SEL-3021
Serial Encrypting Transceiver
Security Policy

Document Version 1.11

Schweitzer Engineering Laboratories, Inc.

May 14, 2008

TABLE OF CONTENTS

1. MODULE OVERVIEW 3

2. SECURITY LEVEL 4

3. MODES OF OPERATION 4

4. PORTS AND INTERFACES 5

TRUSTED DATA PORT 6
UNTRUSTED DATA PORT 6
USER INTERFACE 6

5. IDENTIFICATION AND AUTHENTICATION POLICY 6

6. ACCESS CONTROL POLICY 9

ROLES AND SERVICES 9
UNAUTHENTICATED SERVICES 10
DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 11
DEFINITION OF MODULE PUBLIC KEYS 12
DEFINITION OF CSPS AND PUBLIC KEYS MODES OF ACCESS 12

7. OPERATIONAL ENVIRONMENT 13

8. SECURITY RULES 13

9. PHYSICAL SECURITY POLICY 15

PHYSICAL SECURITY MECHANISMS 15
OPERATOR REQUIRED ACTIONS 15

10. MITIGATION OF OTHER ATTACKS POLICY 16

11. REFERENCES 16

12. DEFINITIONS AND ACRONYMS 16

13. SECURE DELIVERY AND OPERATION 16

1. Module Overview

The SEL-3021 Serial Encrypting Transceiver is a multi-chip standalone cryptographic module (Hardware P/N SEL-3021 Versions 00016A10 (USB) or 00006A10 (Wireless), Firmware Versions SEL-3021-1-R102-V0-Z001001-D20080505 and SEL-3021-1-R101-V0-Z001001-D20070521) encased in a hard, opaque, tamper evident commercial grade plastic case. The cryptographic boundary is the entire module.

The SEL-3021 is an EIA-232 "bump in the wire" encryption module. The SEL-3021 is designed to protect latency-sensitive devices that send and receive critical, sensitive data such as electric power revenue meters, protective relays, Programming Logic Controllers (PLC), Remote Terminal Units (RTU), and Supervisory Control and Data Acquisition (SCADA) equipment from unauthorized access, control, monitoring, and malicious attack. Figure 1 shows a SEL-3021 Serial Encrypting Transceiver.

Figure 1 – Image of the SEL-3021 Serial Encrypting Transceiver

The SEL–3021 consists of two EIA-232 ports, referred to as the Local Interface and the Remote Interface. The Local Interface connects to a device that requires data protection, e.g. the SCADA master, RTU or computer serial port. The Remote Interface connects to an untrusted channel, e.g. a modem connected to a leased phone line or network connection device. The Local Interface exchanges plaintext (unencrypted) data between the protected device and the SEL–3021. The Remote Interface exchanges encrypted data between the local SEL-3021 device and one, or more remote SEL–3021 devices.

The SEL–3021 also incorporates a secured User Interface (IEEE 802.11b wireless or USB 2.0). The interface is secured by cryptographic authentication and encryption: 128-bit AES encryption and HMAC-SHA-1 for authentication. This encrypted interface allows system operators to securely monitor the Local and Remote Interface channel health and to program system parameters without removing the SEL–3021 from service.

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- 128-bit AES CBC mode encryption for securing all messages on the User Interface.
- HMAC-SHA-1, with 128-bit key strength, for authenticating all messages on the User Interface.
- 128-bit AES CTR mode encryption for securing In-Band data transmission on the untrusted, serial interface.
- 128-bit AES Key Wrap for securing all Out-Of-Band session key transports on the untrusted, serial interface.

- 128-bit AES ECB mode
- SHA-1
- DSA-1024 using SHA-1

The SEL-3021 cryptographic module relies on the implemented deterministic random number generator (DRNG) that is compliant with FIPS 186-2 Appendix 3.1with 512-bit seed key (XKEY) value. The DRNG seed key (XKEY) is supplied by a non-deterministic random number generator (NDRNG) comprised of a hardware-implemented, amplified noise sampler.

