2900-1 (DDCEI 3-5-4)

27 August, 1999

SMART CARD AND SMART CARD READER SPECIFICATIONS

FOR THE GOVERNMENT OF CANADA ENTRUST TOKEN

Prepared by: CR Clupp
Captain
DDCEI 3-5-4
996-6203

1. General

The Government of Canada (GOC) has chosen the Entrust family of encryption products to provide identification/authentication, confidentiality and digital signature (non-repudiation) services for the Information Technology Infrastructure (ITI). GOC has a requirement for a high assurance, processing and storage device which will enable users to carry their identity with them (i.e. portability) for use within the GOC ITI as one component of the Security Architecture. Integrated Circuit Cards/Smart Cards (ICC) and smart card readers/interface devices (IFD) will be used to provide a high level of assurance for the protection of departmental users' Entrust credentials, private signature and decryption keys and encryption/decryption processes. The ICC will protect the users' Entrust credentials from tampering, forgery and unauthorized use. The private signature encryption key will be generated on, stored on and only used on the token (i.e. private signing key will **never** leave the token). The private key decryption key will be stored on the token and all private key decryption operations will be performed on the token. The following high level specifications will outline the mandatory characteristics and standards that the smart card and smart card reader must adhere to in order to fulfill the GOC requirement.

2. Applicable Standards and Specifications

All referenced standards and specifications refer to the most recent version of the document as of Friday, August 27, 1999.

2.1. ISO/IEC 7810: Identification Cards – Physical Characteristics

2.2. ISO/IEC 7811: Identification Cards – Recording Technique

2.2.1 ISO/IEC 7811-1 Part 1: Embossing

2.2.2 ISO/IEC 7811-1 Part 2: Magnetic Stripe

2.2.3 ISO/IEC 7811-1 Part 3: Location of embossed characters on ID-1 cards

2.2.4 ISO/IEC 7811-1 Part 4: Location of read-only magnetic track –Track 1 and 2

2.2.5 ISO/IEC 7811-1 Part 5: Location of read-write magnetic track –Track 3

2.2.6 ISO/IEC 7811-1 Part 6: Magnetic Stripe – High Coercivity

2.3. ISO/IEC 7812: Numbering system and registration procedure for issuer identifiers

2.4. ISO/IEC 7813: Identification Cards – Financial Transaction cards

2.5. ISO/IEC 10373: Identification Cards – Test Methods

2.6. ISO/IEC 7816: Identification Cards – Integrated Circuit Cards with Contacts

2.6.1 ISO/IEC 7816-1: Physical characteristics

2.6.2 ISO/IEC 7816-2: Dimensions and locations of the contacts

2.6.3 ISO/IEC 7816-3: Electronic signals and transmission protocols

2.6.4 ISO/IEC 7816-4: Interindustry commands for interchange

2.6.5 ISO/IEC 7816-5: Numbering system and registration procedure for application identifiers

2.6.6 ISO/IEC 7816-6: Interindustry data elements

2.7. National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Series of Standards

2.7.1 FIPS140-1: Security Requirements for Cryptographic Modules

2.7.2 FIPS 186: Digital Signature Standard (DSS)

2.8. Public-key Cryptography Standard (PKCS)

2.8.1 PKCS#1: RSA Encryption Standard (version 1.5)

2.8.2 PKCS#11: Cryptographic Token Interface Standard (version 1.0)

2.9. Personal Computer Smart Card (PC/SC) Specification

3. Smart Card (ICC) Specifications

3.1 Physical Characteristics:

The physical characteristics of the ICC shall be ISO/IEC 7816-1 compliant and meet the requirements of ISO/IEC 7810, ISO/IEC 7811 parts 1 to 5, ISO/IEC 7812 and ISO/IEC 7813.

3.1.1 ICC shall be tested in accordance with ISO/IEC 10373 for:

a. Bending properties; and

b. Torsion properties

3.1.2 The ICC test methods described in the Annex to ISO/IEC 7816-1 shall be utilized and adhered to as applicable

3.2 Dimension and Contact Position:

The dimension and position of the contacts shall comply with Figure 2 of ISO/IEC 7816-2

3.2.1 Contacts shall be located on the front face of the card (i.e. the face opposite from the magnetic stripe) as shown in Annex A of ISO/IEC 7816-2 and in accordance with the criteria specified in ISO/IEC 7811-1 and 7811-2

3.2.2 Isolation of contacts shall be in accordance with Annex B of ISO/IEC 7816-2

3.3 Electrical Signals and Transmission Protocols:

Electrical signals and transmission protocols shall conform to the ISO/IEC 7816-3 standard.

