Cryptographic Module Security Policy

for

jNet Citadel-OS on Atmel AT90SC144144CT

Document Version 1.1

February 22, 2007

Prepared by:

jNet Technology, Inc.
560 South Winchester Blvd., Suite 500
San Jose, CA 95128

Proprietary Notice

Glossary

• TDES	Triple DES
• AES	Advanced Encryption Standard
• AID	Application Identifier
• AP	Application Provider
• APDU	Application Protocol Data Unit
• API	Application Programming Interface
• ATR	Answer To Reset (contact mode)
• CBC	Cipher Block Chaining
• CRC	Cyclic Redundancy Check
• DAP	Data Authentication Pattern
• DES	Data Encryption Standard
• DPA	Differential Power Analysis
• DRNG	Deterministic Random Number Generator
• ECB	Electronic Code Book
• EEPROM	Electrically Erasable and Programmable Read Only Memory
• EMI	Electromagnetic Interference
• ISO	International Standard Organization
• MAC	Message Authentication Code
• NDRNG	Non Deterministic Random Number Generator
• OP	Open Platform
• PIN	Personal Identification Number
• PKCS	Public Key Cryptographic Standards
• RAM	Random Access Memory
• ROM	Read only Memory
• RSA	Public key cryptographic algorithm invented by Rivest, Shamir and Adleman
• SHA-1	Secure Hash Algorithm
• SPA	Simple Power Analysis

1. Introduction

1.1. Purpose

This document describes the Security Policy implemented by the Citadel-OS cryptographic module submitted for validation in accordance with FIPS140-2 Level 3 standard. Included are the description of the security requirements for the module and a qualitative description of how each security requirement is achieved.

1.2. Scope

The Cryptographic Security Policy specifies the security rules under which the cryptographic module operates. It does not describe the requirements for the entire system.

1.3. References

- Atmel Corporation, SecureAVR AT90SC144144C Specification, June 2004
- National Institute of Standards and Technology (NIST), FIPS Pub 46-3, Data Encryption Standards, October 25, 1999.
- National Institute of Standards and Technology (NIST), FIPS Pub 140-2, Security Requirements for Cryptographic Modules, May 25, 2001.
- National Institute of Standards and Technology (NIST), FIPS Pub 186-2, Digital Signature Standard (DSS), January 27, 2000.
- RSA Security Inc, Public-Key Cryptographic Standard PKCS #1, Version 2.1, June 14, 2002.

1.4. Module Overview

The Citadel-OS device is based on Atmel SecureAVR product family. It is shown in Figure 1 and is a single-chip cryptographic module (HW P/N AT90SC144144CT, Version AdvX V01.01; FW Version 1.0). The cryptographic core is defined when the CPU executes instructions at the privileged level and has exclusive access to all available resources.

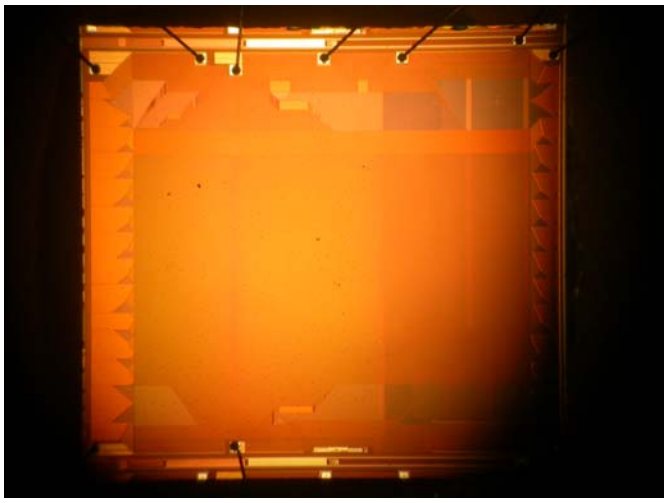

Figure 1. Atmel's AVR AT90SC144144CT single chip.

Table 1. Pin assignments for AVR device.

Pad Name	Description	Logical Interface
P1	Vcc supply voltage 3 to 5V +/- 0.5V	Power Input
P2	RST (Reset)	Control Input
P3	CLK (Clock)	Control Input
P4	Reserved for Future Use (RFU)	Not Connected
P5	GND (Ground)	Power Input
P6	Not used	Not Connected
P7	I/O bi-directional line	Data Input / Output, Control Input, Status Output
P8	Reserved for Future Use (RFU)	Not Connected

1.4.1. Power Interface

The Citadel-OS crypto module obtains all of its power requirements from external sources. The Vcc power is used by the internal (on-chip) power regulator and to supply power to some of the I/O pins. In the ISO 7816 smart module configuration, Vcc is provided on P1 and ground on P5.

1.4.2. Cryptographic Module Specification

The primary purpose of the Citadel-OS module is to provide a platform for a native, privileged application to perform on-device cryptographic operations in a FIPS 140-2 compliant runtime environment. The Citadel-OS module supports standard RSA, SHA-1, AES and TDES algorithms. The module security comes from both firmware and hardware. Data integrity and security are provided through cryptographic services and the defensive nature of the Citadel-OS implementation. In addition, the cryptographic module hardware provides tamper-resistance and tamper-evidence features, that meet FIPS 140-2 Level 4 physical security requirements. However, it shall be noted that FIPS 140-2 validation does not include any privileged applications.