The SEL-3021 cryptographic module only runs in FIPS mode.

4. Ports and Interfaces

The SEL-3021 cryptographic module provides the following physical ports and logical interfaces:

Physical Port	Protocol	Logical Interface
DB9 DTE	EIA-232	Data input/output (switchable trusted or untrusted data port) Control input (Management operations such as SMI)
DB9 DCE	EIA-232	Data input/output (switchable trusted or untrusted data port) Control input/Status output (when in upgrade or reset mode and Management operations such as SMI)
Wireless User Interface (Available if USB User Interface is not installed)	802.11b	Control input/Status output Data input/output
USB User Interface (Available if Wireless User Interface is not installed)	USB 2.0	Control input/Status output Data input/output
Reset button	N/A	Control input, used for zeroization
Compression terminal, for power (5 to 24 Volts DC)	N/A	Power
Alarm contact (compression terminal connector)	N/A	Status output
LED (Green LED located on the rear of the module)	N/A	Status output

Trusted Data Port

The Trusted EIA-232 interface receives plain text data from the trusted source and passes it to the encrypting data path. The Trusted EIA-232 interface receives decrypted data from the decryption data path and transmits it to the trusted source. The user is allowed to select whether the DTE or DCE physical DB9 serial port is the trusted port. The other port is set as the Untrusted interface.

Untrusted Data Port

The Untrusted EIA-232 interface receives cipher text data from the encrypting data path and sends it to an untrusted source. The Untrusted EIA-232 interface receives encrypted data from an untrusted source. The untrusted port passes the encrypted message to the decrypting data path. The decrypting data path then decrypts the received message and transmits it to the trusted source.

User Interface

The User Interface consists of either an IEEE 802.11b wireless interface or a USB 2.0 interface and PC SW (the software is not included in the module boundary). The User Interface exists for the sole purpose of monitoring and configuring the module.

5. Identification and Authentication Policy

Assumption of roles

The SEL-3021 Serial Encrypting Transceiver supports four distinct operator roles; the Security Officer, the Operator, Upgrade, and the Remote Device (User). The cryptographic module enforces the separation of roles using role-based user authentication. A user must prove knowledge of the appropriate key in order to authenticate to the module.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Security Officer	Role-based user authentication	Knowledge of Security Officer Encryption Key (128-bit AES key), the Security Officer Authentication Key (128-bit HMAC-SHA-1 key) and the Security Officer

		Password (6-80 printable ASCII characters)
Upgrade	Role-based user authentication	Knowledge of Upgrade Encryption Key (128-bit AES key), and the Upgrade DSA Key (1024-bit key)
Operator	Role-based user authentication	Knowledge of Operator encryption key (128-bit AES key), the Operator authentication key (128-bit HMAC-SHA-1 key) and the Operator password (6-80 printable ASCII characters).
Remote Device (User)	Role-based user authentication	Knowledge of System Encryption Key (128-bit AES key).

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Encryption Key, Authentication Key, and Password (Security Officer and Operator roles)	In order to authenticate as the Security Officer or Operator, an attacker must know the values of the cryptographic security parameters (CSPs) associated with the desired role (128 bit encryption key, the 128 bit authentication key, and the password). Assuming that all parameters are independent, and that a minimum-length, six-byte password is used, the probability that a random attempt will succeed or a false acceptance will occur is 1/(2^128*2^128*92^6) = 1.42 E -89. This analysis assumes that a random password is selected from a 92-character printable ASCII alphabet. We also assume that the exact value of all CSPs must be correctly guessed in order to successfully authenticate (i.e. the individual CSPs cannot be guessed or broken separately). This assumption is true for the SEL-3021

