SEL-3025 Serial Shield®

Serial Cryptographic Transceiver

Instruction Manual

Attention

The SEL-3025 is a cryptographic device. Limit access to the SEL-3025, ACSELERATOR QuickSet, and SEL-3025 Instruction Manual to authorized personnel only. Do not copy these items. Securely store these items when not in use. Destroy these items when no longer needed.

FIPS VALIDATED 140-2 ™

20151009

SEL SCHWEITZER ENGINEERING LABORATORIES, INC.

PM3025-01

PM3025-01

Table of Contents

Section 8: Testing and Troubleshooting

Appendix A: Firmware and Manual Versions

Appendix B: Firmware Upgrade Instructions

Appendix C: Importing or Exporting Settings

Appendix D: User-Based Accounts

Appendix E: Syslog

Appendix F: Networking Fundamentals

Appendix G: Classless Inter-Domain Routing (CIDR)

Appendix H: X.509

This page intentionally left blank

List of Tables

This page intentionally left blank

List of Figures

Preface

Manual Overview

This instruction manual describes the functionality and use of the SEL-3025 Serial Shield®. It includes the information that is necessary to install, configure, test, and operate this device.

An overview of the manual's layout and the topics that are addressed follows.

Preface. Describes the manual organization and conventions used to present information.

Section 1: Introduction and Specifications. Introduces SEL-3025 applications, connectivity, and use requirements. This section also lists specifications.

Section 2: Installation. Provides dimension drawings on the SEL-3025 and instructions for initializing the SEL-3025.

Section 3: Managing Users. Explains how users are managed on the SEL-3025.

Section 4: Using the PC Serial Security Kit to Protect Engineering Access Communication. Describes use of the PC Serial Security Kit in obtaining secure engineering access communications through an SEL-3025.

Section 5: Administering Engineering Access With acSELerator QuickSet. Describes acSELerator QuickSet simplification of SEL-3025 deployment for engineering access by managing keys and groups of users.

Section 6: Job Done Examples. Provides four Job Done examples. These examples provide step-by-step configuration of the SEL-3025 for application in various SCADA and engineering access environments.

Section 7: Settings and Commands. Lists and describes all the SEL-3025 settings.

Section 8: Testing and Troubleshooting. Describes the diagnostic functions of the SEL-3025 and provides troubleshooting guidelines.

Appendix A: Firmware and Manual Versions. Lists firmware and manual revisions.

Appendix B: Firmware Upgrade Instructions. Provides instructions to update the firmware in the SEL-3025 Serial Shield.

Appendix C: Importing or Exporting Settings. Explains use of settings files in expediting configuration tasks and helping to diagnose system problems.

Appendix D: User-Based Accounts. Provides an introduction to User-Based Accounts and the benefits associated with using User-Based Accounts.

Appendix E: Syslog. Provides an introduction to the Syslog protocol and its uses in SEL products.

Appendix F: Networking Fundamentals. Provides an overview of Windows Networking and network configuration.

Appendix G: Classless Inter-Domain Routing (CIDR). Explains CIDR and CIDR notation.

Appendix H: X.509. Explains the structure and use of X.509 certificates.

Safety Information

Dangers, Warnings, and Cautions

The manual uses three kinds of hazard statements, defined as follows:

⚠DANGER
Indicates an imminently hazardous situation that, if not avoided, **will** result in death or serious injury.

⚠WARNING
Indicates a potentially hazardous situation that, if not avoided, **could** result in death or serious injury.

⚠CAUTION
Indicates a potentially hazardous situation that, if not avoided, **may** result in minor or moderate injury or equipment damage.

Safety Symbols

The following symbols are often marked on SEL products.

⚠	**⚠CAUTION** Refer to accompanying documents	**⚠ATTENTION** Se reporter à la documentation
⏚	Earth (ground)	Terre
⊜	Protective earth (ground)	Terre de protection
⎓	Direct current	Courant continu
∿	Alternating current	Courant alternatif
≂	Both direct and alternating current	Courant continu et alternatif
📖	Instruction manual	Manuel d’instructions

Safety Marks

General Safety Marks

⚠CAUTION Incorrect wiring may result in damage to the unit.	**⚠ATTENTION** Filage incorrect peut provoquer des dommages à l’unité.