1.4.2.1. Atmel Secure ICs: SecureAVR AT90SC144144C

The SecureAVR is a low-power, high-performance secure microcontroller family with programmable Flash code memory, Eeprom data memory and a crypto-processor based on AVR RISC architecture. By executing powerful instructions in a single clock cycle, the AVR device can achieve throughputs close to one MIPS per MHz. Its Harvard architecture supports 32 general-purpose registers directly connected to the ALU, allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

This chip uses the new AVR core that allows linear addressing of up to 8 M bytes of code and up to 16 M bytes of data as well as a number of new functional and security features. The AT90SC144144C includes 144K bytes of Atmel's high density, nonvolatile Eeprom memory. The

on-chip downloadable code flash on AT90SC144144C allows the program memory to be downloaded post issuance.

The crypto engine featured in the AT90SC-XXX series has a high-performance 16-bit processor dedicated to perform fast encryption or authentication functions. Additional security features include power and frequency protection logic, logical scrambling on program data and addresses, differential power and timing analysis countermeasures and memory access controlled by a supervisor mode.

1.4.2.2. Crypto Module Architecture

The Citadel-OS cryptographic module allows for two-factor authentication of a personal security device to application infrastructures supporting them. The protocol uses strong cryptographic algorithms (TDES) for authentication and critical data integrity checking.

The cryptographic module consists of a combination of firmware and hardware to support an environment for secure execution. The AT90SC144144CT executes its code out of flash and CRC16 program integrity check is performed on code flash contents before entering an operational mode. The contents of various key sets and critical security parameters are stored in 144K bytes of available EEPROM with each data structure having a validation field (CRC16) that is checked for consistency before each use. The validation field CRC16 is recomputed after any write access to a data structure.

If additional applications are added to this module, then these additional applications will need to go through a separate FIPS 140-2 validation. The "cryptographic boundary" for the Citadel-OS module vis-à-vis the FIPS 140-2 validation is solely comprised of the chip (ICC).

1.4.3.jNet Native Citadel-OS Runtime Environment

jNet Citadel-OS is developed on top of Atmel SecureAVR core. Each of the on-module cryptographic algorithms including DRNG, TDES, SHA-1, AES and RSA has been individually validated for compliance with FIPS requirements [FIPS140-2 Appendix A, FIPS140-2 Appendix C].

The FIPS-approved mode is the standard operational mode for the Citadel-OS crypto module. The lifecycles and state transitions follow industry standard implementations specified in Global Platform documentation, version 2.0.1. The Global Platform specification defines module and application life cycle states and state transitions.

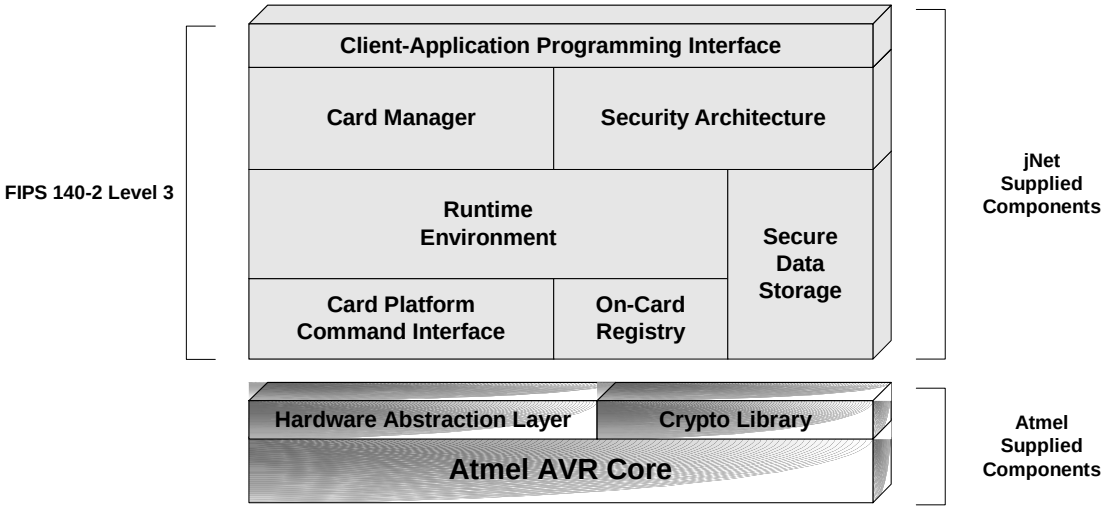

Figure 2. High-level architecture of Citadel-OS module.

1.4.4. Interface Security

At no time are private and secret keys, authentication data, or CSPs imported or exported in plaintext. The dedicated path is available by means of Global Platform Secure Channel. At start-up, the ISO 7816 interface is established as the communication channel with the host for the duration of the session. During a session, all logical paths are carried on the chosen physical path. The interface with the host computer is a command-response interface, where all communication with the host are inhibited until a command is executed. In particular, a command to generate a key or key pair causes communication with the host to be suspended until the key generation is either completed successfully or aborted. At the conclusion of most operations, a response message is returned to the host containing only the return status code.