	because the device does not give any feedback indicating the success or failure of any one CSP value. Assuming that the SEL-3021 can process 1000 guesses per second (this is a very conservative value as the SEL-3021 will not be able to process authentication attempts at anywhere near this rate), the probability of successfully authenticating to the module within one minute is 8.54 E -85.
Upgrade Encryption Key and DSA Key (Upgrade role)	Assuming that all parameters are independent, the probability that a random attempt will succeed or a false acceptance will occur is 1/(2^128*2^1024) = 1.63 E -347. We assume that the exact value of all CSPs must be correctly guessed in order to successfully authenticate (i.e. the individual CSPs cannot be guessed or broken separately). This assumption is true for the SEL-3021 because the device does not give any feedback indicating the success or failure of any one CSP value. Assuming that the SEL-3021 can process 1 guess per minute (this is a very conservative value as the SEL-3021 will not be able to process authentication attempts at anywhere near this rate), the probability of successfully authenticating to the module within one minute is 1.63 E -347.
Encryption Key (Remote Device role)	The probability that a random attempt will succeed or a false acceptance will occur is 1/(2^128) = 2.94 E -39. The module is capable of performing approximately one authentication every .02 seconds (based on the size of the authentication dialog frames and the maximum baud rate of the SEL-3021). This results in a maximum authentication dialog-processing rate of 3000 attempts per minute. The probability of successfully authenticating to the module within one minute is 8.82 E -36.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
Security Officer: The Security Officer role is only available on the user interface. This role shall provide all of the services necessary to program all of the SEL-3021 settings including all cryptographic security parameters (CSPs). In addition, the Security Officer role can view all settings (except CSPs) and all device status variables.	• Initiate Security Officer Session on the User Interface: This service opens an authenticated Security Officer role session on the user interface. • View all Settings Except CSPs: This service allows the authenticated user to view all device settings except those listed below as CSPs. This service is only available via the User Interface. • Change all Settings: This service allows the authenticated user to change the value of all device settings including all CSPs. This service is only available via the User Interface. • Show Status via User Interface: This service allows the authenticated user to view the operational status of the device. This service is only available via the User Interface. • Clear Status Log: This service allows the authenticated user to reset all device status variables. This service is only available via the User Interface. • Initiate Bypass Mode: This service allows the user to change settings that force the device to pass data received on the Trusted and Untrusted Interfaces through the module without encrypting or decrypting the data.
Operator: The Operator role is only available on the user interface. This role shall provide all of the services necessary to program all non-sensitive SEL-3021 settings. The Operator role will **not** have access to	• Initiate Operator Session on the User Interface: This service opens an authenticated Operator role session on the User Interface. • View Non-Critical Settings: This service allows the authenticated user to view all device settings that do not compromise the security of the network. This service is only available via the User Interface. • Change Non-Critical Settings: This service allows the

sensitive settings including all cryptographic security parameters (CSPs). In addition, the Operator role can view all non-sensitive settings and all device status variables.	authenticated user to change the value of all device settings that do not compromise the security of the network. This service is only available via the User Interface. • Show Status via User Interface: See above. • Clear Status Log: See above.
Remote Device (User): This role shall provide all of the services necessary for the secure, reliable transport of data over an untrusted network	• Initiate Remote Device Session on the Untrusted Interface: This service opens an authenticated Remote Device role session on the Untrusted interface. • Encrypt User Data: This service AES encrypts data passed into the cryptographic module from the Trusted Interface. The encrypted data is then transmitted on the Untrusted Interface. • Decrypt User Data: This service AES decrypts data passed into the cryptographic module from the Untrusted Interface. The decrypted data is then transmitted on the Trusted Interface. • Encrypt Management Data: This service encrypts session keys (using the AES key wrap algorithm). The encrypted management frames are then transmitted on the Untrusted Interface. • Decrypt Management Data: This service decrypts session keys received on the Untrusted Interface (using the AES key wrap algorithm).
Upgrade: The Upgrade role is only available when the device is placed in upgrade mode. This role shall provide all of the services necessary to upgrade the SEL-3021 firmware.	• Upgrade Firmware: This service allows the authenticated user to change the firmware. This service is only available via the DCE serial port when the device is placed in upgrade mode.

Unauthenticated Services

The SEL-3021 cryptographic module supports the following unauthenticated services:

- Show status via LED: This service provides the current status of the cryptographic module.

