Sm@rtCafé Expert 3.2 by Giesecke & Devrient with ActivIdentity Digital Identity Applet Suite V2 for Extended PIV

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Version 1.2
November 2009

Table of Contents

1. INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for Sm@rtCafé Expert 3.2 by Giesecke & Devrient with ActivIdentity Digital Identity Applet Suite V2 for Extended PIV. This security policy describes how the cryptographic module: G&D Sm@rtCafé Expert 3.2 smart Card and ActivIdentity (AI) JavaCard applet framework meets the security requirements of FIPS 140-2 **[FIPS140-2]** and how to run the module in a secure FIPS 140-2 approved mode. This policy is prepared as part of the Level 2 FIPS 140-2 validation.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 References

This document deals with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy and has been written in parts describing GlobalPlatform functionality.

More information is available specifically on the Smart Card Sm@rtCafé Expert 3.2 from the following sources:

- Overview information of Giesecke & Devrient products and services can be found at: www.gdai.com
- For answers to technical or sales related questions, please refer to the contacts listed on the Giesecke & Devrient website at www.gdai.com
- More information on ActivIdentity products and services can be found at www.Actividentity.com

[GPCS]	GlobalPlatform Card Specification, v2.1.1, March 2003
[ISO]	ISO/IEC 7816-3 : Second edition 1997-09-18, Identification cards - Integrated circuit(s) cards with contacts - Part 3 : Electronic signals and transmission protocols, ISO/IEC FCD 7816-4: 2003 (Draft) Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange, Working draft dated 2003-01-17, ISO SC17 Document 17N2268T, ISO/IEC 7816-5 : 1994, Identification cards - Integrated circuit(s) cards with contacts - Part 5 : Numbering system and registration procedure for application identifiers, ISO/IEC FCD 7816-6 : 2003 (Draft), Identification cards - Integrated circuit(s) cards with contacts - Part 6 : Interindustry data elements for interchange – FCD dated 2003-01-17, ISO SC17 Document 17N2270T, ISO/IEC FCD 7816-8: 2003 (Draft), Integrated circuit(s) cards with contacts, Part 8: Interindustry commands for a cryptographic toolbox. FCD dated 2003-01-17, ISO SC17

	Document 17N2272T, ISO/IEC FCD 7816-9: 2003 (Draft), Integrated circuit(s) cards with contacts, Part 9: Interindustry commands for card and file management. FCD dated 2003- 01-17, SC17 Document 17N2274T.
[JCS]	Java Card ™ 2.2.1, Card Specification, October 2003, Sun Microsystems
[X9.31]	American Bankers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, Washington, D.C., 1998.
[FIPS140-2]	National Institute of Standards and Technology, FIPS 140 -2 Standard, 2002
[DES]	National Institute of Standards and Technology, Data Encryption Standard, Federal Information Processing Standards Publication 46-3, October 25, 1999.

Table 1 References

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine Model
- Sm@rtCafé Expert 3.2 Reference Manuals
- ActivIdentity Digital Identity Applet Suite V2 for Extended PIV (specifically (v2.6.2B) Card Edge Specifications
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation are produced separately by Giesecke & Devrient and ActivIdentity. With the exception of this non-proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is proprietary to Giesecke & Devrient as well as ActivIdentity and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Giesecke & Devrient or ActivIdentity.

2. CRYPTOGRAPHIC MODULE SPECIFICATION

The cryptographic module comprises the G&D Sm@rtCafé Expert 3.2 smartcard loaded with the ActivIdentity Digital Identity Applet Suite V2 for Extended PIV (namely applet v2.6.2B for the submitted package).

2.1 Sm@rtCafé Expert

2.1.1 Overview

Sm@rtCafé Expert 3.2 (Hardware version: P5CD080 and P5CD144; Firmware version: CPDIxJC_RSEFI-025CD080V402 and CPDYxJC_RSEFI-025CD144V503) was developed by G&D and constitutes a complete operating system for smart cards. Providing a complete set of International Organization for Standardization (ISO), Europay, MasterCard and Visa (EMV) and proprietary enhanced commands, the Sm@rtCafé Expert 3.2 incorporates standards-based functionality along with its own optimized command set.

Sm@rtCafé Expert 3.2 contains an implementation of the GlobalPlatform (GP) Version 2.1.1 specification **[GPCS]**, which defines a secure infrastructure for post-issuance programmable smart cards. The GP specification defines a life cycle for GP compliant cards.

Sm@rtCafé Expert 3.2 offers Java Card technology **[JCS]** and GlobalPlatform 2.1.1 **[GPCS]** services to applets.

State transitions between states of the life cycle involve well-defined sequences of operations. Cards that have been issued are necessarily in a “SECURED” state. This means that the G&D Security Domain has been loaded onto the card plus a set of keys and a PIN through which the Cryptographic Officer can be authenticated.

Sm@rtCafé Expert 3.2 is based on the NXP smart card controller P5CD080 and P5CD144.

Some highlighted features of Sm@rtCafé Expert 3.2 are:

- SHA-1 and SHA-256 Hash algorithms
- Compliant to ISO 7816 Parts 1-7 **[ISO]**
- RSA up to 2048 bit modulus for:
  - Digital signature generation and verification
  - Key generation

- Encryption/Decryption for key transport only

- Triple-DES Encryption/Decryption **[DES]**
- AES Encryption/Decryption
- DSA signature generation and verification

2.1.2 Approved Smart Card configurations

Sm@rtCafé Expert 3.2 is available in two different modules. The following table list their differences.

Module	P5CD080	P5CD144
EEPROM size	80 KB	144 KB
Interfaces	Dual Interface (contact and contactles)	Dual Interface (contact and contactles)

2.2 ActivIdentity Digital Identity Applet Suite V2 for Extended PIV (specifically v2.6.2B)

ActivIdentity Digital Identity Applet Suite V2 for Extended PIV (specifically 2.6.2B) supports identity-based authentication of the Card Holder, Application Operators, and Cryptographic Officers, using PIN/ PUK or TDES keys. All services provided by the cryptographic module are protected by an identity based access control policy following the result of the authentication. This validation effort is aimed at the systems software, virtual machines, Card Manager application, and ActivIdentity applets. If additional applets are loaded into this cryptographic module, then these additional applets require a separate validation, and they must be FIPS 140-2 validated. The cryptographic module checks all validated applets, and will not load any applets that do not have the correct MAC.

ActivIdentity Applet Suite V2.6.2B is composed of the following elements:

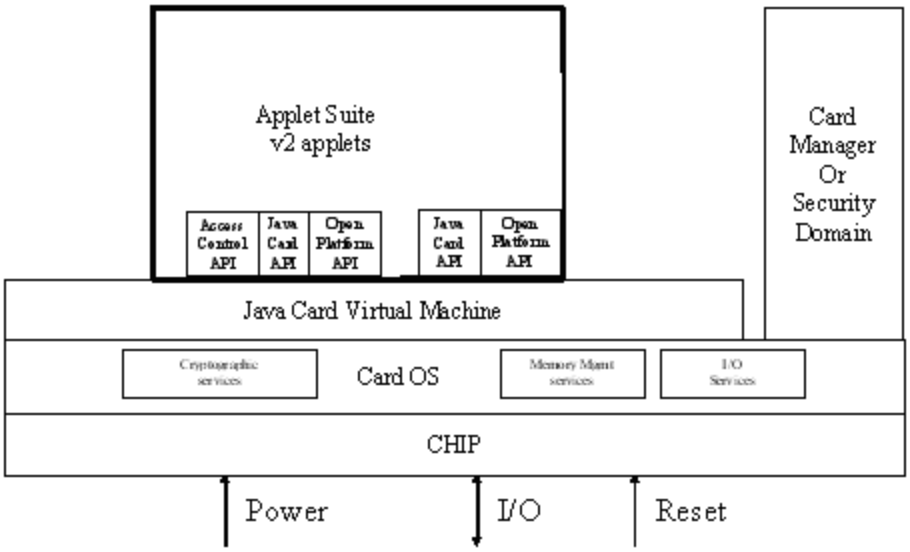
- ASC library package version 2.6.2B.3
- ACA applet package version 2.6.2B.4
- PKI/GC/SKI applet package version 2.6.2B.4
- PIV End Point Wrapper module 2.6.2B.4
- PIV End Point Extended module 2.6.2B.4

- SMA applet package version 2.6.2B.3

The applet and library package byte code is loaded in the cryptographic module memory. Note that the ASC library package consists of static utility classes only accessed by the applet, and the library cannot be accessed directly by off-card entity. The applets offer services to external applications, relying on key management, secure memory management and cryptographic services, provided by the card platform itself. The services are activated with “APDU commands” sent to the cryptographic module.

Applets depend on a unique security domain (SD) for the security configuration. This SD can be either the Card Manager or a separate security domain. The Card Manager is itself a security domain with additional services. Every security domain holds one or more security domain key sets composed of TDES keys.

