Security Policy

For

Axalto Cryptoflex 32K e-Gate Smart Card

Public Version 1.2

Table of Contents

1 Scope of Document

This document defines the Security Policy for the Cryptoflex 32K e-Gate smart card. Included is a description of the basic security requirements for the Cryptoflex 32K e-Gate card and a qualitative description of how each security requirement is achieved.

2 Introduction

The Cryptoflex 32K e-Gate smart card is an ISO/IEC 7816 and USB Specification v1.1 compliant smart card which supports a command set aimed at allowing the mutual authentication of identities with "card acceptance devices" (and PCs or other terminals that they might be connected to) using strong cryptography. Specifically, the DES/TDES algorithm is used within authentication commands used between the card and the card acceptance device environment to authenticate identities. Establishment of identities using these commands is then used to fulfill "access conditions" which limit the ability of the external world to access information and/or commands on the card.
The Cryptoflex 32K e-Gate smart card is capable of supporting both the ISO/IEC 7816 and the USB specifications communication protocols. In other words, the Cryptoflex 32K e-Gate can also "speak" directly to a USB port. No matter which link level electrical connection is used, application layers still communicate via APDUs.

3 Security Level

The Cryptoflex 32K e-Gate 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	2
Software Security	2
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	3
Self Test	2

3.1 Cryptographic Module Specification

Cryptoflex 32K e-Gate is a single chip implementation of a cryptographic module.

Cryptoflex 32K e-Gate is an ID-1 class card which adheres to the various ISO/IEC specifications for Integrated Circuit based identification cards (ICC). The “cryptographic boundary” for the Cryptoflex 32K e-Gate card vis-à-vis the FIPS140-1 certification is the “module edge”. The module is comprised of the chip, the contact faceplate, and the micro-electronic connectors between the chip and the contact pad. The physical security of the module is constructed so as to meet the requirements of the FIPS 140-1 level 2 certification.

The Cryptoflex 32K e-Gate chip is comprised of the following elements:

STMicroelectronics ST19XT34 8 bit microcontroller
Systems software and cryptographic software installed in ROM as part of the chip manufacturing process. This is the hard mask (HM) designated by a version number This hard mask identification number can be retrieved from the card using a standard command.
Power-up self-test software installed in EEPROM as part of the card manufacturing operation, Softmask (SM) designated by a version number,
Key and PIN storage in EEPROM as part of the card personalization operation.

Two configurations are FIPS validated:

1. HM 01v01, SM 05v01
2. HM 01v03, SM 05v02

3.2 Module Interfaces

The electrical and physical interfaces to the Cryptoflex 32K e-Gate chip, as a cryptographic module, are comprised of the 8-electrical contacts from the face of the module to the chip. These contacts conform to the following specifications:

3.2.1 PHYSICAL INTERFACE DESCRIPTION

The Cryptoflex 32K e-Gate module supports eight contacts which lead to pins on the chip. Only five of these are used for ISO mode, and four for USB mode, both modes include the same two Vcc and Ground contacts. The position of these contacts comply with ISO/IEC 7816-2.

Minimum contact surface area: 1.7mm * 2.0 mm

Contact dimensions are those of a standard credit card compliant with ISO/IEC 7816-1:

Dimension	Value
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

3.2.2 ELECTRICAL SPECIFICATIONS

Specific electrical functions of the contacts:

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

ICC supply current:

- MAX: 50 mA at 5MHz
- TYP: 5 mA at 5MHz

Module structure and ICC electrical contacts defined by ISO/IEC 7816-1&2.
Electrical signaling between the "card acceptance device" (CAD) and the module defined by ISO/IEC 7816-3 and by USB Specification V1.1.
Module security and key access command set defined by ISO/IEC 7816-4.
CAD to module communication protocols defined by ISO/IEC 7816-3 & 4.

3.2.3 LOGICAL INTERFACE DESCRIPTION

Once electrical (physical) contact and data link layer contact is established between the module and the CAD, the module functions as a "slave" processor to implement and respond to the CAD's "master" commands. The module has a well defined command set to which it responds. Access to specific commands is limited by the establishment of Access Conditions based on knowledge of PINs or keys stored in the module.