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2 via a power-cycle.

- Zeroize: This service actively destroys all plaintext critical security parameters stored in the module (except for the Upgrade Encryption Key). The zeroize service is activated via the reset button. The Upgrade Encryption Key can be zeroized by loading a new firmware image, via the Upgrade Firmware service, which contains an all zero Upgrade Encryption Key.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

Security Officer Encryption Key: 128-bit AES key used during the Security Officer authentication and session key exchange handshake process.

Security Officer Authentication Key: 128-bit HMAC key used during the Security Officer authentication and session key exchange handshake process.

Security Officer Password: 6-80 printable character password used during the Security Officer authentication and session key exchange handshake process.

Operator Encryption Key: 128-bit AES key used during the Operator authentication and session key exchange handshake process.

Operator Authentication Key: 128-bit HMAC key used during the Operator authentication and session key exchange handshake process.

Operator Password: 6-80 printable character password used during the Operator authentication and session key exchange handshake process.

User Interface Session Encryption Key: 128-bit AES key used to encrypt user interface data during Security Officer or Operator role sessions on the User Interface (after authentication and session key exchange handshake).

User Interface Session Authentication Key: 128-bit HMAC key used to authenticate user interface frames during Security Officer or Operator role sessions on the User Interface (after authentication and session key exchange handshake).

System Encryption Key: 128-bit AES key used to encrypt all control frames (out-of-band frames) transmitted over the Untrusted Interface (including the Remote Device authentication handshake and session key exchange frames).

Data Session Encryption/Decryption Key: 128-bit AES key used to encrypt user data frames (in-band frames) transmitted over the Untrusted Interface (after Remote Device authentication and key exchange).

DRNG State: 512-bit State maintained by the FIPS 186-2 DRNG.

DRNG Seed key: 512-bit key used to seed the FIPS 186-2 DRNG.

Upgrade Encryption Key: 128-bit AES key used to decrypt a received firmware image.

Definition of module public keys

The following are public keys contained in the module:

Upgrade DSA Key: 1024-bit DSA key used to verify a received firmware image was signed by an authenticated source.

Definition of CSPs and public keys Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

G: Generate

S: Set

U: Use

D: Delete

Table 6 – CSP and Public Key Access Rights within Roles & Services

				Service	CSP Access Operations
Security Officer	Operator	Remote Device	Upgrade		
X				Initiate Security Officer Session on the User Interface	U – Security Officer Encryption Key U – Security Officer Authentication Key U – Security Officer Password G – User interface Session Encryption Key G – User interface Session Authentication Key
	X			Initiate Operator Session on the User Interface	U – Operator Encryption Key U – Operator Authentication Key U – Operator Password G – User interface Session Encryption Key G – User interface Session Authentication Key
X				View all Settings Except CSPs	U – User interface Session Encryption Key U – User interface Session Authentication Key
X	X			View Non-Critical Settings	U – User interface Session Encryption Key U – User interface Session Authentication Key

X				Change all Settings	U – User interface Session Encryption Key U – User interface Session Authentication Key S – Security Officer Encryption Key S – Security Officer Authentication Key S – Security Officer Password S – Operator Encryption Key S – Operator Authentication Key S – Operator Password S – System Encryption Key
X	X			Change Non-Critical Settings	U – User interface Session Encryption Key U – User interface Session Authentication Key
X	X			Show Status via User Interface	U – User interface Session Encryption Key U – User interface Session Authentication Key
X	X			Clear Status Log	U – User interface Session Encryption Key U – User interface Session Authentication Key
X				Initiate Bypass Mode	U – User interface Session Encryption Key U – Wireless Session Authentication Key
			X	Upgrade Firmware	U – Upgrade Encryption Key U – Upgrade DSA Key S – Upgrade Encryption Key S – Upgrade DSA Key
		X		Initiate Remote Device Session on the Untrusted Interface	U – System Encryption Key G – Data Session Encryption Key
		X		Encrypt User Data	U – Data Session Encryption Key
		X		Decrypt User Data	U – Data Session Encryption Key
		X		Encrypt Management Data	U – System Encryption Key
		X		Decrypt Management Data	U – System Encryption Key

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the SEL-3021 does not contain a modifiable operational environment.