The ownership of a key set allows for establishing a Secure Channel (SC) between the host and either the security domain or the security domain applets. Generally, the SC is used for administrative operations such as entering the application keys in the applet instances belonging to the security domain, or entering new key sets in the security domain itself. Note that a security domain key set can be used to enter a replacement key set in the same security domain – the replacement involves the deletion of the original key set. This is how a Card Security Controller role (CSC), which solely owns the replacement key set, can take control of the personalization of all applet instances belonging to a security domain.



Applet Suite v2.6.2B supports execution of services via contact and contacless interfaces. Only a few services are contactless enabled, while all applet commands can execute with a contact reader.

The v2 applet suite consists of six applets:

- **Access Control Applet (ACA)** – This applet is responsible for Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services. Three off-card entity authentication methods – GP secure messaging, PIN, and ActivIdentity External Authentication are included by default in the ACA applet.

- **PKI/Generic Container/ SKI (PKI/GC/SKI) Applet** – The PKI/GC/SKI Applet can be used to provide secure storage for PKI credentials, and other data that are required for implementation of card services including single sign-on applications, identity, and benefits information. This applet is responsible for RSA-based cryptographic operations using the RSA private key stored in the PKI buffers. The applet also exposes services for OTP (One Time Password) through a synchronous or asynchronous authentication

- **ASC Library package** – This is the library package that implements functions required by other applets. The library functions are not directly accessible via the cryptographic module command interface.

- **PIV EP Wrapper Applet** – This applet implements the Personal Identity Verification services from NIST SP800-73-1. It exposes the End Point (EP) APDU commands from this specification. The Applet is a wrapper on top of V2.6.2B applets (ASC Lib, ACA and GC/PKI/SKI above). Its purpose is to access PIV Card-Edge and objects although objects are stored in V2.6.2B applet instances. This PIV Applet cannot operate in a standalone mode; it must link with ACA and GC/PKI/SKI(s) applet to operate properly. This applet can only be instantiated in a strictly compliant mode to SP800-73-1 and data model.

- **PIV EP Extended (Ext) Applet** – This Applet implements SP800-73-1 (both at card-edge and data model levels) and is extended to support additional features on top of native PIV such as support of additional PKI RSA keys (example for administrator login. PKI Key Encryption Key, SSO (single sign-on) storage, SKI authentication mechanisms, etc. This applet can be instantiated in PIV EP mode (native PIV features) or in PIV Ext mode (extensions are accessible through the 800-73-1 card edge.).

- **Secure Messaging Anonymous (SMA) plug-in Applet** – this is a secure messaging plug-in to the ACA applet. It provides PKI based key establishement and secure messaging (using Triple-DES) to secure the communication between an off-card entity and any card applications

2.3 Physical Security with Well-Defined Interfaces

The Sm@rtCafé Expert 3.2 with ActivIdentity Digital Identity Applet Suite V2 for Extended PIV meets overall Level 2 requirements of FIPS140-2.

The physical form of the module is a single chip coated in epoxy, with an attached faceplate and an ISO/IEC 7816 contact interface. It is intended to meet overall FIPS 140-2 Level 2 requirements (see Table 2 below).

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference/Electromagnetic Compatibility	3
9	Self-tests	2

10	Design Assurance	2
11	Mitigation of Other Attacks	2

Table 2 – Intended Level according to FIPS 140-2

2.3.1 Chip modules Overview:

This section is applicable to the following chips: NXP P5CD080 and NXP P5CD144

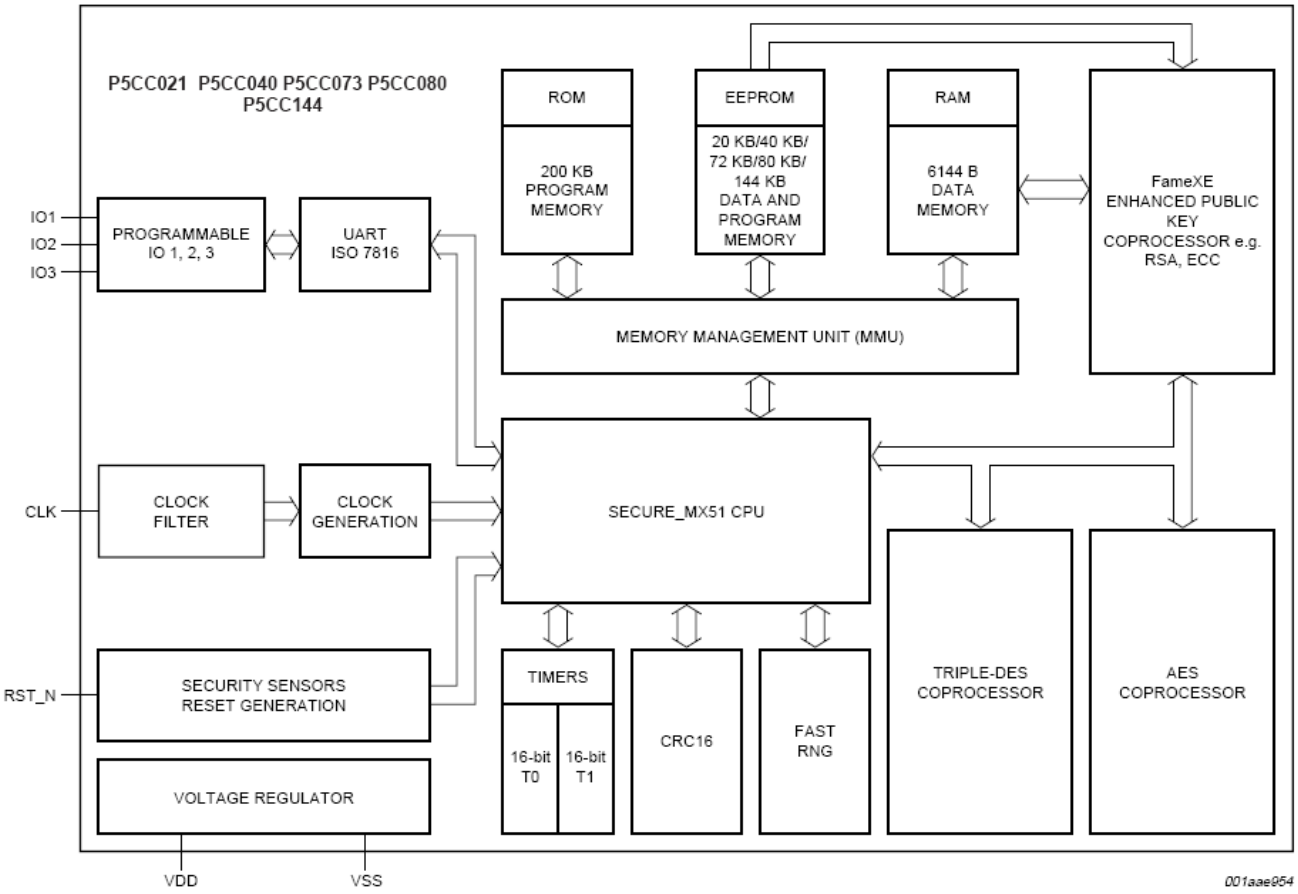


Figure 1 Block Diagram of the NXP P5CD080 and NXP P5CD144

The module is composed of a single chip micro-controller, coated in epoxy, with an attached faceplate, an ISO/IEC 14443 A contactless interface and an ISO/IEC 7816 contact interface.

The chip contains the processor, Read Only Memory (ROM - 200 kilobytes), Random Access Memory (RAM - 6144 bytes), Electrically Erasable Programmable ROM (EEPROM - 80 kilobytes (NXP P5CD080), 144 kilobytes (NXP P5CD144), co-processors, input/output (I/O), and timers. The power interface accepts voltages in the range of +5V +/-10% and +1,8V +/-10%.

The smart card controller provides a number of hardware features, including

- High/Low frequency detector
- High/Low voltage detector
- High/Low temperature detector

If the frequency, voltage, or temperature are higher than the maximum value or lower than the minimum value, the module is reset.

The chip is embedded in epoxy, which completely encapsulates the whole Integrated Circuit (IC). Only micro-wires connecting to the faceplate penetrate the epoxy, connecting to the faceplate interface of the module. Attempts to tamper with the module result in damage to the epoxy, the plastic card, or the metal faceplate (scratches, chips, dents, etc.).

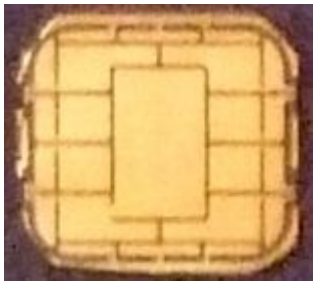


Figure 2 Picture of theNXP P5CD080 and NXP P5CD144 module faceplate

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.

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.

The NXP P5CD080 and NXP P5CD144 smart card controllers provide strong enclosure by coating module components in an epoxy. Physical removal of the epoxy will cause serious damage to the ICC such that all CSPs are destroyed.