3.3.1 The ICC will be used in multiple IFDs from various vendors:

a. The ICC shall be designed in such a way as to ensure that insertion of a class A or class B ICC into a class A, class B or class AB IFD will not cause damage to the ICC or the IFD (eg. if a class B ICC (3v supply voltage) is inserted in a class A IFD (5v VCC) no damage shall occur to the ICC or IFD)

3.3.2 The ICC shall support either the “T=0” or “T=1” asynchronous half-duplex protocol types. The “T=14” protocol shall not be used

3.4 Interindustry Commands for Interchange:

The ICC file structure, command sets and security architecture shall be ISO/IEC 7816-4 compliant and shall not provide open access to commands which would circumvent the Entrust security controls

3.5 Cryptographic processors and algorithms:

3.5.1 The set of asymmetric cryptographic algorithms implemented on the ICC must include the following algorithms used by GOC and supported by Entrust:

a. RSA – in accordance with PKCS#1 [with at least a 1024 bit key length]; and

b. DSA – in accordance with FIPS 186 [with at least a 1024 bit key length].

3.5.2 All cryptographic modules must be designed to meet FIPS 140-1 level 2 criteria for physical characteristics:

a. Physical security mechanisms shall be designed such that unauthorized attempts at access, use or modification will have a high probability of being detected subsequent to the attempt by visible signs (i.e. tamper evident)

b. The chip shall be of production-grade quality, which shall include standard passivation techniques (i.e. a sealing coat applied over the chip circuitry to protect it against environmental or other physical damage)

c. The chip shall be covered with an opaque tamper evident coating (e.g. an opaque tamper evident passivation material, or an opaque tamper evident material covering the passivation)

d. Documentation shall be provided which includes a complete specification of the physical embodiment and security level for which the physical security mechanisms of the cryptographic module are designed, as well as a complete description of the applicable physical security mechanisms that are employed by the module

3.5.3 Application programming interfaces that provide cryptographic services must adhere to the Entrust implementation of the PKCS#11 standards

3.5.4 The ICC Vendor shall prove compatibility with Entrust Technologies family of encryption products for the following functions:

a. Signature key pair shall be generated on the ICC during the normal Entrust Entity initialization process;

b. The ICC shall store user credentials to permit portability, including but not limited to the following:

(i) private signature key;

(ii) private key decryption key;

(iii) CA public signature verification certificate

(iv) public signature verification certificate; and

(v) key history.

c. The Entrust userid and password shall be used for identification and authentication (I&A)

d. The ICC shall perform operations on the message hash using the Entrust private signature key

3.5.5 The ICC shall perform signature of hash on the token in less than 3 seconds. The 3 seconds shall be based on I/O times, key retrieval and the actual signature operation.

3.5.6 The private signing key shall never leave the token.

3.5.7 The ICC shall employ a random number generator in accordance with FIPS 186, Appendix 3.

3.5.8 Symmetric cryptographic algorithms employed on the ICC for the purpose of protecting passwords/PIN numbers, the Entrust credentials or other sensitive information shall be at minimum 168 bit 3DES or 128 bit CAST. All other algorithms are subject to GOC approval.

3.6 ICC Architecture

The ICC shall be designed to meet or exceed the following architectural requirements:

3.6.1 ICC shall have at least 8 Kbytes capacity to store the Entrust credentials including private keys for encryption/decryption and other user information

3.6.2 RAM capacity shall be at least 240 bytes

3.6.3 ROM capacity shall be at least 13K bytes

3.6.4 ICC shall have at least an 8 bit CPU

3.6.5 Internal clock frequency of ICC shall be at least 3Mhz

3.6.6 Number of write/erase cycles on persistent memory must be at least 100,000

3.7 ICC Logical Security Measures

ICCs shall have logical security measures implemented in the micro-controller OS to assure data integrity, authentication and confidentiality. The following features shall be implemented:

3.7.1 Transport codes to protect the cards during transportation from the manufacturer to the card issuer. These codes shall be used to prevent information from being loaded onto the card without the issuer knowing about it. The method implemented for the distribution of these codes from manufacturer to issuer shall be approved by GOC

3.7.2 ICCs shall utilize a numbering system and registration procedure for issuer identifiers in accordance with ISO/IEC 7812

3.7.3 User definable private or secret zones that can only be accessed by the card's OS with the correct permissions to protect confidential information such as PINs or private cryptographic keys from external access shall be provided. Access to these areas shall be configurable by the issuer using GOC specific access control mechanisms

3.7.4 Write protected files to prevent the altering of stored information without the OS having the correct permissions to do so (i.e. Entrust credentials)

3.7.5 On-chip processing shall be used to perform the following operations:

a) generate signature key;

b) perform digital signatures;

c) verify and authenticate external messages;

d) encrypt stored passwords; and

e) encrypt other on-chip stored data

3.8 ICC Physical Security Measures

ICCs shall have physical security mechanisms in accordance with FIPS 140-1 level 2 in order to protect the micro-controller from tampering.