1.4.5. Interface Mapping

The logical interfaces are mapped to the physical port in the following manner:

- Data input → Command Interface (P7) → ISO 7816
- Data output →Command Interface (P7)→ ISO 7816
- Control input → Command Interface (P7) → ISO 7816
- Status output → Command Interface (P7) → ISO 7816

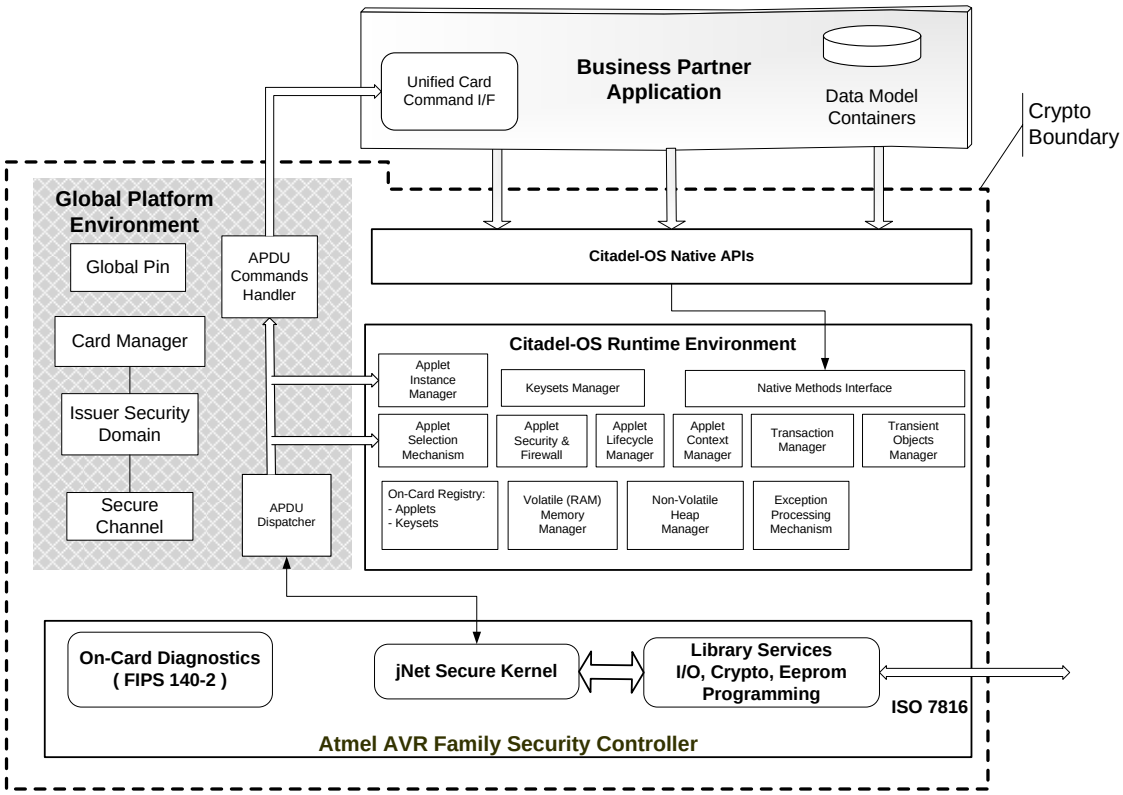

Figure 3. Detailed architecture of Citadel-OS crypto module with FIPS 140-2 validation scope (crypto-boundary) outlined with a dashed line.

1.4.6. Card Cryptographic Functions

The purpose of the cryptographic module is to provide a FIPS approved platform for applications that may in turn provide cryptographic services to end-user applications. The keys represent the identity of the roles involved in controlling the module. A variety of FIPS 140-2 validated algorithms are used in the Citadel-OS to provide cryptographic services.

Some of these cryptographic services are made available only to applications via internal APIs. Since the module described in this security policy does not include any instantiated applications some security services may not be available to any operator of the module. They are however listed here in italic font to inform applet developers of all cryptographic services built into the module.

The cryptographic functions provided by the Citadel-OS include:

- *TDES, (2 keys TDES) [Certificate # 437]: The TDES (ECB and CBC modes) algorithm is used*:
    - for authenticating the operator
    - for encrypting data flow from the off module to the on-module environment. The reverse direction is not encrypted; i.e. the status words returned in response to an APDU are not encrypted.
    - as a TDESMAC to verify the integrity of the message
    - TDES functions (CBC and ECB) are also provided as services to application, through APIs. These services are not available to any of the current operators of the module.
- *AES (ECB and CBC modes) [Certificate #399]: The AES function (CBC) is provided as a service to applications through an internal APIs.*
- *SHA-1 [Certificate #470]: The SHA-1 function is provided as a service to applications through an internal APIs.*
- *RSA (up to 2048 bit keys) [Certificate #144]: RSA signature generation and verification functions are provided as services to applications through internal APIs.*
- *DRNG ANSI X9.31 [Certificate #214]*

AES, TDES, RSA, SHA-1 algorithms are provided as services to applications that may be loaded onto the Citadel-OS module during future validations.

The module also implements the following non-Approved algorithm:

- *NDRNG*

2. Security Level

The Citadel-OS cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2, as shown in Table 2. The individual security requirements specified for FIPS 140-2 meet the level specifications indicated in the following table.