The module has been tested for and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for home use as defined in Subpart A of FCC Part 15.

2.3.2 The contact Interface

There is only one physical contact interface to the module, the faceplate, which contains eight contacts, pinned as defined in ISO 7816-2. All FIPS 140-2 logical interfaces map to this single faceplate as detailed in Table 3.

FIPS 140-2 Logical Interface	Physical Interface
Data Input Interface	Faceplate
Data Output Interface	Faceplate
Control Input Interface	Faceplate
Status Output Interface	Faceplate
Power Interface	Faceplate

Table 3 - FIPS 140-2 Logical Interfaces

Additionally, the eight contacts of the faceplate can be mapped to the logical interfaces as depicted in Table 4.

Contact	Function	FIPS 140-2 Logical Interface
C1	Power supply	Power Interface
C2	Reset	Control Input Interface
C3	Clock	Control Input Interface
C4	Not connected	N/A
C5	Ground	Power Interface
C6	Not connected	N/A
C7	Input/Output for serial data	Data Input Interface, Data Output Interface, Control Input Interface, Status Output Interface
C8	Not connected	N/A

Table 4 - Contact to Function Mapping

As described in ISO 7816-2, when the module is first inserted into the reader (also referred to as the terminal), a RST signal is transmitted to contact C2. Power is applied via contact C1; C7 is set to reception mode; and the external clock is established via contact C3. The I/O interface (C7) has reception and transmission modes. The smart card reader sends commands to the module and the module transmits responses using contact C7.

2.3.3 The contactless Interface

This interface operates in accordance with ISO/IEC 14443A; the T=CL protocol is supported according to ISO/IEC 14443-4.

2.3.4 The cryptographic boundary

In the scope of this document, the Sm@rtCafé Expert 3.2 is considered as a single chip implementation of a cryptographic module.

The cryptographic boundary for Sm@rtCafé Expert 3.2 is the single chip micro-controller, coated in epoxy, with an attached faceplate, and the dual interface (ISO/IEC 7816 contact and ISO/IEC 14443A contactless interfaces) for the NXP P5CD080 and NXP P5CD144.

The chip is therefore providing the physical boundary.

2.4 Finite State Machine Model

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 module is published as a separate document.

2.5 Software Security

The firmware for the Sm@rtCafé Expert 3.2 is protected from modification due to the fact that it is stored in ROM. This systems software is written primarily using a high-level programming language and the machine language specific to the underlying chip that allows for performance increase or to enhance security of the module.

It is loaded onto the module during manufacturing and does not allow for modification. An Error Detection Code (EDC) is calculated over the firmware during this installation and is checked at each power up. Attempts to modify the firmware require direct access to the IC and are prevented by the physical security described in section 2.3 above.

The card systems software includes an on-card Java Card Virtual Machine. Applets are isolated 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.

Each applet is loaded on the card within a Secure Channel, which is protected by a TRIPLE-DES MAC. Sm@rtCafé Expert 3.2 also provides a Data Authentication Pattern for each loaded applet. This insures that the chip issuer has digitally signed each applet

that is to be loaded on the chip, allowing prior security verification of each applet and avoiding the loading of any unauthorized applet during the manufacturing process.

During the manufacturing process, only trusted (validated against FIPS 140-2) applets are loaded onto the chip. These include the Card Manager applet and the G&D Security Domain.

After completion of the manufacturing process (including pre-personalization) when the chip has reached its normal Operating Life Cycle State (Card Manager Secured State), only trusted FIPS 140-2 validated applets shall be loaded or installed onto the module. Furthermore, at the time of loading, these applets must be identified as part of the cryptographic module. The FIPS 140-2 validation testing targeted this specific configuration of smartcard and applets. Changes to that configuration (for example, loading another applet), would constitute a new module, and the new configuration would need to undergo 140-2 testing for FIPS 140-2 compliance.

2.5.1 Command Structure

The module provides a well-defined, static set of commands. A smart card reader sends these commands to the module and then responses are transmitted from the module to the reader. Only these commands are available to an operator, and only the faceplate interface may be used to access the module's functionality.

The details of these commands are defined in the Sm@rtCafé Expert 3.2 Technical Specification Document that is included as a proprietary and private extension to this Sm@rtCafé Expert 3.2 Policy document. Other commands are also exposed by the ActivIdentity Digital Identity Applet Suite V2 for Extended PIV (V2.6.2B) to fultill a complete set of services.

Sm@rtCafé Expert 3.2 is only capable of operating in response to commands sent from the reader in what is called a command-response pair. The reader sends an Application Protocol Data Unit (APDU) to the module and module responds with an APDU.

The APDU sent by the reader consists of a header and a body. The header contains a class byte differentiating between ISO defined command and private commands, an instruction byte containing the command code, and parameters relating to the command. The body contains any data that is needed for the command and, if necessary, the length of the expected data.

The response APDU transmitted by the module consists of a body and a trailer. The body contains any data that is returned in response to the command and the trailer contains the status message.

This card also provides an additional set of on-card services through the Java Card and Global Platform APIs. The API classes and their associated methods are also defined in

Sm@rtCafé Expert 3.2 Technical Specifications. These services are only available internally, to an applet loaded on the card (here the ActivIdentity Applets in the context of this certificate). They cannot be accessed from outside the module.

3. ROLES & SERVICES

The module defines three distinct roles that are supported by the on-module cryptographic system; the Card Security Controller (CSC, also called Cryptographic Officer) role, the Application Operator role, and the Card Holder role.

3.1 Roles

The module supports two groups of roles: the Cryptographic Officer (CO/CSC) and the User-related ones:

- ***The Cryptographic Officer (also called Card Security Controller: CSC):*** This role is responsible for managing the security configuration of the Card Manager and Security Domains. The CSC role authenticates to the cryptographic module by demonstrating to the Card Manager application that he possesses the knowledge of a GP secure channel TDES key set stored within the Card Manager. By successfully executing the GP secure channel mutual authentication protocol, the CSC role establishes a secure channel to the Card Manager and executes services allowed to the CSC role in a secure manner. The CSC role can also be responsible for unblocking the PIN using a specific unblock PIN XAUT key with ActivIdentity external authentication protocol.

- ***The User-related roles*:**
  - **Card Holder Role (CH)** - The Card Holder role is responsible for ensuring the ownership of his cryptographic module, and for not communicating his PIN to other parties. An applet authenticates the Card Holder by verifying his PIN.
  - **Application Operator Role (AO)** – The Application Operator role represents an external application requesting the services offered by the applets. An applet authenticates the Application Operator role by verifying possession of the Application External Authenticate (XAUT) TDES key. The AO is also able to provide the PUK credential to unblock the PIN (SP800-73-1).

3.2 Role Authentication

The cryptographic module supports identity based role authentication. The module specifies one Crypto-Officer role (Card Security Controller) and two User roles (Card Holder and Application Operator). The Card Security Controller (CSC) role authenticates to the module using the knowledge of three Triple-DES keys uniquely identifying the Crypto-Officer. The Application Operator authenticates to the module using a unique Triple-DES key or the PUK credential. While the Card Holder (CH) role authenticates to the module using a PIN. In each case the authentication is identity based as different CH or AO operators will have different authentication key/PIN and there can only be one CSC per module.

3.2.1 User Role Authentication

The Card Holder role is authenticated with a PIN:

- **PIN**: The Card Holder role must send a VERIFY APDU to the module to access services protected with PIN access control rules (PIN once for session or PIN-Always). The APDU corresponding to the applet service protected by the PIN, can access the service before the cryptographic module is removed or a reset command is sent to the cryptographic module.

The Application Operator role is authenticated by the possession of a TDES key or a 8 bytes-string for PIN Unblocking Key (PUK):

- **Application External Authentication (XAUT) key**: The Application Operator role must prove the possession of a particular TDES key to access the PKI/GC/SKI buffer, or update service protected with the External Authentication protocol using this particular key. An 8-byte challenge is first obtained from the applet. The application controlled by the operator encrypts the challenge with a 112-bit TDES key (or 168-bit key), and submits the resulting cryptogram to the module for verification. The APDU corresponding to the particular applet service protected by the XAUT key, can access the service before the cryptographic module is removed or a reset command is sent to the cryptographic module.

- **Unblock with PUK:** The AO can also complete the PIN unblock operation with the PUK (which is loaded under the CSC/CO role).

3.2.2 Cryptographic Officer Role Authentication

The Cryptographic Officer role is authenticated by a TDES key set in the case of secure channel key set, or a TDES key in the case of XAUT key.

- **Secure Channel key set:** The Cryptographic Officer (CO/CSC) role must prove the possession of a key set composed of three TDES keys. Two keys (K_{MAC}, K_{ENC}) are used to generate session keys according to Global Platform specification. The session keys ensure the confidentiality of the command payload, allow the mutual authentication of the parties and protect the APDU command integrity. A third key (K_{KEK}) is used to wrap keys transported within the APDU command.