3.2.4 ROLES & SERVICES

Two roles control the Cryptoflex 32K e-Gate module throughout its lifetime: the Cryptographic Officer and the User. The general capabilities of these roles are as follows:

Cryptographic officer:

- is established in control of the card during the manufacturing process
- controls definition of module file structure
- defines default PIN
- defines PIN-reset PIN
- controls key loading
- controls card issuance to User

User:

- is established in control of the card by the Cryptographic Officer
- controls user PIN
- uses the keys (perform cryptographic operations) on the card

The Cryptographic Officer is identified through possession of the Master Transport Key (MTK) for the Cryptoflex 32K e-Gate module. This key is required to enable creation of the file system. The access conditions limiting the file creation activity are established as part of the manufacturing process, as is the definition of the MTK.

The User is identified through possession of the Application Access Key (AAK). This key is a PIN code which is established by the Cryptographic Officer during the personalization of the module prior to issuing the card to the User's possession. With knowledge of the AAK, a new AAK can be defined by the User.

3.2.5 FINITE STATE MACHINE

The Cryptoflex 32K e-Gate module is compliant with the ISO/IEC 7816-4 specifications. Either in ISO mode or in USB mode, this means that the card communicates via Application Protocol Data Unit packets transferred from the CAD to the module, followed by a response APDU from the module back to the CAD. Within this protocol, the module functions as a pure, finite state machine.

The Finite State Model for the Cryptoflex 32K e-Gate card is published as a separate document.

3.2.6 PHYSICAL SECURITY

The physical security of the Cryptoflex 32K e-Gate module is designed to meet FIPS 140-1 level 2 requirements.
If the module is attacked through physical means, the attack will be evident due to the disturbance of the packaging of the module. The ICC is embedded within an epoxy coating which is difficult to penetrate without leaving evidence of the attack. Further, the packaging itself is resistant to penetration.

3.2.7 SOFTWARE SECURITY

The system software for the Cryptoflex 32K e-Gate module is a hard mask; that is, the system software is stored in ROM during the manufacturing process for the ICC which is inserted into the card. Once manufactured, it is impossible to alter the ROM code.

In order to achieve FIPS compliance for certain commands, a FIPS approved pseudo-random number generation function and power-up self-tests for the cryptographic operations have been added to the system software in softmask.

Software security of the Cryptoflex 32K e-Gate module is strictly controlled by:

- Master Transport Key protection for the creation of the on card file systems and specific Crypto-officer commands,
- PIN access control for files and specific user commands

3.2.8 OPERATING SYSTEM SECURITY

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

3.2.9 KEY MANAGEMENT

Secret or private keys to be used with the DES, TDES, and RSA signature algorithms are generated either on-card or off-card as part of the card personalization operation. If generated off-card, these keys are encrypted and then loaded onto the card during personalization.
A FIPS approved key generation command is available on card (ANSI X9.17 PRNG method).
All of the key information is stored in special files (i.e. files with well defined names) associated with the on-card file system. These keys are then used to establish identities which are used to fulfill access conditions placed on various commands which the card can execute.
Key management is largely rooted in the establishment of the root of the file system during card manufacture. A Master Transport Key is installed in an elementary file within the Master File (root) file of the card's file system. All commands are then given an access condition (by the CREATE FILE command used to create the MTK file) that requires knowledge of the MTK before any command on the card can be executed. The MTK is known only to the Cryptographic Officer who controls the card after it leaves the manufacturing facility. All other files, including key files, which are stored on the card require an action by the Cryptographic Officer who may, in the course of establishing a more complex file structure on the card, allocate privileges to the User role. Thus, all key management derives from knowledge of the MTK.

All secret and private keys can be zeroized by loading a null value for each key..

3.2.10 CRYPTOGRAPHIC ALGORITHMS

The purpose of the Cryptoflex 32K e-Gate card is to provide a portable token for use in storing a variety of keys and for providing a secure computing platform to enhance cryptographic services. The keys represent the identity of the roles involved in controlling the card: first, the identity of the Cryptographic Officer and then of the User. The FIPS validated DES and TDES algorithms are used in the Cryptoflex 32K e-Gate card to provide identity authentication services. The FIPS validated SHA-1 algorithm is used to hash data as requested. RSA PKCS1 is used in the Cryptoflex 32K e-Gate to provide signature services.