Table 2. Module security levels specifications.

Security Requirements	Level	Comment
Cryptographic Module Specification	3	
Module Ports and Interfaces	3	
Roles, Services and Authentication	3	
Finite State Model	3	
Physical Security	4	
Operational Environment	N/A	
Cryptographic Key Management	3	
EMI/EMC	3	
Self-Tests	3	
Design Assurance	3	
Mitigation of Other Attacks	3	

2.1 Approved Mode of Operation

The module's normal mode of operation is always a FIPS 140-2 approved mode. The design decisions were made to use only FIPS-approved crypto algorithms when providing services to Crypto Officer or User/Application Developer. The internal code also prevents non-authorized use of cryptographic keys in operations for which they were not intended.

2.1.1 Card's ATR string

The ATR string is as follows, where the version numbers for applications are integrated into an ATR string as seen below. The module operator can determine if he has a correct hardware and firmware by examining the ATR string. It is sent after the module is RESET. For this product it must be as follows to indicate to the operator that the module is in an approved mode:

3B5E11FF6A4E 65742E3134312E01002E0100

Here the historical bytes represent a text string with OS version being 01.00 and 01.00. The string "144" represents an Atmel's AT90SC144144 part of the ATR. The first byte is a major version, second is a minor version. Here is the actual string: "jNet.144.0100.0100"

3. Identification and Authentication Policy

Table 3. Shows the roles that are supported by the Citadel-OS cryptographic module.

Role	Identification	Authentication
User/Application Developer - This role is assumed to perform application development & integration with Citadel-OS. All management functions such as module initialization and key loading are supported in this role.	The identity of the User/Application Developer is specified by providing the Application Developer's key set ID.	INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands used prove knowledge of a TDES key set.
Cryptographic Officer (CO) - This role is assumed to perform cryptographic initialization or a management function such as module initialization, loading of cryptographic keys and CSPs	The identity of the Cryptographic Officer is specified by providing the Cryptographic Officer's key set ID.	INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands used to prove knowledge of a TDES key set.

3.1 Approved Mode of Operation

The Citadel-OS module's normal mode of operation is always a FIPS 140-2 approved mode. No other mode of operation exists when a card containing Citadel-OS module has been issued an application developer. The design decisions were made to use only FIPS-approved crypto algorithms when providing services to either the User or Crypto Officer. The reasons behind this approach were to simplify usage and deployment, application development and streamline the validation phase.

4. Access Control Policy

4.1 Roles & Services – FIPS 140-2 Services

Table 4. Services authorized by roles.

Service Type	Function	Unauthenticated (No Role)	User	Crypto Officer
SELECT	Selects an application. All commands received from terminal are forwarded to a selected application.	**X**	**X**	**X**
INITIALIZE UPDATE	Performs a cryptographic operation by following an authentication protocol using data provided in the data field of the command and returns the result of the cryptographic operation in the response data field.	**X**	**X**	**X**
EXTERNAL AUTHENTICATE	Used to authenticate the host and determine the level of security required for all subsequent commands.		**X**	**X**
INSTALL	Issued to instantiate an instance of already integrated application in code space (ROM or flash). Requires a secure channel.		**X**	**X**
DELETE	Deletes a uniquely identifiable application instance such as an instance of PIV application.		**X**	**X**
PUT KEY	Zeroizes or adds a new key or multiple keys to a key set. Requires secure channel.		**X**	**X**
PIN CHANGE / UNBLOCK	Resets the retry counter for the PIN to its initial value and initializes the Global PIN with provided data.		**X**	**X**

Service Type	Function	Unauthenticated (No Role)	User	Crypto Officer
GET STATUS	Retrieves status on package and/or application based on provided AID.		**X**	**X**
SET STATUS	Modifies the module Life Cycle State or the Application Life Cycle State.		**X**	**X**
GET DATA	Retrieves data content of the single data object whose tag is provided in a data field. No CSP services are available.	**X**	**X**	**X**
PUT DATA	Replaces data content of a single data object in a module application with new content.		**X**	**X**

4.2 Cryptographic Keys & Critical Security Parameters

Table 5-a. Non-volatile Cryptographic Keys contained in the module. Note: Modules are shipped with CO key set (these include Kco_{enc}, Kco_{mac}, Kco_{kek})already installed.

Key Name	Abbreviation	Description
Crypto Officer Encryption Key	Kco_{enc}	This is a TDES key. It is used for Crypto Officer's encryption session key generation during secure channel setup via INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands.
Crypto Officer Message Authentication Key	Kco_{mac}	This is a TDES key. It is used for generation of MAC session keys for Crypto Officer.
Crypto Officer Key Encryption Key	Kco_{kek}	This is a TDES key. It is used to unwrap the inbound key set for the Crypto Officer.
Internal Encryption Key	K_{ikek}	This is a TDES key. It's unique for every application and it used to encrypt/decrypt the Crypto Officer's keys when stored or retrieved to/from Eeprom. This key is generated during application instantiation and is zeroized when an application is DELETED
User Encryption Key	Ku_{enc}	This is a TDES key. It is used to generated User's encryption session key during secure channel setup via INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands. This key is

Key Name	Abbreviation	Description
		loaded/zeroized via the PUT KEY command.
User Message Authentication Key	Ku_{mac}	This is a TDES key. It is used for generation of MAC session keys for User / Application developer. This key is loaded/zeroized via the PUT KEY command.
User Key Encryption Key	Ku_{kek}	This is a TDES key. It is used to unwrap inbound key set for User. This key is loaded/zeroized via the PUT KEY command.