- **Unblock PIN with XAUT key:** The Cryptographic Officer (CO/CSC) role performs the ActivIdentity external authentication protocol using the XAUT TDES key. The PIN is unblocked if the CSC role is successfully authenticated.

3.3 Services

3.3.1 Crypto Officer Administrative Services

The Crypto Officer uses a command set for the administration of the G&D Security Domains and to load applets onto the module. The following APDUs are sent to Card manager/Security Domain:.

- **DELETE ALL**: is used to delete all packages and applet instances installed from those packages that have been loaded after completion of the card via LOAD commands.
- **GET STATUS**: if the Card Manager is the current application, this command is used to retrieve Card Manager information according to a given search criteria.
- **PIN CHANGE / UNBLOCK**: this command replaces or unblocks the Global PIN (Card Holder PIN).
- **SET STATUS**: this command is used to modify the life cycle state of the module or the life cycle state of an application.
- **INSTALL:** the INSTALL command instructs a Security Domain or the Card Manager which installation step it shall perform during an application installation process.
- ***LOAD:*** the LOAD command loads the byte-codes of the Load File (package) defined in the previously issued INSTALL command.
- **DELETE:** the DELETE command deletes a Load File (package) or an Application (applet instance).
- **EXTERNAL AUTHENTICATE**: this command is used by the module to authenticate the host, establish the Secure Channel, and to determine the level of security required for all subsequent commands within the Secure Channel. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.
- **PUT DATA**: this command is used to store or replace one tagged data object provided in the command data field.
- **PUT KEY**: this command is used to add, replace or modify a single key or key sets.

Applets loaded onto the Sm@rtCafé Expert 3.2 module post-issuance must be FIPS 140-2 validated.

Applets are loaded through a Secure Channel established by the Crypto Officer with the Card Manager during the Identification/authentication process. The applet is divided in a series of blocks that fit in a LOAD command. The loading is managed in a series of

LOAD commands, each one transmitting a block, encrypted and followed by a TRIPLE-DES MAC with the Secure Channel session keys established during the identification process. The correct transmission of each block of the applet and therefore of the whole applet is ensured by the TRIPLE-DES MAC.

Optionally a mechanism called “GP DAP” enables the applet provider to check that his applet has been correctly loaded independently of the Issuer. The following DAP verification modes may be used

- Single DES plus final Triple DES as defined in **[GPCS]**, C.5.1
- Full Triple DES
- RSA with PKCS#1 Scheme as defined in **[GPCS]**, C.5.2

The DES Load File Data Block Signature verification consists of a series of DES MAC verification, ended by a TRIPLE-DES MAC verification. All the DES and TRIPLE-DES MAC operations use the”GP DAP” TRIPLE-DES key, loaded in the G&D Security Domain. The FIPS configured card prevents an operator from using this method of DAP verification, as DES is not a FIPS approved algorithm.

The full Triple DES DAP verification consists of a series of TRIPLE-DES MAC verification. All the TRIPLE-DES MAC operations use the”GP DAP” TRIPLE-DES key, loaded in the G&D Security Domain. Full TRIPLE-DES DAP verification is allowed in the Approved mode of operation.

The RSA Load File DAP is calculated using a PKCS#1 singature. The SHA-1 message digest is padded according to PKCS#1 V1.5 and encrypted with the private RSA key. DAP verification using RSA keys are allowed in the Approved mode of operation.

The following APDUs are sent to ActivIdentity applets:

- **CHANGE REFERENCE DATA:** This APDU intends to create the PIN and PUK in the card. It is also used to update the PUK value.
- **EXTERNAL AUTHENTICATE**: Similar to command sent to Card manager/Security Domain
- **GENERATE ASYMMETRIC KEY PAIR:** This APDU has the same role than GENERATE KEY PAIR but it can also return the public modulus on demand. This APDU is present for compliance with PIV specifications
- **GENERATE KEY PAIR:** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. The public key is output as the response of this command and not stored on the card.

- **GET DATA**: This command is used to retrieve a single data object
- **PRIVATE SIGN/DECRYPT:** This APDU uses the RSA private key in the PKI buffer to sign data.
- **PUT DATA:** This APDU intends to set the applet properties, load keys as well as personalize the container managed under the PIV Ext applet. This APDU is present for compliance with PIV specifications.
- **PUT KEY**: This APDU is used to either enter the XAUT keys (like used to unblock the PIN), the RSA private key component or the SKI key for One Time Password generation. The APDU must be used with a secure channel established by CSC role. The APDU format is compliant with GP specifications.
- **READ CERTIFICATE / STATIC BUFFER:** This APDU is used to read the data from the selected buffer.
- **REGISTER ACR:** This APDU manages the mapping between ACRID and actual APDU instruction as well as record the ACR definition for the applet services.
- **REGISTER APPLET*:*** This APDU is to register applet instances to the ACA instance so that the access control and secure message service can be provided.
- **RESET RETRY COUNTER*:*** This APDU is used to unblock the cardholder PIN and restore the VERIFY service with a new counter value if the CSC role is authenticated successfully. The command operates as long as the unblock counter has not expired.
- **SET APPLICATION UID**: This APDU is sent when the UID associated with the applet instance needs to be changed
- **SET PROPERTIES:** This APDU creates and sets the object properties for GC/PKI/SKI applet.
- **SET STATUS**: This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, and PERSONALIZED
- **UPDATE CERTIFICATE / STATIC BUFFER:** This APDU is used to update the data stored in the selected buffer.
- **UPDATE PROPERTIES*:*** This command updates the ACA properties

3.3.2 *Application Operator Role:*

The following APDUs are sent to ActivIdentity applets:

- **AC EXTERNAL AUTHENTICATE**: This APDU is used in combination with a Get Challenge to authenticate the Application Operator using the AC external authenticate protocol.
- **GENERATE ASYMMETRIC KEY PAIR*:*** This APDU has the same role than GENERATE KEY PAIR but it can also return the public modulus on demand. This APDU is present for compliance with PIV specifications. This APDU is present for compliance with PIV specifications.
- **GENERATE KEY PAIR*:*** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. The public key is output as the response of this command and not stored on the card.
- **GET DATA**: This command is used to retrieve a single data object like PIV object content
- **PUT DATA*:*** This APDU is present for compliance with PIV specifications and it is used to personalize containers managed under the PIV Ext applet
- **READ CERTIFICATE / STATIC BUFFER*:*** This APDU is used to read the data from the selected buffer.
- **UPDATE CERTIFICATE / STATIC BUFFER*:*** This APDU is used to update the data stored in the selected buffer.
- **RESET CARD*:*** This command resets the card content (buffer content, PKI credentials, SKI keys as well the PIN/PUK)
- **RESET RETRY COUNTER*:*** This APDU is used to unblock the PIN with PUK string.

3.3.3 *Cardholder Role*

The following APDUs are sent to ActivIdentity applets:

- **CHANGE REFERENCE DATA:** This APDU is used to change the cardholder PIN if the Card Holder is correctly authenticated.
- **GENERATE ASYMMETRIC KEY PAIR:** This APDU has the same role than GENERATE KEY PAIR but it can also return the public modulus on demand. This APDU is present for compliance with PIV specifications. This APDU is present for compliance with PIV specifications.

- **GENERAL AUTHENTICATE**: The APDU is for PKI operations (via the PIV EP wrapper and PIV EP Ext)
- **GENERATE KEY PAIR:** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. The public key is output as the response of this command and not stored on the card.
- **GET DATA**: This command is used to retrieve a single data object like PIV object content
- **INTERNAL AUTHENTICATE (GENERAL AUTHENTICATE command)**: The APDU is for SKI operations and to generate a cryptogram from the card for verification by the calling application.
- **PRIVATE SIGN/DECRYPT:** This APDU uses the RSA private key in the PKI buffer to sign data.
- **PUT DATA:** This APDU intends to personalize the card objects. This APDU is present for compliance with PIV specifications.
- **PUT KEY**: This APDU is used to either enter the XAUT keys, the RSA private key component or the SKI key for One Time Password generation. In a Cardholder role, the APDU must be used with a SMA channel to encrypt the key component.
- **READ CERTIFICATE / STATIC BUFFER:** This APDU is used to read the data from the selected buffer.
- **UPDATE CERTIFICATE / STATIC BUFFER:** This APDU is used to update the data stored in the selected buffer.
- **UPDATE PROPERTIES:** This command updates the ACA properties
- **VERIFY**: This APDU checks the PIN presented by the cardholder against the current PIN.

3.3.4 Unauthenticated/No Role services:

The following APDUs are sent to Card manager/Security Domain:

- **MANAGE CHANNEL**: this command is used to open or close a logical channel.
- **GET DATA**: the GET DATA command is used to retrieve a single data object. This 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.