Other Safety Marks

⚠DANGER Disconnect or de-energize all external connections before opening this device. Contact with hazardous voltages and currents inside this device can cause electrical shock resulting in injury or death.	**⚠DANGER** Débrancher tous les raccordements externes avant d’ouvrir cet appareil. Tout contact avec des tensions ou courants internes à l’appareil peut causer un choc électrique pouvant entraîner des blessures ou la mort.
⚠DANGER Contact with instrument terminals can cause electrical shock that can result in injury or death.	**⚠DANGER** Tout contact avec les bornes de l’appareil peut causer un choc électrique pouvant entraîner des blessures ou la mort.
⚠WARNING Have only qualified personnel service this equipment. If you are not qualified to service this equipment, you can injure yourself or others, or cause equipment damage.	**⚠AVERTISSEMENT** Seules des personnes qualifiées peuvent travailler sur cet appareil. Si vous n’êtes pas qualifiés pour ce travail, vous pourriez vous blesser avec d’autres personnes ou endommager l’équipement.
⚠WARNING Use of this equipment in a manner other than specified in this manual can impair operator safety safeguards provided by this equipment.	**⚠AVERTISSEMENT** L'utilisation de cet appareil suivant des procédures différentes de celles indiquées dans ce manuel peut désarmer les dispositifs de protection d'opérateur normalement actifs sur cet équipement.
⚠WARNING In order to avoid losing system logs on a factory-default reset, configure the SEL-3025 to forward Syslog messages.	**⚠AVERTISSEMENT** Pour éviter de perdre les enregistrements du système sur un redémarrage défini par défaut, configurer le SEL-3025 pour envoyer les messages de l'enregistreur du système (“Syslog”).
⚠CAUTION Equipment components are sensitive to electrostatic discharge (ESD). Undetectable permanent damage can result if you do not use proper ESD procedures. Ground yourself, your work surface, and this equipment before removing any cover from this equipment. If your facility is not equipped to work with these components, contact SEL about returning this device and related SEL equipment for service.	**⚠ATTENTION** Les composants de cet équipement sont sensibles aux décharges électrostatiques (DES). Des dommages permanents non-décelables peuvent résulter de l’absence de précautions contre les DES. Raccordez-vous correctement à la terre, ainsi que la surface de travail et l’appareil avant d’en retirer un panneau. Si vous n’êtes pas équipés pour travailler avec ce type de composants, contacter SEL afin de retourner l’appareil pour un service en usine.

Examples

This instruction manual uses several example illustrations and instructions to explain how to effectively operate the SEL-3025 Serial Shield. These examples are for demonstration purposes only; the firmware identification information or settings values included in these examples may not necessarily match those in the present version of your SEL-3025 Serial Shield.

Technical Assistance

Obtain technical assistance from the following:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 USA
Phone: +1.509.332.1890
Fax: +1.509.332.7990
Internet: www.selinc.com
Email: info@selinc.com

This page intentionally left blank

Section 1

Introduction and Specifications

Introduction

This section includes the following information about the SEL-3025 Serial Shield® cryptographic transceiver.

- ➤ *Product Overview*
- ➤ *Application Overview*
- ➤ *Functional Description*
- ➤ *HTTPS Web Interface*
- ➤ *Connections, Reset Button, and LED Indications*
- ➤ *Software System Requirements*
- ➤ *General Safety and Care Information*
- ➤ *Related Products*
- ➤ *Specifications*

Product Overview

The SEL-3025 is a bump-in-the-wire device that adds strong FIPS 140-2 level 2 validated cryptographic security to serial communications lines by using the SEL-3044 or SEL-3045 cryptographic integrated card. It is designed for point-to-point, point-to-multipoint supervisory control and data acquisition (SCADA) networks, and many-to-many configurations such as remote engineering access, where multiple users need access to multiple devices.