Table 5-b. Volatile Cryptographic Session Keys contained in the module.

Key Name	Abbreviation	Description
Crypto Officer Encryption Session Key	$S\text{-}Kco_{enc}$	This is a TDES key. It is used to encrypt/decrypt data input during secure channel operation and is generated using the INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands. This key is zeroized at the closure of the Secure Session.
Crypto Officer Message Authentication Session Key	$S\text{-}Kco_{mac}$	This is a TDES key. It is used during MAC computation/verification and authentication of the Crypto Officer. This key is zeroized at the closure of the Secure Session.
User Encryption Session Key	$S\text{-}Ku_{enc}$	This is a TDES key. It is used to encrypt/decrypt data input during secure channel operation and is generated using the INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands. This key is zeroized at the closure of the Secure Session.
User Message Authentication Session Key	$S\text{-}Ku_{mac}$	This is a TDES key. It is used during MAC computation/verification and authentication of the User. This key is zeroized at the closure of the Secure Session.

Table 6. Critical Security Parameters in Citadel-OS module.

Security Parameter	Abbreviation	Description
Global PIN	GPIN	This is a PIN object associated with the Global Platform specification. It's presented in encrypted fashion using the authenticated PIN CHANGE UNBLOCK command via Secure Channel. Its reference value is 0x00. This PIN is not used by the module for authentication purposes. The Global PIN is zeroized via the PIN CHANGE/UNBLOCK command.

Table 7. Access rights within services with supported operational modes for each service type.

Service Type [Operational mode]	**Cryptographic Keys & CSPs**	**Roles**
INITIALIZE UPDATE	Kco_{enc} Kco_{mac} Ku_{enc} Ku_{mac}	Used for generation of session keys to setup secure channel (Kco_{enc} or Ku_{enc}) and authenticate its message contents (Kco_{mac} and Ku_{mac})
EXTERNAL AUTHENTICATE	Kco_{enc} Kco_{mac} Ku_{enc} Ku_{mac} $S\text{-}Kco_{enc}$ $S\text{-}Kco_{mac}$	Used for generation of session keys to setup secure channel (Kco_{enc}) and authenticate its message contents (Kco_{mac}).
INSTALL	$S\text{-}Kco_{enc}$ $S\text{-}Kco_{mac}$	The Secure Channel must be set up prior to performing the INSTALL command.
PUT KEY	Kco_{kek} Ku_{kek}	The Kco_{kek} key is used for decrypting all TDES keys delivered to Card Manager through Secure Channel. The Ku_{kek} key is used for encrypting all TDES keys delivered to the Security Domain of the User/Application Developer. When being stored in Eeprom, the K_{ikek} key is used for

Service Type [Operational mode]	**Cryptographic Keys & CSPs**	**Roles**
	K_{ikek} S-Kco_{enc} S-Kco_{mac}	encrypting TDES keys before writing.
PIN CHANGE / UNBLOCK	Kco_{kek} Ku_{kek} S-Kco_{enc} S-Kco_{mac} S-Ku_{enc} S-Ku_{mac} GPIN	Since PIN is always presented in encrypted fashion to the card, the Kco_{kek} key is used during this service to decrypt GPIN's contents for comparison. Global Platform PIN-related APDU command.
DELETE	S-Kco_{enc} S-Kco_{mac} S-Ku_{enc} S-Ku_{mac}	The Secure Channel must be set up prior to performing DELETE command.
GET STATUS	S-Kco_{enc} S-Kco_{mac} S-Ku_{enc} S-Ku_{mac}	The Secure Channel must be set up prior to performing GET STATUS command.
SET STATUS	S-Kco_{enc} S-Kco_{mac} S-Ku_{enc} S-Ku_{mac}	The Secure Channel must be set up prior to performing SET STATUS command.
GET DATA	S-Kco_{enc} S-Kco_{mac}	The Secure Channel must be set up prior to performing GET DATA command.

Service Type [Operational mode]	**Cryptographic Keys & CSPs**	**Roles**
	S-Ku_{enc} S-Ku_{mac}	
PUT DATA	S-Kco_{enc} S-Kco_{mac} S-Ku_{enc} S-Ku_{mac}	The Secure Channel must be set up prior to performing PUT DATA command.

.

5. Security Rules

This section documents the security rules enforced by the Citadel-OS crypto module to implement the security requirements of a FIPS 140-2 Level 3 device.

5.1 Identification and Authentication

The Cryptographic Officer (CO) must prove to have the TDES key set stored in the Citadel-OS module associated with the Card Manager. Through the INITIALIZE UPDATE and EXTERNAL AUTHENTICATE command pair, the CO and Citadel-OS module will mutually authenticate each other. The same applies to User/Application Developer. The authenticated login either by the CO or by User/Application Developer is invalidated upon reset or power cycle of the module.