- **SELECT**: this command is used for selecting an application (Card Manager or G&D Security Domain).
- **GET FREE SPACE**: GET FREE SPACE is used to display the largest free memory block for package loading or the complete available free EEPROM or the complete available Clear-On-Reset (COR) /Clear-On-Deselect (COD) space.
- **INITIALIZE UPDATE**: this command is used to initiate a Secure Channel with the Card Manager or a Security Domain attached to an applet. Sm@rtCafé Expert 3.2 module and host session data are exchanged and session keys are generated by the Sm@rtCafé Expert 3.2 module upon completion of this command. However, the Secure Channel is not considered open until completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.

A user can initiate module self-tests by issuing a card reset and issuing an APDU command. The module provides a Get ATR service to retrieve the module ATR value on power-up.

All commands (except Manage Channel, Select, Initialize update, Get Free Space and Get Data) need a secured channel to be executed by either a CO or User. During the secure channel opening, the command access condition is specified ('CLEAR','MAC','MAC+ENC') and an access control is done on received commands.

The following APDUs are sent to ActivIdentity applets:

- **GET CHALLENGE:** This APDU is used in combination with AC external authenticate to perform an external authentication of the Application Operator in order to unblock the PIN. It is also involved when opening a SMA session.
- **GENERAL AUTHENTICATE**: The APDU is for PKI operations (via the PIV EP wrapper and PIV EP Ext) as well as when opening a SMA session
- **GET ACR:** This APDU is used to retrieve the ACR definition for the services.
- **GET DATA**: This command is used to retrieve a single data object, such as the Card Identification data.
- **GET PROPERTIES**: This APDU is used to obtain information about applet instance configuration.
- **GET RESPONSE**: This command is restricted to T=0 ISO protocol for an incoming command which has data to send back. That data is received with the GET RESPONSE command sent immediately after the command to which it is related.

- **INITIALIZE UPDATE**: this command is used to initiate a Secure Channel with the applet. Same role as for the Card Manager/Security Domain.
- **LOGOUT:** To logout all authenticated roles.
- **UPDATE PROPERTIES:** This APDU modifies the applet properties The APDU is accessible from ACA applet.
- **READ BINARY:** This APDU reads binary data stored on the card. This command is deprecated in v2.6.2a.
- **READ CERTIFICATE / STATIC BUFFER:** This APDU is used to read the data from the selected buffer.
- **UPDATE CERTIFICATE / STATIC BUFFER:** This APDU is used to update the data stored in the selected buffer.
- **SELECT**: This command is used for selecting an application (Card Manager, security domain or Applet). The Card Manager may be selected either for the loading of a Load File or for installing a previously loaded application (or security domain)
- **PRIVATE SIGN/DECRYPT:** This APDU uses the RSA private key in the PKI buffer to sign data (involved with PIV Card Authentication Key)
- **MANAGE SMA**: The APDU is used to explicitly close the SMA secure session

3.3.5 Relationship between Roles & Services

Role / Authentication Method Vs. Services	**Cryptographic Officer (CO/CSC)** (G&D Card Manager)	**Cryptographic Officer (CO/CSC)** (G&D Security Domain)	**No Role / None**
INSTALL	X	X	
LOAD	X	X	
DELETE	X	X	
DELETE ALL	X		
EXTERNAL AUTHENTICATE	X	X	
GET DATA			X
GET FREE SPACE			X
GET STATUS	X		
INITIALIZE UPDATE			X
PIN CHANGE/UNBLOCK	X		
PUT DATA	X	X	

PUT KEY	X	X	
SELECT			X
MANAGE CHANNEL			X
SET STATUS	X		

Table 5 Relationship between Roles & Services for Card Manager / Security Domain

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC) / SECURE CHANNEL	Application Operator / XAUT (or PUK)	Card Holder / PIN	Applet v2.6.2b	
					ISO 7816	ISO 14443
AC EXTERNAL AUTHENTICATE			X		X	
CHANGE REFERENCE DATA (change PIN)				X	X	
CHANGE REFERENCE DATA (Create PIN/PUK + Update PUK)		X			X	
EXTERNAL AUTHENTICATE	X				X	
GENERATE KEY PAIR		X	X	X	X	
GENERATE ASYMMETRIC KEY PAIR		X	X	X	X	
GENERAL AUTHENTICATE	X			X	X	X
GET ACR	X				X	
GET CHALLENGE	X				X	X
GET DATA	X	X	X	X	X	X
GET PROPERTIES	X				X	X
GET RESPONSE	X				X	X
INITIALIZE UPDATE	X				X	
INTERNAL AUTHENTICATE				X	X	X
LOGOUT	X				X	
MANAGE SMA	X				X	X
PRIVATE SIGN/DECRYPT	X	X		X	X	X
PUT KEY		X		X (SMA-ENC minimum)	X	

PUT DATA		X	X	X	X	
READ BINARY	X				X	X
READ CERTIFICATE / STATIC BUFFER	X	X	X	X	X	X
REGISTER APPLET		X			X	
REGISTER ACR		X			X	
RESET CARD			X		X	
RESET RETRY COUNTER (with PUK)			X (PUK)		X	
RESET RETRY COUNTER (without PUK)		X	X		X	
SET APPLICATION UID		X			X	
SELECT	X				X	X
SET PROPERTIES		X			X	
SET STATUS		X			X	
UPDATE CERTIFICATE / STATIC BUFFER	X	X	X	X	X	
UPDATE PROPERTIES	X	X		X	X	
VERIFY				X	X	X

Table 6 Relationship between Roles & Services for ActivIdentity Applet

3.3.6 Applets Services

Applets that are developed and downloaded onto the module shall use the Sm@rtCafé Expert 3.2 Java Card APIs. These APIs are listed in a detailed separate proprietary document and are only accessible by on-card applets. The APIs containing cryptographic services are:

- Key Generation:

  - RSA key pair generation: this API generates a pair of RSA keys.
  - DSA key pair generation: this API generates a pair of DSA keys as per FIPS 186-2.

- Message Digest:

- SHA-1: this API performs a SHA-1 Message Digest.
- SHA-256: this API performs a SHA-256 Message Digest.

- Random Numbers Generation:

- Secure Random Generation: this API generates a random data, using output from the ANSI X9.31 FIPS140-2 approved method (Deterministic RNG) xored with random data generated by Hardware Random Generator (Non- Deterministic RNG) provided by the chip.

- Signature and Verification:

- RSA using SHA-1: for origin authentication and Data integrity verification.
- DSA using SHA-1: for origin authentication and Data integrity verification.
- TRIPLE-DES MAC: these APIs offer TRIPLE-DES MAC in CBC and ECB modes with various padding (no padding, PKCS5, ISO9797 M1 and M2).

- Encryption/Decryption:

- TRIPLE-DES/AES: these APIs offer TRIPLE-DES/AES encryption and decryption services using CBC or ECB mode using various padding (no padding, PKCS5, ISO9797 M1 and M2).

The above stated algorithms shall be used only in a FIPS approved mode of operation and their use will be tested during the applet's FIPS 140-2 validation.

The GP specification defines various GP APIs that may be used by the applets and that provide the same services as the Card Manager Commands (such as secure channel opening). In particular, the Global PIN verification may be implemented by the applets through the use of a dedicated API (note: Global PIN is not currently called by ActivIdentity Applet V2.6.2B)

3.3.7 Card Cryptographic Functions

The cryptographic module provides a FIPS approved platform for applets that provide cryptographic services to end -user applications.

FIPS 140-2 validated algorithms in the cryptographic module provide cryptographic services; these include:

- **TRIPLE-DES (3 key TRIPLE-DES)**:
  - The TRIPLE-DES (ECB/CBC mode) algorithm is used:

- for authenticating the Crypto Officer (EXTERNAL AUTHENTICATE command)
- for encrypting data flow from the host to the card. The reverse direction is not encrypted; i.e. the data and the status words returned in response to an APDU are not encrypted.
- as a TRIPLE-DES MAC to authenticate the originator and to verify the integrity of the message

- TRIPLE-DES MAC is also used together for DAP verification
- TRIPLE-DES and TRIPLE-DES MAC functions are also provided as services to applets, through JavaCard APIs.

- **AES (128, 192 and 256-bit key-sizes)**:
  - AES functions are only provided as services to applets, through JavaCard APIs.
- **SHA-1**:
  - The SHA-1 function is only provided as a service through Java APIs to applets.
- **SHA-256**:
  - The SHA-256 function is only provided as a service through Java APIs to applets.
- **RSA PKCS#1 (1024-2048 bit keys)**:
  - RSA Signature Verification services are used during DAP verification.
  - RSA Sign/Verify functions are only provided as services to applets, through JavaCard APIs. The applet shall use RSA only for key wrapping/unwrapping or signature generation/verification.
- **DSA (1024 bit key sizes)**
  - DSA Sign/Verify is only provided as as services to applets, through JavaCard APIs
  - Only 1024 bit key sizes are allowed for use in FIPS mode

3.3.8 RNG

The cryptographic module offers a RNG implementation in which the output from a FIPS-Approved ANSI X9.31 (Appendix A.2.4) DRNG XORed with random data generated by Hardware Random Generator of the chip.