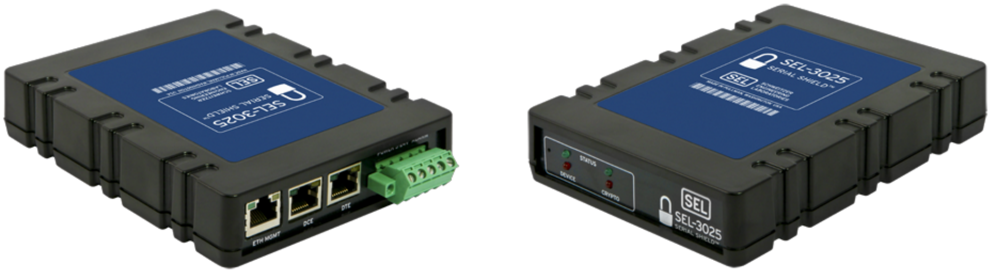


Figure 1.1 SEL-3025 Serial Shield

The SEL-3025 offers two cryptographic protocols for authentication and integrity of data communications. Secure SCADA Communications Protocol (SSCP) provides authentication and optional encryption of each message. Streaming Encryption Protocol (SEP) provides authentication upon establishment of a channel and secure low-latency channel encryption.

Use of the SEL-3025 protects against forged, modified, spliced, reordered, or replayed messages. The SEL-3025 also prevents unauthorized device access by rejecting all communications session requests from sources that cannot pass cryptographic session authentication.

For dial-up applications such as engineering access, SEL offers the 915900225 PC Serial Security Kit, which provides SSCP protection to a serial port on the PC.

Figure 1.2 shows a typical engineering remote access application, where an engineering workstation uses a modem to retrieve data or make configuration changes to a remote device over an untrusted communications channel. Publicly accessible channels, such as a plain old telephone service (POTS), a dial-up connection, or a radio link, are considered to be untrusted communications channels because unauthorized individuals could alter the data these media carry. An attacker could also access the channel and inject malicious data to cause such an unwanted action as an unauthorized breaker operation.

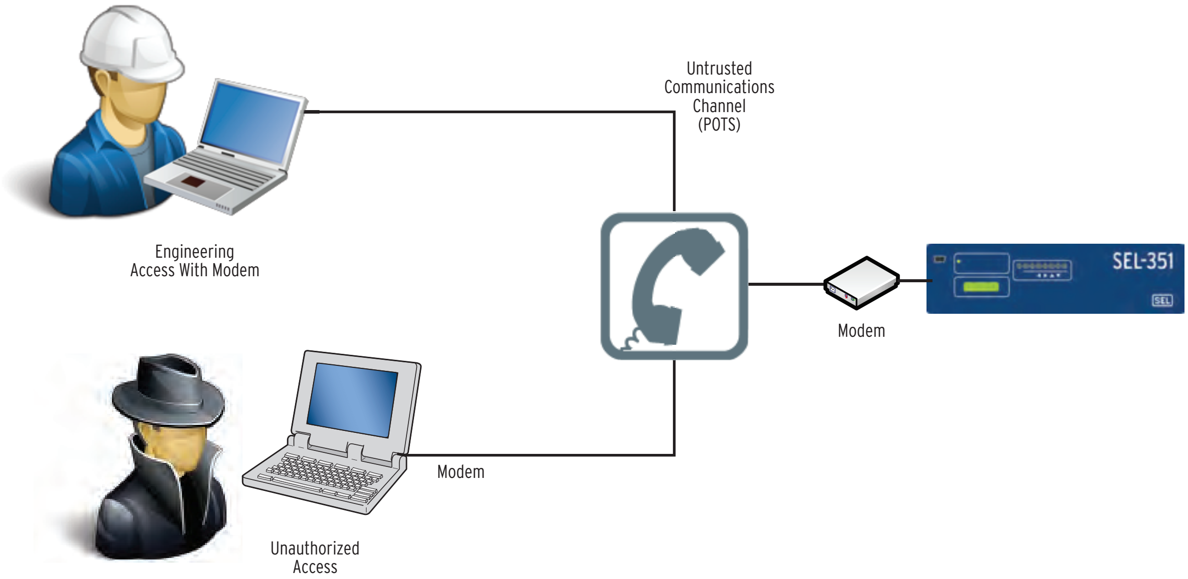


Figure 1.2 Typical SCADA Communications Channel

Figure 1.3 shows the SCADA communications link now secured through use of an SEL-3025 cryptographic transceiver at the remote end and the 915900225 PC Serial Security Kit at the engineering workstation. You can secure engineering access over an untrusted communications channel by adding cryptographic protection as follows:

- ➤ Install the 915900225 PC Serial Security Kit on the engineering workstations used for remote access.
- ➤ Install an SEL-3025 at the remote location between the remote device and the modem.

With the SEL-3025, legitimate communication still flows seamlessly between the master and remote devices. The transceiver blocks all unauthorized access to the protected master and remote intelligent electronic devices (IEDs).