Table 8. Roles and Authentication Mechanisms

Role	Authentication Mechanism	Strength of Authentication Mechanism
Crypto Officer	Secure Channel based on TDES session keys with TDES MAC	2^80
User /Application Developer	Secure Channel based on TDES session keys with TDES MAC	2^80

5.2 Access Control Security

- Keys must be loaded over a secure channel established by the operator. The keys must be wrapped with either the Kco_{kek} or Ku_{kek}
- The Global Platform PIN can only be loaded over an encrypted secure channel and is wrapped with Kco_{kek} or Ku_{kek}.

5.3 Cryptographic Keys & Card Holder PIN Contents Destruction

All cryptographic session keys in the module used for Secure Channel operation are automatically zeroized by the Security Domain code (set to value of zero) upon closing of the Secure Channel. The Crypto Officer or User/Application Developer keys sets are destroyed (set to Eeprom's default value of 0xFF) upon hardware detection of any chip tampering either through micro-probing or FIB. The same applies to the Global PIN value which is also zeroized by underlying hardware circuitry.

6. Physical Security

6.1 Physical Security Mechanisms

The Citadel-OS cryptographic module includes the following physical security mechanisms:

- Environmental failure protection (EFP) features for temperature, voltage, internal clock frequency, and duty cycle are provided by immediate reset circuitry.
- The removal-resistant coating with hardness and adhesion characteristics covers the single-chip cryptographic module, and attempts to peel or pry the coating from the module results in irreparable damage to the module.
- The shield removal detection circuitry results in reset upon an attempt to remove the metal coating from the unit.

6.1.1 Temperature Environmental Failure Protection

The temperature variations attack is a type of fault induction attack that utilizes temperature manipulation to cause processing errors within the cryptographic module. An analysis of these errors and their patterns using cryptographic module, can sometimes reveal certain features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys. The Citadel-OS employs the temperature variations detector to defend against such attacks by causing a reset when temperature goes outside specified operating norms.

6.1.2 Abnormal Voltage Failure Protection

The Voltage Attack is a type of fault induction attack that utilizes voltage manipulation to cause processing errors within the cryptographic module. The analysis of these errors and their patterns is an attempt to reveal certain features and implementations of cryptographic algorithms and, subsequently, discover the values of cryptographic keys. The Citadel-OS protects against the threat of voltage induced failure attacks using a built-in abnormal voltage detector available on SecureAVR cores.

6.2 Physical Attacks

This section details the physical attacks which have been considered as part of this vulnerability analysis and documents the methods used to provide protection against them. Physical attacks are defined here as those which involve invasive manipulation of the device by external means such as microprobing or deprocessing. Each subsection details a physical attack and then defines the security features that are used to prevent this type of attack.

6.2.1 Probing, Observation and Modifying Internal Signals

The success of this type of attack is dependent on both the device manufacturing process and the security features incorporated into the devices.

- The AT90SC families fabrication process is planarised, thus making it more difficult to identify the circuits. This also makes it more difficult to reverse engineer the devices.
- The devices use standard cells allowing auto place and route, which also makes it difficult to identify the circuit. This feature also makes it more difficult to reverse engineer the devices.
- Certain features of this device are protected by a security erase of the NVMs. Where this is the case upon detection of attack, the NVM array is erased, and the device placed in a

continuous reset state. The device may only exit the reset state once the cause of the violation has been removed, and a cold power on sequence has been performed.

- The devices contain a self-protected active anti-tamper barrier that protects the sensitive parts of the circuit from direct probing. When this active barrier is breached a security erase of the NVM occurs and the device is placed in continuous reset condition.
- The address and data bus lines of the memory modules are encrypted. This makes it more difficult to read the desired information.
- The keys for the AVR ROM and Crypto ROM can be varied between different embedded applets.
- The AVR ROM, the Crypto ROM and the RAM encryption are not affected by the NVM key. To alter this key successfully an attacker must be able to modify the values of these protected bytes very precisely as they are signed when programmed. Should the stored sign value not match the value calculated during power on the device shall not exit reset.
- Modifying the NVM key successfully is unlikely to benefit an attacker as the NVM contents will be scrambled differently and thus the information will not be of use.
- For Flash devices: Modifying the NVM key successfully will not benefit an attacker as the NVM contents will be scrambled differently and thus the info, both EEPROM data and application code will not be of use.
- The analysis of the devices using E-beam testers is countered by the possibility of having an internal jittered clock for both the AVR and the crypto-processor, which will blur the images. In addition to this, the active shield will prevent the attacker from obtaining an image from the lower metal layers.
- The analog security cells connection is protected by a challenge/answer dynamic protocol on Power on Reset that will trigger if an attacker tries to disconnect the outputs of these cells.

6.2.2 Reading of Memory Contents

The following security features are used to combat against attacks, which attempt to read the contents of the AVR ROM, EEPROM, RAM or Crypto ROM modules.