Random number generation is done on the card for the purpose of generating random challenges (nonces) to be used in the authentication of identity and for use in generating RSA public/private key-pairs and DES/TDES secret keys.
A X9.17 PRNG exists on the card to generate FIPS approved RSA key pairs and DES/TDES secret keys.

3.2.11 EMI/EMC

The Cryptoflex 32K e-Gate module has been tested to meet the EMI/EMC requirements specified by FCC Part 15, Subpart J, Class B.

3.2.12 SELF-TESTS

The Cryptoflex 32K e-Gate module performs the required set of self-tests at power-up time and reset, both in ISO and USB mode. When the Cryptoflex 32K e-Gate 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 module. A series of GO/NO-GO tests are then performed by the card before it responds (as specified by ISO/IEC 7816) with an Answer To Reset (ATR) packet of information. These tests include:

EEPROM soft-mask CRC test
Algorithm (known answer) tests for:

- DES ECB encryption & decryption
- TDES ECB encryption & decryption
- RSA (PKCS 1) Signature
- SHA-1 Hashing

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.

Conditional tests:

- A continuous test is performed on the ANSI X9.17 PRNG after each random number generation.

- A pair-wise consistency test is performed during RSA key pair generation.

If any of these tests fail, an error status is output and the current cryptographic operation is halted and the card goes to the idle state waiting for another command.

4 Roles and Services

The Cryptoflex 32K e-Gate module defines two distinct roles that are supported by the on-card cryptographic system: the Cryptographic Officer and the Cardholder (User). The Cryptographic Officer is established in control of the card during the manufacturing process and this role is authenticated to the card by knowledge of a key set, generally referred to as the Master Transport Key (MTK). The Cardholder (User) role is authenticated by knowledge of a PIN.

Cryptoflex 32K e-Gate cards that are to be deployed are prepared in a batch operation called pre-personalization. This operation specifically includes installing the basic file structure on the card and establishing the access conditions for this file structure. Establishing the file structure first requires creating a Master File on the card. System software establishes the access condition that knowledge of the MTK is required to create the Master File; hence, this is an operation which can only be performed by the Cryptographic Officer.

The basic file system typically has specific files allocated for holding keys. These files are created with associated files which contain PIN codes. During pre-personalization, a generic PIN code is created on the card. At this time, there are no application keys present on the card and card security is still maintained by physical possession of the card by the Cryptographic Officer and knowledge of the MTK.

During the personalization operation in which each card is personalized for an individual cardholder, keys are generated in the off-card environment and loaded , encrypted form, onto the card (into the pre-existing key files) under control of the Cryptographic Officer.

When the Cryptographic Officer installs the file structure on the card and establishes the generic PIN, a “CryptoOfficer Unblock PIN” may also be established. Knowledge of this PIN is retained by the Cryptographic Officer. If a blocked card is presented to the Cryptographic Officer, it may be “rehabilitated” through knowledge of the “CryptoOfficer Unblock PIN”.

The Cryptoflex 32K e-Gate module insures the authentication of off-card entities and provides them with cryptographic services according to their role and as such is a role-based authentication module..