3.4 Critical Security Parameters (CSP):

Key	Key type	Generation	Entry	Storage	Use
Crypto-Officer keys	112 bit Triple-DES keys	External by manufacturing	Pre-configured	Garbled in the module's non-volatile memory	Authentication of Crypto-Officer
Session keys of Crypto-Officer	112 bit Triple-DES keys	Authentication of Crypto-Officer	Generated on card during secure channel establishment	Garbled in volatile memory	Secured and or encrypted communication between terminal and module depending on security level of authentication.
Delegated Management Token Key	1024 bit RSA key	External by Crypto-Officer	Load in encrypted form with PUT KEY command	Garbled in the module's non-volatile memory	Authorization of Delegated Management commands
Delegated Management Receipt Key	112 bit Triple-DES key	External by Crypto-Officer	Load in encrypted form with PUT KEY command	Garbled in the module's non-volatile memory	Confirmation of command execution
RSA DAP verification key	1024 bit RSA key	External by Crypto-Officer	Load in encrypted form with PUT KEY command	Garbled in the module's non-volatile memory	Load File Data Block Signature verification
TDES DAP verification key	112 bit Triple-DES key	External by Crypto-Officer	Load in encrypted form with PUT KEY command	Garbled in the module's non-volatile memory	Load File Data Block Signature verification
User keys	112 bit Triple-DES keys	External by Crypto-Officer	Load in encrypted form with PUT KEY command	Garbled in the module's non-volatile memory	Authentication of User
Session keys of User	112 bit Triple-DES keys	Authentication of User	Generated on card during secure channel establishment	Garbled in volatile memory	Secured and or encrypted communication between terminal and module depending on security level of

Key	Key type	Generation	Entry	Storage	Use
					authentication.
External Authentication Keys (XAUT)	112 or 168 bit Triple-DES keys	External by Crypto-Officer	Load in encrypted form with PUT KEY command	Garbled in the module's non-volatile memory	TDES keys that enable the authentication of either Application Operators or Cryptographic Officers (RESET RETRY COUNTER command for Unblocking the PIN).
SKI Key for OTP	112 or 168 bit Triple-DES keys	External by Crypto-Officer	Load in encrypted form with PUT KEY command	Garbled in the module's non-volatile memory	TDES key is involved during generation of the One Time Password and then authentication from the card to the calling application.
RSA private keys in the ActivIdentity Applet	1024-2048 bits RSA	Generated or unwrapped by the PKI/GC or PIV EP applet using the Java Card cryptographic services	Load in encrypted form with PUT KEY command (or generate on-board using GENERATE KEY PAIR)	Garbled in the module's non-volatile memory	These keys are used to generate signatures.
PIV private key objects in the ActivIdentity Applet	1024-2048 bits RSA	Generated or unwrapped by the PKI/GC or PIV EP applet using the Java Card cryptographic services	Load in encrypted form with PUT KEY command (or generate on-board using GENERATE ASYMMETRIC KEY PAIR)	Garbled in the module's non-volatile memory	Four RSA keys are managed in the Applet Suite. Keys are defined in the PIV specification (SP800-73-1) and are attached with key IDs:

Key	Key type	Generation	Entry	Storage	Use
					9Ah (PIV Authent), 9Ch (PIV Digital Signature), 9Dh (PIV Key Management), and 9Eh (PIV Card Authent)
RSA public keys in the ActivIdentity Applet	1024-2048 bits RSA	Generated by the PKI/GC or PIV EP applet using the Java Card cryptographic services	Returned in response to GENERATE ASYMMETRIC KEY PAIR or GENERATE KEY	Garbled in the module's non-volatile memory	Public keys are stored under the form of public key certificate and recorded in GC buffers that belongs from the GC/PKI/SKI applet. There is a certificate slot booked for each RSA private key defined in the card
Global PIN	PIN	External – entered by Crypto-Officer	Load in encrypted form with PIN CHANGE / UPDATE command	Garbled in the module's non-volatile memory	
Card Holder Personal Identification Number (CH PIN)	PIN (Minimum 6 bytes in the card)	External – entered by Crypto-Officer for PIN creation	Loaded or modified via the CHANGE REFERENCE DATA command. The initial PIN is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set, and can be	Garbled in the module's non-volatile memory	To authenticate the Card Holder. It contains authentication string that belongs to the Card Holder. CH PIN and associated attributes are managed from the ACA Applet, which relies on Java

Key	Key type	Generation	Entry	Storage	Use
			changed later by the user after a successful user authentication event.		Card PIN management service.
PIN Unblocking Key (PUK)	The PUK pattern is 8 bytes long in the card and it contains a static byte sequence unique in each card issued.	External – entered by Crypto-Officer	Loaded or modified via the CHANGE REFERENCE DATA command. The PUK is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set.	Garbled in the module's non-volatile memory	The PUK is managed inside the ACA. It is used to authenticate the AO. Its role is to unblock the PIN.
X9.31 DRNG keys	112 bit Triple-DES keys	Internal by HW random number generator of the module	Internally initialized with individual keys randomly selected by the module	Garbled in the module's non-volatile memory	Used by X9.31 DRNG
ANSI X9.31 seed	16 byte random number	Internal by HW random number generator of the module	Internally initialized with individual keys randomly selected by the module	Garbled in the module's non-volatile memory	Used by X9.31 DRNG

For the purposes of FIPS, all keys and CSPs are considered stored in plaintext form.

4. SECURITY RULES

4.1 Applet Loading Security Rules

Only applets validated according to FIPS 140-2 shall be loaded onto the cryptographic module. Applets can only be loaded through a secure channel thus requiring TRIPLE-DES MAC verification over each Load block.

In the Sm@rtCafé Expert 3.2 module, the applet is always loaded by the Issuer (Cryptographic Officer) or authorized by Issuer in case of Delegated Management.

4.1.1 "GP Delegated Management"

If Delegated Management is used, the Crypto Officer has to set Delegate Management Keys for Token verification (K_{Token}) and Reciept generation ($K_{Receipt}$), install the G&D Security Domain with Delegated Management privilege and set Secure Channel keys of this Security Domain.

User of G&D Security Domain can load packages or install applications on the card, only if he/she establishes a secure channel and presents the card with a Token during the GP Install for Load command. The Token is a RSA signature generated by the Card Issuer using the Card Issuer private key to ensure that the Card Issuer has authorized the load process and the Load File or the install process. If the token verification is successful, the card processes the Load command and answers with a reciept, i.e. a TRIPLE-DES MAC generated by the Card, acknowledging that the operation was successfully performed. For details see GP 2.1.1 **[GPCS]**.

4.1.2 "GP DAP"

If the G&D Security Domain is instantiated with a DAP verification privilege, an applet may be loaded with an optional DAP. If the G&D Security Domain is instantiated with mandated DAP verification privilege, a DAP is required.

The mechanism designated as "DAP" in GP 2.1.1 **[GPCS]** enables the applet provider to check, independently of the Issuer (Cryptographic Officer), that his applet has been correctly loaded. This check is done by MAC verification on the Load File. DAP may be generated either using TRIPLE-DES or RSA.

As identified in Section 3.2.1, only DAP verification using full TRIPLE-DES or RSA may be used in the Approved mode of operation.

This process is described in detail in the Reference Manual Sm@rtCafé Expert 3.2.

4.2 Access Control Security Rules

- Cryptographic Keys must be loaded through a secure channel and encrypted with the K_{kek}. Therefore the keys are always loaded in encrypted form.

- Global PIN / Cardholder PIN / PUK are set through a secure channel and encrypted with the K_{kek}. Therefore are always transferred in encrypted form.

4.3 Physical Security Rules

The physical security of the Sm@rtCafé Expert 3.2 smart card is designed to meet FIPS 140-2 level 3 requirements whereas the module is globally validated to Level2. A hard opaque epoxy is used to encapsulate the module to meet level 3 requirements. Once it is manufactured, the Sm@rtCafé Expert 3.2 belongs to the Cryptographic Officer until it is ultimately issued to the end user.

4.4 Key Management Security Policy

4.4.1 Cryptographic key generation

-TRIPLE-DES Session key derivation for Secure Channel, conforming to Open Platform Card Specification v2.1.1 **[GPCS]**. The random data required for opening a Secure Channel is generated using the FIPS140-2 approved ANSI X9.31 DRNG **[X9.31]** xored with random data generated by Hardware Random Generator of the chip.

- RSA and DSA key pair generation using FIPS140-2 approved ANSI X9.31 DRNG **[X9.31]** xored with random data generated by Hardware Random Generator of chip.

4.4.2 Cryptographic key entry/output

If Keys are imported they shall always be encrypted with the K_{kek} and transferred by using the Put Key command within a secure channel.

During this process, the keys are double encrypted (using the Session Key K_{enc} and the K_{kek}) if the Secure Channel security level is set to MAC+ENC.

Public key output is in non encrypted format. Other than public keys, no secret and private keys can be output from the module.