8. Security Rules

The SEL-3021 cryptographic module's design corresponds to the module's security rules. This section documents the security rules enforced by the SEL-3021 to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module provides four distinct operator roles. These are the Security Officer role, the Upgrade role, the Operator role, and the Remote Device role.

2. The cryptographic module provides role-based authentication.
3. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
4. The cryptographic module encrypts message traffic using the AES algorithm.
5. The cryptographic module performs the following tests:

A. Power up Self-Tests:

1. Cryptographic algorithm tests:
    a. AES CBC Known Answer Test
        i. 128-bit key
    b. DRNG Known Answer Test
        i. FIPS 186-2
    c. HMAC SHA-1 Known Answer Test
    d. SHA-1 Known Answer Test
    e. DSA Known Answer Test (Signature Verification)
        i. 1024-bit key
2. Software Integrity Test: 32-bit CRC calculated over the program image. If the calculated CRC value does not match the value in FLASH, the device declares a FLASH failure and disables itself.

B. Conditional Self-Tests:

1. Continuous Random Number Generator Test (RNG test is performed on NDRNG and DRNG): This test compares the last 32 bit NDRNG (512 bit for DRNG) output with the current 32 bit NDRNG (512 bit for DRNG) output. If the two values are equal, there are two further attempts to generate a different (N)DRNG output. If all three attempts fail, the device declares an (N)DRNG failure and the device is disabled.
2. Bypass Mode Test (performed when the module goes from bypass mode to secure mode, or from secure mode to bypass mode): Known answer test on the entire encrypt and decrypt data paths.
3. Software/Firmware Load Test: The module verifies a DSA digital signature when loading firmware.

C. Critical Functions Tests:

1. Runtime SDRAM Failure Tests: Read and write tests are performed on the system SDRAM. This continuously checks the SDRAM address space during runtime. If an

error is detected, the device declares a RAM failure and disables itself.

2. Settings Integrity Test: 32-bit CRC calculated over the settings image. If the calculated CRC value does not match the value in FLASH, the device declares a FLASH failure and disables itself

6. At any time the operator is capable of commanding the module to perform the power-up self-tests by power-cycling the module.
7. Prior to each use, the internal RNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.
8. Data output is inhibited during self-tests, zeroization, and error states, and logically separate from the key generation process.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module does not support multiple concurrent operators via the User Interface. The module maintains logical separation of multiple, concurrent Remote Devices (Users) by maintaining a unique identification field for each User.
11. The module supports a bypass mode that requires two, independent internal actions to activate.
12. Upon power-cycle, the module clears all previous authentications. The authentication procedure is reset and must be re-established.
13. The CSPs and authentication data are physically and logically protected from unauthorized disclosure, modification, and substitution, as they are not accessible to unauthenticated users from outside of the module boundary.

9. Physical Security Policy

Physical Security Mechanisms

The SEL-3021 multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components entirely enclosed within an opaque enclosure. The enclosure cannot be penetrated without causing tamper evidence via the tamper evident labels. The enclosure is sonically welded to prevent undetected access.
- The circuitry is encapsulated in a hard, opaque, potting material. The circuitry cannot be accessed without causing tamper evidence.

Operator Required Actions

The operator is required to periodically inspect the enclosure for tamper evidence.

There are two tamper labels, one on each side, on the locations shown below:

Figure 2 – Tamper Label Locations

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate any attacks outside of the scope of FIPS 140-2.

11. References

12. Definitions and Acronyms

13. Secure Delivery and Operation

The security of the SEL-3021 cannot be assured if the device is received from the factory with evidence of tampering. If the shipping packaging or the tamper evident seal on the SEL-3021 show signs of tampering, contact an SEL customer service representative.