Card Holder, and Cryptographic officer role.
- The applets shall provide role-based authentication.
- Cryptographic services are restricted to authenticated roles.
- The Role authentication methods (ACRs) for each applet service are set by the Cryptographic officer during Applet instantiation and cannot be modified during the lifetime of the ID applet instance.
- When authentication of the role cannot be performed because the related key or password or key attributes are missing, the corresponding service must be disabled.
- The results of authentication must be set in transient memory and therefore cleared when the module is powered down.
- The Applet instance configuration may require the combined authentication of different roles to access a particular service. For instance the Application Operator and then the Card holder must both authenticate themselves to access the UpdateBuffer service.
- The Card Holder can access services requiring Application Operator authentication after the Application Operator has been authenticated successfully.
- The Application Operator can access services requiring Card Holder authentication by PIN after the Card Holder has been authenticated successfully. This rule is not applicable for services requiring Card Holder authentication with PIN ALWAYS.

5.4 Key management

- RSA private keys and 3DES keys must be transported encrypted to the card.

5.5 PIN management

- The password or PIN that is used by the applet to authenticate the Card Holder must not be divulged to other parties than the Card Holder.
- The ID applet must be configured by the cryptographic officer so that:
  - After M consecutive unsuccessful PIN code validation attempts, the Card Holder services must be disabled. (eg. The PIN is blocked)
  - After N consecutive unsuccessful PIN unblocking attempts using OP authentication with incorrect key or parameters, the card Holder services are permanently disabled (eg. The PIN is locked)
  - The PIN length must always be comprised between 4 to 8 alphanumeric characters

6 Definition of Security Relevant Data Items

6.1 List of SRDIs

The following Security Relevant Data Items (SRDIs) are managed from the applets:

- **Authentication Method (or ACR)**: These data elements define the Authentication Method that is permanently set for the service. The ACRs are set by the Cryptographic Officer upon applet instantiation.
- **External Authentication Keys**: These are 3DES keys that enable the authentication of Application Operators (GC read / GC Write) or Cryptographic Officers (PIN Unblock).
- **RSA private keys**: are managed (generated, unwrapped) from the PKI applet using the java card cryptographic services. These keys are used to sign data.
- **RSA public keys**: Public keys are generated on card from the RSA key pair generation, and exported off card.
- **X.509 Certificates**: The certificates corresponding to the private keys present in the card are managed by the applets.
- **Personal Identification Numbers or passwords (**PIN): PINs and PIN attributes are managed from the ID applet, which relies on the Java Card PIN management service.
- **Open Platform Key Sets:** are managed by the card manager or security domain. These keys enable the authentication of the Cryptographic Officer, and the encryption of inputted keys. They are inputted into the module via the Put Key command.

6.2 Access to SRDIs vs. Services

The following matrices show for each applet how services access SRDIs.

6.2.1 PIN Applet

PIN applet
Columns: Services(roles)
Rows: Access to SRDIs

	Card Holder	**Cryptographic Officer**	INSTALL-instantiate (C.O)	CHANGE PIN/UNBLOCK(C.O)	GET PROPERTIES(any)	INITIALIZE UPDATE(any)	EXTERNAL AUTHENTICATE(C.O)	VERIFY CHV(C.H)	PUT KEY(C.O)	GET CHALLENGE(any)	AC EXTERNAL AUTHENTICATE(C.O)	CHANGE PIN AFTER FIRST USE(any)
Access Control Rules												
Install ACR		X	X									
PIN or Password												
Install PIN		X	X									
Change/Unblock PIN	X	X		X								
Verify PIN	X							X				
External Authentication Keys												
Delete key		X							X			
Import key		X							X			
Verify cryptogram		X		X							X	
Card Manager Key set												
Verify Cryptogram		X		X			X		X			
Decrypt APDU payload		X		X					X			

6.2.2 PKI Applet

PKI applet services Columns: Services(roles) Rows: Access to SRDIs	***Card Holder***	***Cryptographic Officer***	INSTALL instantiate (C.O)	GET PROPERTIES (any)	INITIALIZE UPDATE(any)	EXTERNAL AUTHENTICATE(C.O)	GENERATE KEY PAIR (C.O or CH)	GET CERTIFICATE(any)	SIGN(C.H)	PIN VERIFY(C.H)	PUT KEY(C.O)	
Access Control Rules												
Install ACR		X	X									
PIN or Password												
Verify PIN	X									X		
RSA Key Pair												
Generate Key Pair	X	X					X					
Import CRT components		X									X	
Delete private key		X									X	
Sign data	X								X			
Card Manager Key set												
Verify Cryptogram		X									X	
Decrypt Data		X				X					X	

6.2.3 GC Applet

GC applet services Columns: Services(roles) Rows: Access to SRDIs	**Card Holder**	**Cryptographic Officer**	**Application Operator**	INSTALL (Instantiate)	GET PROPERTIES (any)	INITIALIZE UPDATE (any)	EXTERNAL AUTHENTICATE (C.O)	UPDATE BUFFER (C.0 or A.O or C.H)	READ BUFFER (C.0 or A.O or C.H)	GET CHALLENGE (any)	PUT KEY (C.O)	GC EXTERNAL AUTHENT(A.0)	PIN VERIFY (C.H)
Access Control Rules													
Install ACR		X		X									
PIN or Password													
Verify PIN	X												X
External Authentication Keys													
Delete key		X									X		
Import key		X									X		
Verify cryptogram			X									X	
Card Manager Key set													
Verify Cryptogram		X						X	X		X		
Decrypt Data		X					X	X	X		X		

7 References

Global Platform - Open Platform – Card Specification v2.0.1 – 7 April 2000.