4.4.3 Cryptographic key storage

The Keys contain the following parameters:

- Key id, which is the Id of the key,

- Algo Id, which determines which algorithm to be used,

- Integrity Check value for the key.

Symmetric keys are garbled by XOR calculation with card individual random number.

Secret part x of DSA key is garbled by multiplication with card individual random number.

Exponent of RSA private key is garbled by multiplication with card individual random number.

DP and DQ of RSA CRT private key is garbled by multiplication with card individual random number.

P and Q of RSA CRT private key is garbled by modulo calculation with card individual random number.

PQ of RSA CRT private key is garbled by XOR calculation with card individual random number.

RSA public key is not garbled.

PINs (and PUK) are encrypted by DES calculation using a card individual key.

4.4.4 Cryptographic key destruction

The module replaces initialitzation Key K_{init} of Card Manager with first new keyset loaded into Card Manager.

Security Domain (Card Manager and G&D Security Domain) Keysets (including K_{ENC}, K_{MAC} and K_{KEK}) loaded onto the card can be deleted using the Delete APDU or replaced by reloading another key set for Crypto Officer and User using the Put Key command

The module destroys cryptographic session keys K_{SMAC} and K_{SENC} of Security Domain (Card Manager and G&D Security Domain) when closing of a secure channel.

The key(s) for “GP DAP” $K_{DAP,}$ PK_{DAP} can only be updated. To delete DAP verification key(s), the Security Domain containing the key must be deleted. This operation deletes all the keys contained in the Security Domain.

The keys loaded for Delegated Management K_{Token} and $K_{Receipt}$ can be zeroized by overwriting them with new values using the Put Key command or using the Delete command.

The Global PIN/CardHolder PIN or PUK can be zeroized by overwriting with a new value.

Key Management Details can be found in section 6.

All keys including DRNG TRIPLE-DES key for FIPS140-2 approved ANSI X9.31 DRNG **[X9.31]** and the Global PIN can be zeroized by setting the card state to TERMINATED.

4.5 Approved mode

The cryptographic module supports FIPS compliant operation at all times. Note that while the module provides certain non-Approved functions as internal services to applets loaded on the card (via the JavaCard API), these services are not accessible to operators of the module and have only been listed for the benefit of applet developers. It is the responsibility of the applet developer to develop applets that use the provided JavaCard API functions in a FIPS 140-2 compliant manner.

The non-Approved applet services provided by the card's JavaCard API are:

- DSA modulus sizes less than 1024-bits (i.e., 512-bits and 768-bits DSA)
- DES and DES MAC

The ATR value returned by the module during power-up serves as an Approved mode indicator. The ATR returned by Sm@rtCafé Expert 3.2 , version CPDHxJC_RSEFI-025CC073V202 is:
ATR = 3B 74 18 00 00 73 66 74 65

The ATR returned by Sm@rtCafé Expert 3.2 ,version CPDIxJC_RSEFI-025CD080V402 is:
ATR = 3B 7A 18 00 00 73 66 74 65 2D 63 64 30 38 30

The ATR returned by Sm@rtCafé Expert 3.2, version CPDYxJC_RSEFI-025CD144V503 is:
ATR = 3B 7A 18 00 00 73 66 74 65 20 63 64 31 34 34

The value returned by the module after sending the Get Data command: **80 CA DF 7C 49** serves as an Approved mode indicator.

The response to Get Data in the approved mode returned by Sm@rtCafé Expert 3.2 , version CPDHxJC_RSEFI-025CC073V202 is:

Response (the last bits): 0C 08 00 00 6F FD 00 00 00 00 90 00

The response to Get Data in the approved mode returned by Sm@rtCafé Expert 3.2 , version CPDIxJC_RSEFI-025CD080V402 is:

Response (the last bits): 0C 08 00 00 6F FD 6F FD 00 00 90 00

The response to Get Data in the approved mode returned by Sm@rtCafé Expert 3.2 , version CPDYxJC_RSEFI-025CD144V503 is:

Response (the last bits): 0C 08 00 00 6F FD 6F FD 00 00 90 00

5. SECURITY RULES

5.1 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	> 1:2 [112] Due to the communication delay involved with the authentication process, no more than 60 attempts can be made per minute to authenticate to the module.
PIN	2^{48}; A counter can be used in order to limit the number of bad attempts and reduce the risk of attacks (velocity checking). This counter is decremented by 1 at each unsuccessful authentication. With an attempt counter of 15, probability that a random attempt in 1 minute succeeds is much less than 1/100,000. The maximum value of the counter is 15; so no more than 15 attempts can be made in a minute before the PIN is blocked.
PUK	2^{64}; A counter can be used in order to limit the number of bad attempts and reduce the risk of attacks (velocity checking). This counter is decremented by 1 at each unsuccessful authentication. With an attempt counter of 15, probability that a random attempt in 1 minute succeeds is much less than 1/100,000. The maximum value of the counter is 15; so no more than 15 attempts can be made in a minute before the PUK is blocked.

Table 6 Strength of authentication mechanisms

5.2 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Crypto Officer	All CO Services as listed in Section 3.2.1 and 3.3.2
Application Operator	Only User Services as listed in Section 3.3.2
CardHolder	Only User Services as listed in Section 3.3.2

Table 7 Services authorized for roles

5.3 ACCESS RIGHTS WITHIN SERVICES

CSP	Service	Role	Types of Access
TRIPLE-DES CO keys: K_{ENC}, K_{MAC}, K_{KEK}, K_{Token}, $K_{Receipt}$	PUT KEY command	Crypto Officer	Write
TRIPLE-DES CO Keys: K_{ENC}, K_{MAC}	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Execute
TRIPLE-DES CO Key: K_{KEK}	PUT KEY, PIN CHANGE/UNBLOCK commands (encryption of the loaded Key or PIN)	Crypto Officer	Execute
TRIPLE-DES CO Session Keys: K_{SENC}, K_{SMAC}	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Create
TRIPLE-DES CO Session Key: K_{SENC}	Message encryption	Crypto Officer	Execute
TRIPLE-DES CO Session Key: K_{SMAC}	Message integrity	Crypto Officer	Execute
TRIPLE-DES User Keys: SDK_{ENC}, SDK_{MAC}, SDK_{KEK}, K_{DAP}	PUT KEY command	User	Write
TRIPLE-DES XAUT keys	PUT KEY command	Crypto Officer	Write
TRIPLE-DES XAUT keys	AC EXTERNAL AUTHENTICATE & GENERAL AUTHENTICATE, RESET RETRY COUNTER commands	Application Operator	Execute
TRIPLE-DES OTP keys	PUT KEY command	Crypto Officer	Write
TRIPLE-DES OTP keys	GENERAL AUTHENTICATE, INTERNAL AUTHENTICATE commands	Application Operator	Execute
TRIPLE-DES User Keys: SDK_{ENC}, SDK_{MAC}	INITIALIZE UPDATE & EXTERNAL AUTH	User	Execute
TRIPLE-DES User Key: K_{SDKEK}	PUT KEY command (encryption of the loaded Key)	User	Execute
TRIPLE-DES User Session Keys: SDK_{SENC}, SDK_{SMAC}	INITIALIZE UPDATE & EXTERNAL AUTH	User	Create
TRIPLE-DES User Session Key: SDK_{SENC}	Message encryption	User	Execute
TRIPLE-DES User Session Key: SDK_{SMAC}	Message integrity	User	Execute
RSA keys	PUT KEY Command	Crypto Officer	Write
RSA keys	PRIVATE SIGN/DECRYPT/ GENERAL AUTHENTICATE Comamnds (for signature,..)	User, No Role	Execute
“GP DAP” TRIPLE-DES Key: K_{DAP}	PUT KEY command	Crypto Officer	Write
“GP DAP” RSA Key: PK_{DAP}	PUT KEY command	Crypto Officer	Write
“GP DAP” TRIPLE-DES Key: K_{DAP}	LOAD command (MAC verification by G&D	Crypto Officer and User	Execute

	Security Domain)		
"GP DAP" RSA Key: PK_{DAP}	LOAD command (MAC verification by G&D Security Domain)	Crypto Officer and User	Execute
Delegated Management TRIPLE-DES key $K_{Receipt}$	PUT KEY command	Crypto Officer	Write
Delegated Management TRIPLE-DES key $K_{Receipt}$	LOAD command	Crypto Officer	Execute
Global PIN	PIN CHANGE/UNBLOCK command	Crypto Officer	Write
CardHolder PIN	CHANGE REFERENCE DATA	Crypto Officer	Write
CardHolder PIN	VERIFY, CHANGE REFERENCE DATA	User	Execute
PUK	CHANGE REFERENCE DATA	Crypto Officer	Write
PUK	RESET RETRY COUNTER	Application Operator	Execute
TRIPLE-DES DRNG key	INITIALIZE UPDATE command and RSA, DSA key generation	Crypto Officer and User	Execute

Table 7 Access rights within services

6. CRYPTOGRAPHIC KEY MANAGEMENT

The Sm@rtCafé Expert 3.2 with Applets smart card includes the following keys:

- Initialization Key, K_{init} used only for the first Card Manager key-set loading.