4. Smart Card Reader/Interface Device (IFD) Specifications

4.1 Interoperability Specification for ICCs and Personal Computer Systems (PC/SC Specifications)

The IFD shall be compliant with all mandatory PC/SC Specifications and shall incorporate the mechanisms outlined in paragraphs 4.2 and 4.3. Detailed documentation attesting to this compliance shall be provided.

4.2 Physical Interface Requirements

4.2.1 The IFD shall utilize manual card insertion and removal mechanisms.

4.2.2 The ICC shall be positioned in the IFD such that it is always accessible to the card owner.

4.2.3 The IFD shall incorporate a “landing card” or “landing contact” socket design as opposed to a “wiping contact” socket design.

4.2.4 The IFD must be designed to insure that any location guides, clamps, rollers and other mechanisms will not damage the ICC, particularly in areas reserved for the optional magnetic stripe and embossing areas.

4.2.5 The IFD shall incorporate a microswitch as opposed to a blade switch for detection of card presence.

4.2.6 The IFD shall internally support both the T=0 and T=1 Character Protocols as defined in ISO/IEC 7816-3.

4.2.7 The IFD shall observe the following “rules for error free operation” as defined in Para. 4.9.2.2 of Part 2 of the PC/SC Specification:

a. After ATR is complete, the first block transmitted shall be sent by the IFD and may be either an S-block or an I-block.

b. Whenever transmission of a block is complete, the sender shall switch to the receiving state and await a block from the other devices.

After a receiver has read a complete block, per the LEN field, it has the right to send.

c. If node addressing is being used, the node value will be included in the first block sent by the IFD. These values will be used for all subsequent exchanges related to this logical session between the Service Provider and the ICC.

d. If the IFD wishes to change the IFSD from the initial value of 32, it will send an S(IFS request) block. It is recommended this be set to 254 and that this be the first block sent by the IFD to the ICC. The IFD may perform this action independently, but should wait until a Service Provider has initiated a logical session so that the node addressing mode may be properly set.

e. The receiver must acknowledge all I-blocks by sending an appropriate I-block or R-block. R-blocks are used when chaining is in effect.

f. S-blocks are always exchanged in pairs, with an S(request) followed by an S(response).

4.2.8 All readers shall be compatible at the interface between the IFD Handler and the ICC Resource Manager.

4.2.9 IFD proposals shall include all required software in order for the reader to interface with the PC and the ICC. GOC shall not have to acquire additional software in order to properly implement the IFDs

4.3 Functionality Requirements

4.3.1 The IFD shall provide support for protocol selection and the setting of any associated parameters for the purpose of obtaining maximum performance during use of the intended application. The IFD must parse the ATR (answer-to-reset transmission sent by the ICC to the IFD immediately following a reset operation) in accordance with ISO/IEC 7816-3 to determine which options provided by the ICC are also supported by the IFD. The IFD shall wait until the first application connects to the device before it negotiates the protocol settings.

4.3.2 To minimize power consumption when the ICC is expected to be inserted for long periods of time, but used infrequently, the IFD shall support the ability to activate and deactivate an inserted ICC under the control of an ICC Service Provider. A request to activate an ICC shall result in activation of the ICC contacts, generation of a cold reset, and processing of the ATR sequence.

4.3.3 The IFD shall obtain all required power from the existing PC connection. An external power supply shall not be required.

4.4 Form Factor

A variety of form factors shall be available, including but not limited to the following:

4.4.1 PS/2

4.4.2 RS 232

4.4.3 PC Card

4.5 Microsoft OS Compatibility

All proposed IFDs shall have passed the Microsoft Windows Hardware Quality Labs (WHQL) testing program, be in receipt of an official Test Report and the following licenses from Microsoft:

4.5.1 “Designed for Microsoft Windows 95” logo

4.5.2 “Designed for Microsoft Windows NT” logo

4.6 Unix Platform support

The Entrust Smart Card token will be required within the Unix environment to meet the requirements of GOC users in the classified security domain. To meet this requirement it is necessary to have IFDs that can interface to the following Unix operating systems:

4.6.1 Sun Solaris

4.6.2 HP/UX