4.1 Services

Role/Authentication Method vs Services	**SERVICE DESCRIPTION**	Unauthenticated Role	Cryptographic Officer	Cardholder PIN	FIPS mode
CHANGE_CHV	Change PIN on card		X	X	X
DECREASE	Decrease a value in a file record.		X	X	X
GET AC KEYS INDEX	Retrieve a specific access control key index from card			X	X
GET RESPONSE	Retrieve additional information from a command	X			X
INCREASE	Increase a value in a file record.		X	X	X
INVALIDATE	Set state of a file to INVALID; blocks access to file for most commands		X	X	X
LOGOUT AC	Cancel current access control status	X			X
REHABILITATE	Reset status of INVALID file so it can be accessed.		X	X	X
UNBLOCK CHV	Reset the invalid attempts counter for a PIN file		X		X
VERIFY CHV	Prove knowledge of a specific PIN			X	X
VERIFY KEY					NON FIPS
EXTERNAL AUTHENTICATE	Authenticate the identity of the CO		X		X
GET CHALLENGE	Get a nonce to use for subsequent identity authentication command	X			X
INTERNAL AUTHENTICATE	Authenticate the card to the User			X	X
RSA SIGNATURE	Perform RSA sign			X	NON FIPS
RSA SIGNATURE inter	Performs RSA intermediate signature			X	NON FIPS
RSA SIGNATURE last	Performs RSA signature last			X	NON FIPS
SHA-1 INTERMEDIATE	Perform hash for a portion of a byte string	X			X
SHA-1 LAST	Perform final hash operation for a byte string	X			X
CREATE FILE	Create a new file on the card		X		X
CREATE RECORD	Create a new record within a file on the card		X		X
DELETE FILE	Delete a file from the card		X		X
DIR NEXT	Get a directory of the files on a card		X		X
READ BINARY	Read a byte string from a file on the card		X	X	X
READ RECORD	Read a record from a file on the card		X	X	X

SEEK	Look for specific contents in a file		X	X	X
SELECT	Point at a new file	X			X
UPDATE BINARY	Write a byte string into a file		X	X	X
UPDATE RECORD	Write a record into a file		X	X	X
MASK TRACK	Gives version number of the card	X			X
RSA SIGN PKCS1	Performs a RSA PKCS1 signature, in FIPS mode			X	X
RSA KEY GEN	Performs RSA key generation, in FIPS mode			X	X
READ BIN ENC	Output data in encrypted format		X	X	X
DES BLOCK	Executes DES operation			X	NON FIPS
DES BLOCK INIT	Executes DES operation			X	NON FIPS
GENERATE DES KEY	Generates DES secret keys			X	X
UPDATE BIN ENCIPHERED	Load an encrypted key into the card		X	X	X

5 Security Rules

The Cryptoflex 32K e-Gate module implements the security commands which are generically defined in the ISO/IEC 7816-4 specification and which are defined in detail in the Cryptoflex 32K e-Gate Technical Specification. The gist of this security architecture is defined in terms of a file structure implemented on the module.

The file structure is rooted in a Master File which is a “dedicated” or “directory” file; that is, it may contain other dedicated files or elementary files (leaf nodes in the file structure tree). Every dedicated file can have a set of specially named elementary files associated with it (contained by it). These special files can contain a variety of keys. Special commands are used to store values in these key files and other special commands are used to allow an off-card entity to confirm, to the card OS, that it (the off-card entity) knows the key values stored on the card. By doing this, the off-card entity can establish an identity known to the card. This identity (i.e. knowledge of the keys) can then be impressed on other commands as a necessary condition for the command to be executed.

The security infrastructure is established at the time that the Master Files is first created on the card. This is done during the manufacturing process while the card still resides in a secure environment. When the Master File is created, the very same command (which creates the Master File) also creates a key file within the Master File and stores the Master Transport Key (MTK) value in this file. Knowledge of this MTK is then established as a required condition on all commands which can further access or manipulate the file

structure. Thus, once the MTK is established, knowledge of it establishes the role of the Cryptographic Officer; and, only the Cryptographic Officer can access the initial files on the card or can create an additional file structure on the card. All keys inputted to the card are wrapped with the MTK. The Cryptographic officer shall configure the access conditions to never allow the output and the loading of secret or private keys in the clear.

To establish the card file structure, knowledge of the MTK is required.

The key values are entered into the key files using the UPDATE BINARY ENC command. Access to secret or public/private key pairs is restricted to the use of UPDATE BINARY ENC command with this command; the key is encrypted as it crosses the wire from the terminal to the card.

Access Conditions are established with respect to a file or a section of a file structure. The current Access Conditions are stored in RAM. Thus, if power is removed from the card, the RAM is erased and all existing Access Conditions are lost. This prevents the establishment of Access Conditions from surviving across a power-down of the card.

