Cryptographic Module Security Policy for the Litronic Industries Argus/300

Document 1

Version 1.5

Last revision 8/31/98

Background

This document seeks to focus attention on the security policy requirements of FIPS 140-1 as well as the validation requirements imposed by the Derived Test Requirements[1] (DTR).

A. Scope of Document

This document states the security policy for the Argus/300 Cryptographic Module.

B. Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-1.

Table 1. Module Security Level Specification

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

[1] The Derived Test Requirements for FIPS 140-1 is a document developed for NIST by MITRE. This document provides guidance to a validation lab on the interpretation of the FIPS standard and defines actual tests to be performed by the lab during the validation process. This Derived Test Requirements will be refered to as the DTR in the remainder of this document.

C. Roles and Services

The cryptographic module shall support four distinct operator roles. These operator roles are:

1. User Role
2. Security Administrator & User Pair Role
3. Cryptographic Officer
4. Cryptographic Officer Pair Role

The cryptographic module shall enforce the separation of roles using identity based operator authentication. Identities are defined by records stored on an IC card. Each record comprising a plaintext segment containing a mnemonic operator identity, a user type (indicating the role associated with the identity) and a PIN encrypted segment containing a MAC of the plaintext segment and an encrypted DES key. An operator must: present an IC Card, enter an identity and enter the access code (PIN) linked to that identity. Upon authentication, the user assumes the role that is linked to the presented identity and the privileges of that role (including the DES key) are conferred on that user for the duration of the session.

The relationship between identity, role, password and cryptographic key is established at the time that the information is written to the card and cannot, as a practical matter, be modified. A session is terminated when the user logs off, the smart card is withdrawn from the reader, a fault causes the CM to enter the Alarm state or the cryptographic module is powered down for any reason.

When the CM is powered and no users are logged in, the CM provides only "safe" services that are not related to cryptography:

- Power-on Self Test. When power is first applied to the CM, its functional integrity is verified through a comprehensive suite of self-tests.

- Self Test. At any time that the CM is powered and not busy executing a command, a user can command the CM to conduct a suite of self-tests.

- Show Status. Most Commands return the status of the CM to the host PC. The Table Driven Command Processing table in the FSMM document shows those commands that return status. Status consists of either ok or Alarm State.

- Identify an IC Card. A user can, at any time obtain the serial number of the installed IC card.

- User Authentication. At log-on, the user, his/her PIN and identity as well as the IC Card are authenticated and the encryption key associated with his identity is decrypted and made available for use by the user.

In addition to the “safe” services, the *User Role* shall provide all of the services necessary for the secure transport of data over an insecure network. This includes the following services:

- Encrypt Data. While logged on, the user can submit a data file for encryption using the DES encryption key associated with his/her identity.
- Decrypt Data. While logged on, the user can submit a data file for decryption using the DES encryption key associated with his/her identity.
- Log-out. An operator may log-out at any time. At log-out, the user relinquishes the privileges acquired by logging in with an identity and the cryptographic key is deleted from the cryptographic module.

The *Security Administrator and User Pair Role* shall provide all of the services listed above plus those services necessary to:

- Generate MAC. While logged on, the user can create a Message Authentication Code (MAC) for a message using the SHA-1 Message Digest and the DES encryption key associated with his/her identity.
- Verify MAC. While logged on, the user can verify a Message Authentication Code (MAC) for a message using the DES encryption key associated with his/her identity.

The *Cryptographic Officer Role* shall provide in addition to those services provided to the “user” role, those services necessary to:

- Unlock a DES Key. A cryptographic officer can unlock a DES key on an IC card that has been locked by exceeding the permitted number of consecutive unsuccessful password attempts.
- Erase an IC Card. A cryptographic officer can erase an IC card, permanently deleting the entire contents of the card.
- Change Authentication Vector. A cryptographic officer can change the authentication vector for a user.

The *Cryptographic Officer Pair Role* shall provide the services available specifically to the Cryptographic Officer Role as well as those services necessary to:

- Initialize an IC Card. A pair of cryptographic officers can initialize an IC card for use as a cryptographic token.
- Create a DES Encryption Key and add it to an IC Card. A pair of cryptographic officers can generate a DES encryption key and add it and an identity protected by a password to an IC card.