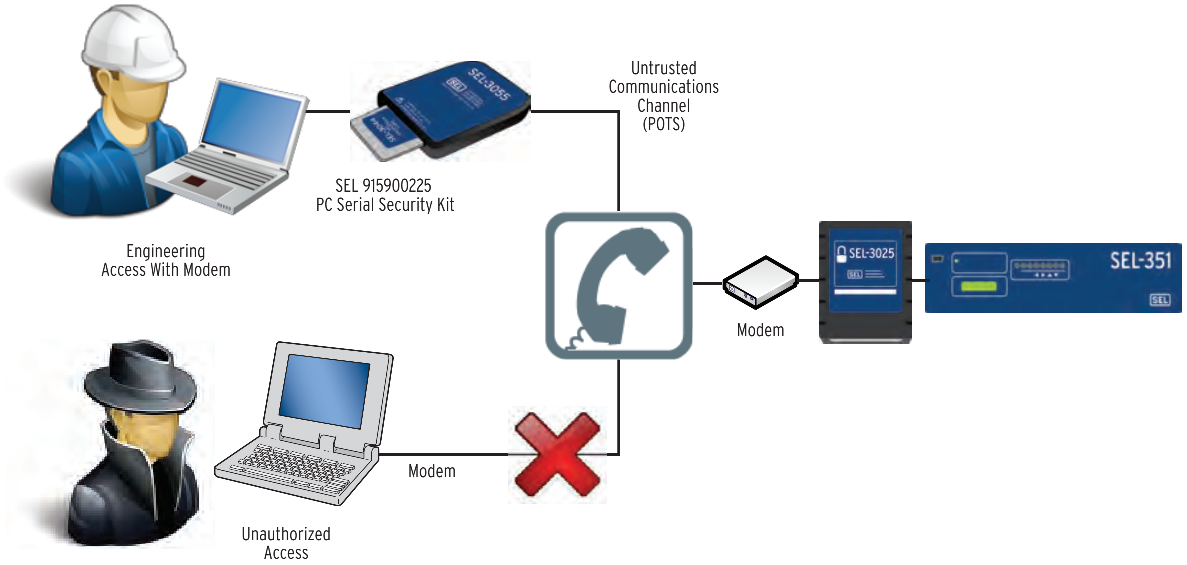

Untrusted Communications Channel (POTS)
SEL 915900225 PC Serial Security Kit
Engineering Access With Modem
Modem
SEL-3025
SEL-351
SEL-3055
Modem
Unauthorized Access

Figure 1.3 Secure SCADA Communications Channel

The SEL-3025, an EIA-232 bump-in-the-wire serial cryptographic transceiver, protects meters, protective relays, programmable logic controllers (PLCs), remote terminal units (RTUs), and personal computers (PCs) from unauthorized access, control, eavesdropping, or malicious attack by authenticating and optionally encrypting all data along the communications path.

- **Proven Cryptographic Serial Protocols.** Order Secure SCADA Communication Protocol (SSCP) to protect engineering access by authenticating every data packet on your serial link. Order Streaming Encryption Protocol (SEP) for the low latency necessary for real-time control and protection.
- **Ease of Use.** Simple configuration and maintenance with a secure web interface allows for convenient setup and management.
- **Seamless Integration.** Bump-in-the-wire design simplifies security retrofit of existing serial communications systems. Upgrade existing modems and radios to crypto-modems and crypto-radios.
- **Flexible Network Architectures.** The SEL-3025 is ideally suited for point-to-point, multidrop, and many-to-many networks.
- **Syslog.** Log events with Syslog for consistency, compatibility, and centralized collection.
- **User-Based Access Control.** Strong access control and individual user accountability.
- **Reliability.** The SEL-3025 is built for availability, hardened for the substation, and covered by a 10-year warranty.

Application Overview

The SEL-3025 is the perfect choice for application in point-to-point, multidrop, and many-to-many networks.

Point-to-Point

Figure 1.4 shows typical point-to-point applications including radios, dial-up modems, fiber-optic modems, and cellular modems. SEL-3025 transceivers use cryptographic protocols to authenticate all data between the two endpoints. The SEL-3025 transceivers also prevent unauthorized access to either endpoint by rejecting all session requests that are not initiated by the authorized source.