6 Definition of Security Relevant Data Items

The Cryptoflex 32K e-Gate smart card Security Relevant Data Items (SRDIs) are the following:

Personal Identification Numbers (PINs)

- Cardholder PIN,
- Crypto officer Unblock PIN

Authentication Keys (DES/TDES):

- MTK
- Internal authentication keys
- Data encryption/decryption keys

RSA key pairs

Each of these SRDIs has a specific purpose within the smart card and within the environment of a smart card inserted into a system encompassing a card acceptance device (aka smart card reader or terminal):

PINs are comprised of a string of 8 numbers which can be attached to files or to file structures on a smart card. By proving knowledge of a particular PIN through a VERIFY CHV command, the CHV access condition is satisfied. Once this condition is satisfied, then commands which have had their access limited by a CHV access condition can be invoked. CHV stands for cardholder verification, and the CHV access condition is usually used to limit access to specific commands only to the bearer of the card. To preserve the overall security of a system, the PIN should be entered through a keypad which is connected to the card in a secure manner; i.e. such that the PIN characters can not be intercepted.

Authentication Keys are keys for encryption algorithms which can be related to files or file structures. Through this relationship, access to the files or file structures (actually to the commands through which the files or file structures are accessed and manipulated) can be limited by requiring knowledge of the keys. This limit is established by placing an access condition on a command which says in effect, if you want to execute this command relative to this file, then you must have already proven that you know this key which applies to this file. For the Cryptoflex 32K e-Gate card, the FIPS approved mode of operations allows DES and TDES algorithms to be used in authenticating knowledge of an Authentication Key.

Authentication Keys and PINs are attached to files or file structures by placing them in specially named files within directories. If one then wants to access a file, it is possible to search up the file tree for the first occurrence of a directory file which contains either (or both) of these special files which contain Authentication Keys or PINs. There are seven of these special files which may be found within a directory (i.e. a Dedicated File):

6.1 Definition of SRDI Modes of Access

The PIN and Authentication Key values are stored in Elementary Files on the Cryptoflex 32K e-Gate smart card. The values are introduced into the files and manipulated once there by using a set of file access commands:

SELECT
UPDATE BIN
UPDATE BIN ENC
DIR NEXT
GET RESPONSE

The PIN and Authentication Key files are initially created with a CREATE FILE command. With this command, the access conditions on the key files can be specified by the same command that creates the file (i.e. the CREATE FILE command). Separate access conditions can be placed on all of the commands noted above. For the PIN and Authentication Key files, typically the only commands which will be allowed are SELECT and UPDATE BIN ENC.

The PIN and Authentication Key SRDIs are actually used by the following commands:

VERIFY CHV
CHANGE CHV
UNBLOCK CHV
GET CHALLENGE
INTERNAL AUTH
EXTERNAL AUTH

Of these, the two cryptographic services are provided by the INTERNAL AUTH and the EXTERNAL AUTH commands. DES and TDES algorithms can be used within these commands to authenticate identities.

6.2 Service to SRDI Access Operation Relationship

The following services are provided to the User and the Cryptographic Officer roles. These various services make use of the indicated access mechanisms on the SRDIs..Service	UPDATEBIN ENC	UPDATE BIN	VERIFY CHV	CHANGE CHV	UNBLOCK CHV	GET CHALLENGE	INTERNAL AUTH	EXTERNAL AUTH	User Role	Cryptographic Officer Role
Load MTK	X									X
Load User Key	X									X
Load User PIN	X	X								X
Modify User PIN				X					X	X
Unblock USER PIN					X					X
Modify User Key	X								X	
Verify User PIN			X						X	
Verify Crypto Officer MTK						X		X		X
Internal Authentication Key							X		X	

The keys through which identities are established are accessed through the indicated commands in the above table. The CHANGE CHV command is used to change the value of the PIN used to authenticate the cardholder to the card. The UPDATE BIN ENC command is used to establish the value of the keys accessed by the INTERNAL AUTH and the EXTERNAL AUTH commands. The UPDATE BIN ENC command is used to "zeroize" the key file.