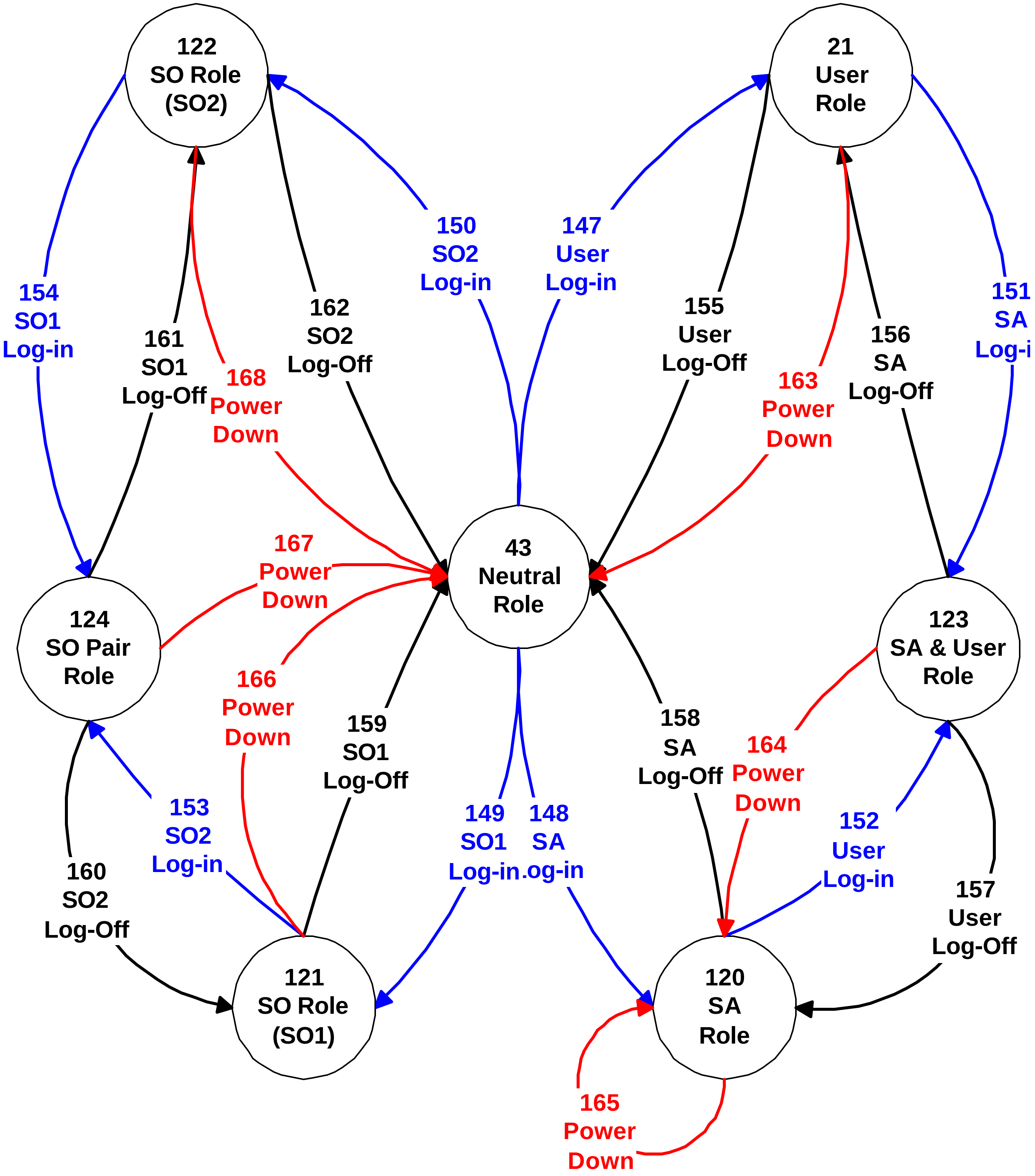
- Generate a Key Encryption Key. The DES keys for the two Cryptographic officers are exclusive ORed together to produce a key for managing the Key Escrow File.

- Translate DES Keys. The *KK obtained by exclusive ORing the keys of the two Cryptographic Officers can be used to encrypt and decrypt the Key Escrow files maintained at the Central Key Translation Center.

- Import Keys. A cryptographic officer pair can import a key encrypted by the a CO key pair.

- Export Keys. A cryptographic officer pair can export a key encrypted by the SO key pair.

The relationship between roles and the events that result in role transition are depicted in the following finite state machine model:


122 SO Role (SO2)
21 User Role
150 SO2 Log-in
147 User Log-in
154 SO1 Log-in
161 SO1 Log-Off
168 Power Down
162 SO2 Log-Off
155 User Log-Off
163 Power Down
156 SA Log-Off
151 SA Log-i
43 Neutral Role
167 Power Down
124 SO Pair Role
123 SA & User Role
166 Power Down
159 SO1 Log-Off
158 SA Log-Off
164 Power Down
153 SO2 Log-in
149 SO1 Log-in
148 SA .og-in
152 User Log-in
160 SO2 Log-Off
157 User Log-Off
121 SO Role (SO1)
120 SA Role
165 Power Down

D. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-1 Level 3 module[2].