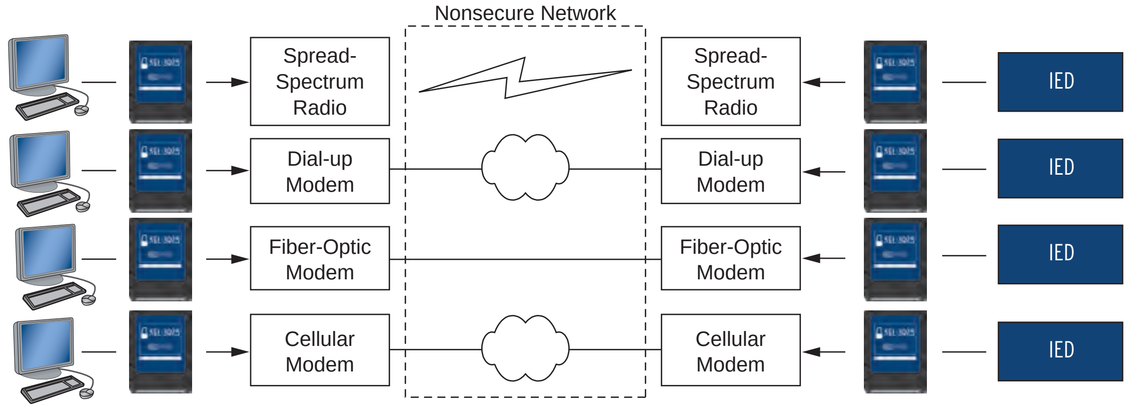


Figure 1.4 Point-to-Point Applications

Multidrop

Many common SCADA systems are configured in a multidrop network architecture in which several devices share a channel. On such a channel, the communications protocol must be designed to avoid collisions and transmission errors that occur when multiple devices attempt to transmit on a shared channel at the same time. Multidrop SCADA systems use a master device to coordinate communication by periodically requesting data from, and sending control commands to, RTUs or IEDs. These master-initiated polling cycles are designed to avoid collisions on the shared transmission channel.

The SEL-3025 is specifically designed to operate in multidrop architectures. In *Figure 1.5*, SEL-3025 devices are installed at the master and remote sites. The master cryptographic transceiver coordinates the exchange of session keys with each remote cryptographic transceiver in the system. This coordinated exchange of session keys avoids data collisions while ensuring that a unique cryptographic key authenticates and protects each connection.

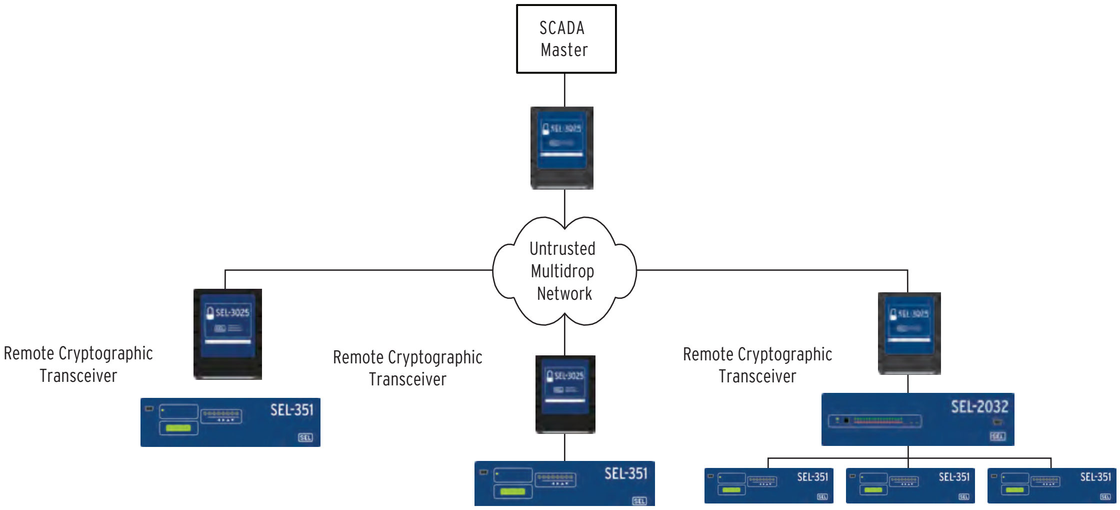

SCADA Master
SEL-3025
Untrusted Multidrop Network
Remote Cryptographic Transceiver
SEL-3025
SEL-351
Remote Cryptographic Transceiver
SEL-3025
SEL-351
Remote Cryptographic Transceiver
SEL-3025
SEL-2032
SEL-351
SEL-351
SEL-351