- The address and data bus lines are divergent and "buried".
- The ROM/Crypto ROM memories used where present are implanted rather than active.
- Although it is possible to reveal the physical contents of a ROM, it is not possible to read the contents of the AVR ROM directly (where present), as the data held in the AVR ROM is scrambled and the memory itself is scrambled, which means that consecutive addresses in the AVR ROM are not consecutive addresses in the memory map.
- Although it is possible to reveal the physical contents of a ROM, it is not possible to read the contents of the Crypto ROM (where present) directly, as the data held in the Crypto ROM is scrambled and the memory itself is scrambled, which means that consecutive addresses in the Crypto ROM are not consecutive addresses in the memory map.
- It is not possible to read the contents of the NVM and RAM memories since this would mean using probing techniques, which are countered by the active barrier.
- The address and data bus lines of the AVR ROM, RAM, EEPROM, Flash and Crypto ROM are encrypted, which makes it more difficult to read the desired information.
- The AVR ROM, the Crypto ROM and the RAM encryption are not affected by the NVM key.
- Modifying the NVM key successfully is unlikely to benefit an attacker as the NVM contents will be scrambled differently and thus the information will not be of use. Furthermore the application should be designed so that NVM bytes are checked for integrity.

- The embedded software can further enhance the scrambling feature on very sensitive data by using the RNG module and/or the cryptographic modules during the card personalization to ensure that all devices have this sensitive data scrambled differently.

7. Mitigation of Other Attacks

7.1 Non Invasive Attacks

This section details the non-invasive attacks that have been considered. Each subsection details a non-invasive attack and then defines the security features that are used to prevent this attack.

7.1.1 UV Light Attacks

An attacker may decide to attempt to modify the NVM contents by exposing them to ultra violet light. This involves some initial preparation of the sample by decapsulating it from its module, however the light attack itself requires no tampering with the chip itself.

If light of sufficient intensity is shone for a long enough period on an NVM cell it may be possible to erase it. The device has the following features, which combat against this type of attack.

- The NVM is fully shielded against UV light, and cannot be modified using this kind of attack.
- The devices contain an UV light detector that will trigger when the surface of the chip is submitted to a certain cumulative UV light. Once this kind of attack is detected, the device stays under infinite reset even when the light source is removed.

7.1.2 Fault Induction

A method of gaining information about the operation of a device and software application is to attempt to induce faults in its operation. By successfully altering the normal course of code execution, disrupting memory modifications, or affecting the operation of on-chip peripherals an attacker may reveal something about the embedded application by e.g. introducing small errors in cryptographic calculations or causing software to output data beyond the intended buffer size. This is, for example the basis of Bellcore and DFA attacks.

The following subsections provide information on the different methods which may be attempted in order to induce such faults. The bulleted items below give information on the features and guidance which are provided to counter such threats.

7.1.2.1 Operating outside specified temperature range

If the device is operated outside its specified temperature range, then NVM writes and the operation of security features may be adversely affected. The device contains a high and low temperature detector, which triggers a continuous reset when the device exceeds the specified operating temperature range.

7.1.2.2 Operating outside specified frequency range

A breach of device security may occur if the device is allowed to operate outside its specified frequency range. Information can be read by probing if the device allows slow clock steps to be applied, i.e. after each clock pulse the hacker could potentially read the data by probing. In addition frequency glitches may cause the device to execute different instructions, that are not supported by the CPU or to access unused areas of the memory map leading to unpredictable device behavior which may be exploited.

The device has the following features which combat this type of attacks.

- Low and high frequency detectors are present, which trigger when the device operates outside its specified frequency range. It should be noted that there are two low frequency detectors: one on the ISO clock, and one on the internal clock.
- The clock pad includes a glitch filter that isolates frequency glitches on the external clock from the internal clock.
- The internal clock is generated by an internal Variable Frequency Oscillator (VFO).

7.1.2.3 Operating outside specified voltage range

When the device is operated outside its specified voltage range, operations on the device may be affected.

In addition, fast glitches on the device supply:

a) May cause the device to execute instructions incorrectly, disrupting normal code flow, executing unsupported opcodes or accessing unused areas of the memory map.

- Low and high voltage detectors are present, which trigger when the device operates outside its specified operating voltage range and generate a immediate frozen security reset.
- The device contains an internal voltage regulator this will isolate voltage glitches on the external supply from the internal supply.
- The device contains a dedicated glitch detector which is intended to detect externally applied power glitches, resetting the device. The targeted level of this detector is intended to catch many glitches which would affect the regulated voltage enough to induce errors in operation.

b) The device has the following features, which combat against this type of attack.

- There are specific device features and software techniques which are designed to protect the application should code execution or hardware calculation be disrupted by this method of attack.
- The devices contain NVM charge pumps thus protecting against attacks that deliberately block the NVM erase voltages.
- The Power On Reset (POR) circuitry and the low voltage detectors guarantee that all analogue blocks have stabilized before the device exits from a cold reset.

7.1.2.4 Subjecting device to light pulses

If the device is exposed to light of a sufficient energy, on specific areas or key circuits, the device may execute incorrectly. This threat is countered by:

- Identifying which circuits to target is difficult due to the metal shield
- Further shielding

7.1.3 Security Measures Against Code Execution Corruption

This section details the hardware features and software recommendations available to increase protection against corruption of code execution or hardware calculations by any method e.g. light, voltage or frequency fluctuations.

- Corruption during the fetching of an instruction may result in the execution of an opcode which does not form part of the legal instruction set. In order to protect against this kind of attack, the products contain an illegal opcode detector.