1. *The cryptographic module shall provide four distinct operator roles. These are the User Role, the Security Administrator and User Pair Role, the Cryptographic Officer Role and the Cryptographic Officer Pair Role.*

2. *The cryptographic Module shall provide identity based authentication.*

   The module will support one user, one Security Administrator, a Security Administrator and User pair, one Cryptographic Officer or a Pair of Cryptographic officers.

3. *Role access code (identity) shall be a minimum of 8 characters and a maximum of 32 characters.*

4. *When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.*

5. *After a maximum (established by the cryptographic officers who initialized the card) consecutive unsuccessful PIN code validation attempts have occurred, the cryptographic module shall lock the card with respect to that identity until such time as the card is unlocked by the same cryptographic officers who initialized the card.*

   This design rule is intended to make a search attack for a PIN code unfeasible

6. *The cryptographic module shall encrypt message traffic using the DES algorithm operated in the Cipher Block Chaining Mode (CBC) as described in FIPS 81.*

7. *Upon the application of power or when commanded by the operator, the cryptographic module shall perform the following tests:*

   a) *Timer Test*
   b) *ROM CRC Test*
   c) *E^{2}PROM Test*
   d) *Internal RAM Pattern Test*
   e) *External RAM Pattern Test*
   f) *Random Number Generator Statistical Test*
   g) *SHA-1 Known Answer Test*
   h) *DES Encryption and Decryption Algorithm Known Answer Test*

[2] Rules are contained in the number paragraphs and are shown in italics. Other information is included for background purposes only.

i) DES S–Box Test

No explicit CPU function test is performed because the rest of the tests are primarily executed in firmware, therefore successful execution of the rest of the test yields the reasonable inference that the CPU operates properly.

8. At any time the module is in an idle state, the operator shall be capable of commanding the module to perform the self test.

9. A message is signed, computing a Message Authentication Code (MAC) as defined in FIPS Pub 113 Computer Data Authentication

10. The Cryptographic Module shall enforce split knowledge and dual control as defined in FIPS Pub 171 Key Management Using ANSI X9.17

E. Definition of Security Relevant Data Items

This and the following two sections specify the relationship between Security Relevant Data Items (SRDIs), the modes of access for SRDIs, and the relevant roles.

There are 9 types of security relevant data items (SRDIs). These are:

a) User Type: a character denoting the roles that may be assumed by the user.

b) User Identity: The 1 to 16 character name of the user. The identity is used at log-in to select the encryption key and user type from those available on the card.

c) User PIN: The 4 to 8 character mnemonic password which is used to MAC the Identity of the user. Verification of the MAC is taken as proof that the PIN presented is itself valid and that it will correctly decrypt the associated DES key. Thus, the PIN is not stored on the card but is authenticated by inference.

d) Maximum PIN Tries: The maximum number or unsuccessful PIN entry attempts before the card is locked to further attempts.

e) PIN Entry Tries: The number of PIN entry attempts since card initialization of last successful PIN entry.

f) DES Key: The 64-bit Data Encryption Standard key as defined in FIPS 46-2

g) Authentication Vector: the set of privileges (i.e. the commands) that a user may exercise.

h) Key Encryption Keys: the pair of Security Officer keys, which when XORed together form the key that is used to encrypt the key escrow data base.

i) MAC: The message authentication code comprising a encrypted message digest computed using SHA-1.

F. Definitions of SRDI Modes of Access

Table 2 below defines the relationship between access to SRDIs and the different module services. The modes of access shown in the table are defined as follows:

a) **Get User Type**: This operation obtains a User type from the Cryptographic Officers to be written to a smart card.

b) **Get User Identity**: This operation obtains a User Identity from the Cryptographic Officers to be written to a smart card.

c) **Read User PIN from KB**: This operation reads the user PIN from the keyboard using the protected PIN path (PPP).

d) **Save PIN Failure Count**: This operation save the count of PIN entry failures since the last success.

e) **Establish Expiration Date:** This operation saves that date on which the current PIN expires.

f) **Create DES Key**: This operation generates a 54-bit random number and appends 8 parity bit to create a DES Encryption Key.

g) **Use DES Key**: This operation uses the plaintext DES key stored in read protected DES IC memory to encrypt or decrypt data.

h) **Encrypt DES Key**: This operation uses the assigned PIN to encrypt the DES key for storage on an IC Card.

i) **Decrypt DES Key**: This operation uses the user PIN to decrypt DES Encryption Key into a read protected register in the DES integrated circuit.

j) **Generate *KK**: This operation generates the Key encryption key from the keys associated with two Cryptographic officers.