Figure 1.5 Multidrop Application

Many-to-Many

Many-to-many network structures are used when there are many users with authorized access to many different endpoints. One session can be established between a user and an endpoint at a given time. Once a user connects with an endpoint device, the SEL-3025 performs as described in a point-to-point application. Sessions through the Serial Shield devices are unique to individual users in a many-to-many network structure. They therefore provide an individual audit trail within each Serial Shield device that can be used to correlate events (such as settings changes on a remote IED) to an individual.

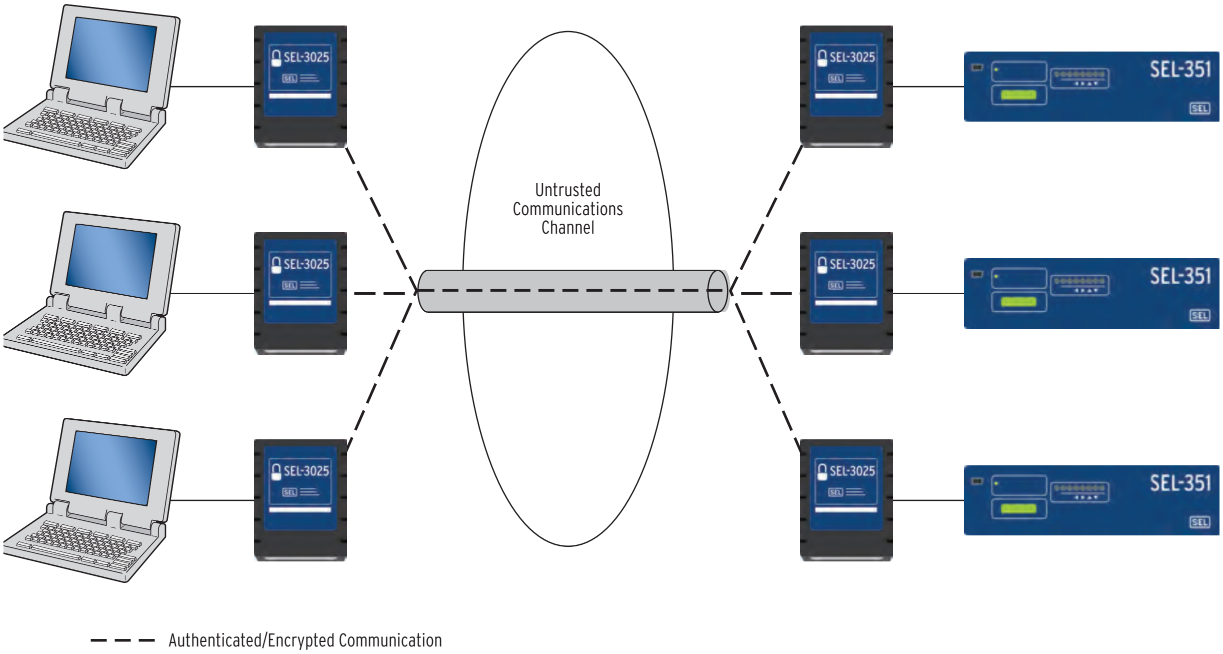

SEL-3025
SEL-3025
SEL-3025
Untrusted Communications Channel
SEL-3025
SEL-3025
SEL-3025
SEL-351
SEL-351
SEL-351
Authenticated/Encrypted Communication

Figure 1.6 Many-to-Many Application

Functional Description

The SEL-3025 cryptographic transceiver provides the physical interface between the device requiring protection and the untrusted communications channel. It also provides the user interface for all configuration settings. The SEL-3025 adds security to control system communications for both control system data and engineering access data by using SSCP or SEP encryption.