- The FireWall includes an illegal address detector, which triggers when the device accesses an unused area of the memory or when the device accesses a protected area.
- A watchdog circuit is included to prevent program runaway, where an induced fault causes access to legal address space containing valid instructions.
- In addition, the protection provided by the Watchdog is further consolidated by having a feature that sets the SVR1.WDOGVI flag and generates an immediate security reset if a Power Down mode entry SLEEP instruction is executed while the Watchdog is enabled.

7.2 Power and Electromagnetic Analysis – AVR Countermeasures

This section details the hardware features available on the device designed to minimize the probability of successful Power and Electromagnetic attacks on software executing on the device. Power Analysis attacks consist of Simple (SPA) attacks which observe power consumption on individual executions, and Differential (DPA) which perform mathematical processing on a series of power traces to recover leaked information.

- Similarly for ElectroMagnetic Analysis there exists SEMA and DEMA techniques.
- The devices contain an internal voltage regulator.
- The AVR clock system enables the software to use powerful SPA, DPA, SEMA and DEMA counter measures.
- The above clock system counter measures is programmed at random during the software execution by making use of the dummy interrupt.
- The VFO output clock is jittered by random frequency jumps.
- The low-level kernel makes use of the AVR dummy instruction to insert, at random, a number of fake AVR instructions.

7.3 Power and Electromagnetic Analysis – Hardware Protection Features

This section details the additional features available to those using the hardware modules in order to provide further protection against Power and Electromagnetic attacks on their operation.

Hardware DES security features:

- The hardware DES block performs DES calculation in 16 clock cycles. The possibility of success of a DPA or DEMA attack is reduced because all bit manipulations associated with each round of DES occurs simultaneously in 1 clock cycle.
- DES keys are loaded into the Hardware DES registers through a Mask register which is designed to obscure any information leakage during key load.
- DES implementation masks critical information to improve leakage.
- The SPA/SEMA protected mode for the DES key loading in the Hardware DES is also used to enhance the resistance against the SPA/SEMA attack.
- The DES is running on the same clock as the AVR.

Crypto Module and Toolbox Security Features:

Detailed below are the hardware features and software implementations available to the crypto processor, designed to minimize the probability of a successful Power or Electromagnetic Attacks:

- The Crypto-processor clock system enables the software to use powerful SPA / DPA / SEMA / DEMA counter measures.
- The VFO output clock is jittered by random frequency jumps.

- The above clock system counter measures can be programmed at random during the software execution by making use of the dummy interrupt.
- The embedded software makes use of the AVR dummy instruction to insert, at random, a number of fake AVR instructions.

8. Inspection and Testing of Physical Security Mechanism

Only destructive tampering or "most invasive" tampering can breach the physical security mechanisms of the Citadel-OS module. Since most invasive tampering would have the probable result of rendering the Citadel-OS module inoperable, no regular regimen of visual or instrumented inspection is required. The cryptographic module comprises a single integrated circuit chip. Physical or electrical probing would require removal of the chip from the manufacturing layers. This would have the almost-certain affect of rendering the module inoperable. In the unlikely event that the chip was invasively probed without disabling the chip, reassembly of the Citadel-OS without evidence to the casual observer would be extremely difficult.

9. Self-test Specifications

The Citadel-OS cryptographic module uses power-up and conditional self-tests to ensure that the module is functioning properly. The power-up self-tests are initiated automatically, but to meet EMV2000 timing requirements for ATR string transmission, all tests are done on reception of the first APDU command sent to the module after reset. All self-tests must be successfully completed before the module will respond to any commands. The module's power-up self-tests include a known-answer cryptographic algorithm test for each cryptographic function, such as encryption, decryption, authentication, and deterministic random number generation, of each FIPS-approved cryptographic algorithm. The full set of built-in power-up self-tests are conducted. The conditional tests are invoked when the applicable security function or operation is required.

The response to power-on is issuance of the Answer-to-Reset (ATR). Power-on or reset are the only methods available for initiating the self-tests.

9.1 Power-up Self Tests

The Citadel-OS cryptographic module performs the power-up self-tests whenever the module is powered up after being either:

- Powered off
- Reset
- Rebooted

The following power-on self-tests are performed:

- Firmware integrity test is performed by doing a CRC16 integrity test over the entire code area of the flash product based on AT90SC144144CT.
- The following cryptographic algorithm known-answer tests:
  - Deterministic random number generation test (DRNG, ANSI X9.31 compliant).
  - RSA sign/verify test
  - SHA-1 HASH test
  - Triple DES CBC MAC encryption test
  - Triple DES CBC mode encryption/decryption test
  - AES-128 CBC encryption/decryption

A known-answer test:

- Applies the cryptographic algorithm to data for which the correct output is already known
- Compares the calculated output with the previously generated output (the known answer)

The known-answer test fails if the calculated output does not equal the known answer.

9.2 Conditional Self Tests

The Citadel-OS cryptographic module performs the conditional tests whenever the conditions specified for the tests occur:

- Continuous DRNG test (ANSI X9.31 spec) with 64-bit frames.
- Continuous NDRNG test with 64-bit frames.
- RSA pair wise consistency tests with sign/verify & encrypt/decrypt mode of operation.
- Software/Firmware load test: N/A. The module does not support the loading of firmware.