k) **Assign PIN**: This operation provides the system with information sufficient to permit authentication of a presented PIN. The PIN in not stored, but rather is used to MAC the user's identity and to encrypt the user's encryption key.

l) **Authenticate PIN**: This operation authenticates a presented PIN by inference. The PIN is used to compute a MAC for the user's plaintext Identity. Identity between the stored MAC and the MAC computer using the presented PIN is taken to be proof that the PIN is identical to the access PIN and will therefore correctly decrypt the DES key. This operation is done for the convenience of the rightful user, since the incorrect PIN applied to decrypt the encrypted DES key would yield a wrong DES key.

m) **Lock DES Key**: This operation bars further attempts at access to a DES key, when a user exceeds the permissible number of consecutive unsuccessful PIN entries.

n) **Unlock DES Key**: This operation unlocks a DES key that has been locked through excessive consecutive unsuccessful PIN attempts.

o) **Generate MAC**: This operation generates a message Authentication Code.

p) **Verify MAC**: This operation Verifies a Message authentication code.

q) **Identify Card**: This operation returns the serial number of the smart card currently in the reader.

r) **Set Authentication Vector**: this service fixes the set of functions that a user can perform.

s) **Modify Authentication Vector**: this service changes the set of functions that a user can perform.

t) **Access Authentication Vector**: This operation gets the authentication vector associated with the current user.

u) **Zeroize CM**: This operation zeroizes all security related data items.

G. Service to SRDI Access Operation Relationship

The following table shows the relationships between user services and SRDI Access Operations:

Table 2 Service Versus SRDI Access	SRDI Modes of Access																					Applicable Role			
User Service	Get User Type	Get User Identity	Read User PIN from KB	Save PIN Faulure Count	Establish Expiration Date	Create DES Key	Use DES Key	Encrypt DES Key	Decrypt DES Key	Generate *KK	Assign PIN	Authenticate PIN	Lock DES Key	Unlock DES Key	Generate MAC	Verify MAC	Identify Card	Set Authenication Vector	Modify Authentication Vector	Translat Key	Access Authentication Vector	Zeroize CM	User Role	Security Admin & User	Crypto Officer Role	Crypto Office Pair
Power-ON Self Test																							✓	✓	✓	✓
Self Test																							✓	✓	✓	✓
User Authentication	✓	✓	✓						✓			✓	✓								✓		✓	✓	✓	✓
Identify Card																	✓						✓	✓	✓	✓
Encrypt Data							✓																✓	✓	✓	✓
Decrypt Data							✓																✓	✓	✓	✓
Log Out																						✓	✓	✓	✓	✓
Generate MAC							✓								✓						✓			✓	✓	✓
Verify MAC							✓								✓	✓					✓			✓	✓	✓
Unlock a DES Key				✓										✓							✓				✓	✓
Erase an IC Card																									✓	✓
Initialize an IC Card				✓	✓			✓			✓							✓	✓		✓					✓
Change Authentication Vector																		✓	✓		✓				✓	✓
Generate DES Key						✓															✓					✓
Import Key																				✓						
Export Key																				✓						
Generate Key Encryption Key										✓											✓					✓

H. DES Encryption Keys

Data security is facilitated through the use of a set of DES keys as follows:

PIN: padded out to 8 7-bit ASCII characters that are converted into a DES key by generating a byte containing the parity bits for each character of the PIN. This key is used (DES ECB) to authenticate a hash of the user's identity on the card and to decrypt the associated DES key.

Security Administrator Key: stored in the battery backed RAM and used only as part of the composite key used to sign files.

User Key: used either for encrypting files (DES ECB) or as part of the composite signing key.

Signing Key: a composite key created by the Exclusive OR of the SA Key and the User Key, kept in the Key Cache of the DES Chip (DES CBC).

Cryptographic Officer Key (*KK$_1$ or *KK$_2$): used only as a component of the Key Management Key.

Key Management Key (*KK): a composite key created by the Exclusive OR of the two Cryptographic Officer Keys) DES CBC).

I. DES Modes

The following are the DES modes and their usage in the Argus/300:

- **OFB** – not used
- **ECB** – user authentication, data encryption and data decryption
- **CFB** – self test (S-box, encryption, decryption)
- **CBC** – Random number generation and key translation

J. Command Authorization

The set of commands that a user is permitted to execute is controlled by his Authentication Vector. The authentication vector is established at card initialization by the SO Pair and may be changed by them at a later time. The Authentication vector is part of the plaintext user authentication data that is protected by a hash that is encrypted by the user's PIN. The commands with numbers 0 through 15 are available to any user (authenticated or not). The Authentication vector controls access to the commands numbered 16 through 79 (not all of which are implemented. A one in a bit position authorizes the user to execute the corresponding command, a zero prohibits execution of the corresponding command.