- Security Domain (Card Manager and G&D Security Domain) key sets each containing three TRIPLE-DES keys stored in EEPROM. Each key is 112-bits.

    1. K_{enc} used for Cryptographic Officer or User authentication per GP Specification

    2. K_{mac} used for Cryptographic Officer or User authentication per GP Specification

    3. K_{kek} used as Key Wrapping Key for encrypting keys input into the module using the Put Key command

- Secure Channel session keys SMAC and SENC. These are 112-bit TRIPLE-DES keys stored in RAM

- "GP DAP" TRIPLE-DES key, a 112-bit TRIPLE-DES key used for DAP verification using TRIPLE-DES MAC.

- "GP DAP" RSA key, a 1024-bit public key used for DAP verification using RSA signature verification.

- TRIPLE-DES DRNG key used with FIPS140-2 approved ANSI X9.31 DRNG **[X9.31]** is generated using Hardware Random Generator of chip during initialization.

- Delegated Management 1024-bit RSA key K_{Token} for Token verification to check if Delegated Management command is authorized by Crypto Officer.

- Delegated Management 112-bit TRIPLE-DES key $K_{Receipt}$ for Receipt generation to prove successful execution of Delegated Management command.

- External Authenticate 112-bit or 168-bit key (maximum number is 8) to authentication of the off card application to the card

- Secret Key for OTP 112-bit or 168-bit key

- RSA Public and Private keys for Authentication, Digital Signature, Decrypt, Backup encryption key…

All keys can be zeroized by setting the card state to TERMINATED.

7. STANDARDS-BASED CRYPTOGRAPHY

The Sm@rtCafé Expert 3.2 module implements strong, standards-based cryptography. It includes the following FIPS-approved algorithms:

- Triple-DES (3 key TRIPLE-DES) (ECB and CBC modes)
- AES (128, 192, 256-bit key sizes) (ECB and CBC modes)
- SHA-1
- SHA-256
- DSA
- RSA CRT
- RSA Sign/Verify

Deterministic Random Number Generation:

- DRNG based on ANSI X9.31 [X9.31] Appendix A.2.4

7.1 Non FIPS-approved algorithms

- DSA modulus sizes less than 1024-bits (i.e., 512-bits and 768-bits DSA)
- DES and DES MAC

7.2 Self-Tests

The Sm@rtCafé Expert 3.2 runs startup and conditional self-tests to verify that it is functioning properly. These startup self-tests are performed before the module processes the first command it receives after a Reset. Conditional self-tests are executed whenever specific conditions are met.

7.2.1 Power-Up Self Tests

The self-tests include:

Software Integrity Tests: The module checks the integrity of its firmware:
ROM: 16 bit hardware CRC
Firmware in EEPROM: 16 bit hardware CRC
Java Code in EEPROM: 16 bit hardware CRC
Cryptographic Algorithm KATs: Known Answer Tests (KATs) are run at power-up for the following algorithms:

Triple-DES KAT
Triple-DES MAC KAT
AES KAT
DSA Sign/Verify test
SHA-1 KAT
SHA-256 KAT
RSA Sign/Verify KAT
RSA CRT KAT
ANSI 9.31 Software RNG KAT

7.2.2 Conditional Tests

Conditional RSA Pairwise Consistency Check: After generating an RSA key pair, the module performs a sign/verify with that key pair to ensure that the key pair is correct.
Conditional DSA Pairwise Consistency Check: After generating a DSA key pair, the module performs a sign/verify with that key pair to ensure that the key pair is correct.
Continuous RNG test: On every output generated by ANSI X9.31 and hardware RNG the module performs a comparison with previously generated random block. The 8 first bytes generated by the ANSI X9.31 DRNG and the hardware RNG are only used for doing this continous comparison and never used for any service like cryptographic calculations. If generated numbers are equal to previous generated numbers, this selftest fails.

If any of these self-tests fail, the module will halt all operations until it is reset.

If module fails a self-test, the module sends the self-test failure indicator and enters the error state. No further communication is possible with the module until it is removed from the terminal and re-inserted or terminal resets the module.

Software/Firmware Load Test: A TRIPLE-DES CBC MAC on the applet Load File is verified whenever an applet is loaded onto the cryptographic module since applet loading always takes place within a Secure Channel. If Security Domain Applet with mandated DAP privilege is installed and the DAP signature verification key is set in this Security Domain, every Package loaded onto the Card has to provide a DAP value (TRIPLE-DES MAC or RSA Signature), which is verified using the K_{DAP} or PK_{DAP}, respectively.
If TRIPLE-DES MAC or DAP verification fails, package load is terminated. For more details see GP 2.1.1 **[GPCS]**.

8. MITIGATION OF ATTACKS

The module implements countermeasures for three attacks commonly used against smart cards: simple power analysis (SPA), differential power analysis (DPA), and timing analysis. These attacks work by monitoring the power consumption (SPA, DPA) or timing of operations during cryptographic processing in order to gain information about sensitive content, such as secret keys.

The module's IC has a co-processor for performing DES and Triple-DES operations. This co-processor was specifically designed by NXP to counter SPA, DPA, and timing analysis attacks. G&D has conducted testing of the module's DES and Triple-DES processing for resistance to these attacks and found that no information was leaked during this processing via these attacks.

The module's RSA implementation has been hardened against SPA, DPA, fault and timing analysis using a variety of techniques. For timing analysis, the timing of the RSA implementation does not correlate to the inputs to the implementation. To counter SPA, conditional jumps based on the exponent and squares were avoided. Randomization of the base and exponent is employed to counter DPA. G&D has conducted testing of the module's RSA processing for resistance to these attacks and found that no information was leaked during this processing via these attacks.

9. SECURITY POLICY CHECK LIST TABLES

9.1 Roles and Required Authentication

Role	Type of authentication	Authentication data
Card Security Controller	GP secure channel mutual authentication protocol	GP secure channel TDES key set of three
Application Operator	AC External Authenticate protocol	Application XAUT TDES key
Card Holder	Verify service	PIN

9.2 Strength of authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
TDES authentication	> 1:2 ^{112} Due to the communication delay involved with the authentication process, no more than 60 attempts can be made per minute to authenticate to the module.
PIN	2^{48};

	With an attempt counter of 15, probability that a random attempt in 1 minute succeeds is much less than 1/100,000. The maximum value of the counter is 15; so no more than 15 attempts can be made in a minute before the PIN authentication is blocked.
PUK	2^{64}; With an attempt counter of 15, probability that a random attempt in 1 minute succeeds is much less than 1/100,000. The maximum value of the counter is 15; so no more than 15 attempts can be made in a minute before the PUK authentication is blocked.

9.3 Services authorized for Roles

Role	Authorized Services
Card Security Controller	The Card Security Controller role services are listed in Section 3.3
Application Operator	The Application Operator role services are listed in Section 3.3
Card Holder	The Card Holder role services are listed in Section 3.3

9.4 Access Rights within Services

Service	CSP	Types of Access (i.e. Read, Write, Execute)
CSC (CSC) Service	GP secure channel TDES key set of three (K_{enc}, K_{Mac}, K_{Kek}), or Unblock PIN XAUT TDES key as well as , Create/Update PIN/PUK	Execute (encrypt, decrypt, update PUK), write (put key, create PIN/PUK)
Application Operator Service	Application XAUT TDES key or Unblock PIN with PUK	Execute (encrypt, decrypt, unblock with PUK)
Card Holder Service	PIN	Execute (Verify), write (Change Reference Data)

9.5 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
Timing Analysis	Counter Measures against Timing Analysis	N/A
Differential Fault Analysis	Counter Measures against Differential Fault Analysis	N/A

10. ACRONYMS

ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
ATR	Answer-To-Reset
CBC	Cipher-Block Chaining
CSC	Card Security Controller
CSP	Critical Security Parameter
CO	Crypto Officer
CRT	Chinese Remainder Theorem
Dap	Data Authentication Pattern
DES	Data Encryption Standard
DPA	Differential Power Analysis
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMV	Europay Mastercard and Visa
EEPROM	Electrically Erasable Programmable ROM
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
G&D	Giesecke & Devrient
GHC	Generalized Hamming Code
I/O	Input/Output
IC	Integrated Circuit
ISO	International Organization for Standardization
JCRE	Java Card ™ Runtime Environment
KAT	Known Answer Test
MAC	Message Authentication Code
MD5	Message Digest algorithm 5
N/A	Not Applicable
NIST	National Institute of Standards and Technology
GP	GlobalPlatform
PIN	Personal Identification Number
PIV	Personal Identification Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
DRNG	Deterministic Random Number Generator
PUK	Pin Unblocking Key
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir and Adleman
RST	Reset

SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
XAUT	External Authentication