SEL-3025 Communications Interfaces

The cryptographic transceiver has two EIA-232/RS-232 serial communications ports that use an RJ45 form factor. The data communications equipment (DCE), also called the trusted interface, connects to a trusted device (i.e., equipment with information requiring protection). The trusted interface and trusted device send and receive data among themselves with no cryptographic security. The data terminal equipment (DTE), or untrusted interface, connects to an untrusted serial network either directly or through communications equipment, such as a modem. Data sent from the trusted device are passed securely over the untrusted interface to the other end of the untrusted serial network. The receiving cryptographic transceiver then accepts the secured data on the untrusted interface, processes the data, and passes the data on to the destination device connected to its trusted port. The SSCP provides cryptographic security that protects all communication sent over the untrusted network.

An RJ45 Ethernet interface, the Ethernet Management Port (**ETH MGMT**), provides secure management through an HTTPS web interface. The HTTPS web interface allows authorized system operators to monitor the local and remote interface channel health and to program system parameters. This user interface also allows operators to monitor channel health and to program system parameters of any other trusted Serial Shield on the same serial network.

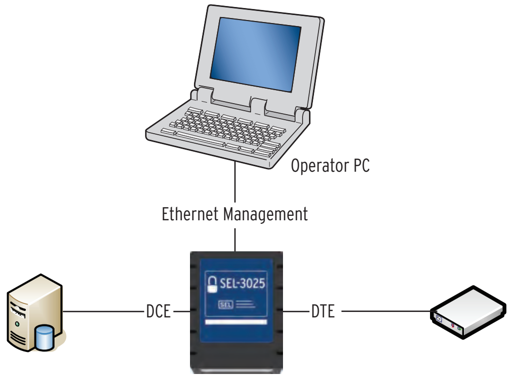


Figure 1.7 SEL-3025 Ports

The SEL-3025 includes many proven technologies to provide for a reliable method of securing sensitive communications. Many of these technologies are new to control systems and may require further explanation. For detailed information on these technologies, please refer to the appropriate appendices included in this manual.

Secure SCADA Communications Protocol (SSCP)

SSCP is a cryptographic protocol used to authenticate and encrypt information exchanged over untrusted communications channels. Serial messages are encapsulated in SSCP packets, which the local SEL-3025 then sends over the communications path to the remote SEL-3025 specified in the DESTINATION field of the SSCP packet header. The remote SEL-3025 validates the received SSCP packet and extracts the data to be sent to the attached device (IED, RTU, PLC, etc.). The remote SEL-3025 logs and reports as errors any unauthenticated packets and blocks the message in the payload from being passed on to the protected device. This prevents a malicious user from passing unauthorized commands to the remote device attached to the SEL-3025 Serial Shield.

All SSCP packets start with the same 10-byte header format, as shown in *Table 1.1*.

Table 1.1 SSCP Header Format

0	1	2	3	4	5	6	7	8	9
SYNC TOKEN		VERSION	DESTINATION		SOURCE		PAYLOAD TYPE	LENGTH	

SYNC TOKEN: The synchronization tokens are the leading two bytes of all SSCP packets. The two bytes are defined as 0x16 and 0x75 to signal the start of an incoming SSCP packet.

VERSION: The VERSION field holds the version of the SSCP protocol in use. Presently, the only version is 1.

DESTINATION: The DESTINATION field contains the two-byte SSCP address of the device that will receive the packet.

SOURCE: The SOURCE field contains the two-byte SSCP address of the device sending the packet.

PAYLOAD TYPE: The one-byte PAYLOAD TYPE field specifies the type of the packet and indicates the type of payload to expect. *Table 1.2* lists the valid payload types.

LENGTH: The two-byte LENGTH field specifies the size of the packet in bytes, not including the 10-byte SSCP header.

Table 1.2 SSCP Payload Types

Value	Payload Type
0x01	Data
0x02	Session Establish Request
0x03	Authentication Challenge
0x04	Authentication Response
0x05	Preshared Key Exchange
0x06	Diffie-Hellman Key Exchange
0x07	Close
8–199	Reserved
200–255	Vendor-Defined

The SSCP protocol uses a keyed hashed message authentication code (HMAC) to authenticate communication between devices. The HMAC, appended to normal data messages and other SSCP-specific packets, allows the receiving device to authenticate the data and the source for each packet in an SSCP communications session. The receiving device must “hold back” the message before sending it to the protected device, because the receiving device must first receive the message and associated authentication information in entirety to verify message authenticity and data integrity. This method causes a latency that is determined by the length of the message and the algorithm that generates the HMAC. HMACs can be truncated to reduce latency at the cost of a less secure communications channel.

Table 1.3 shows a typical SSCP data packet.

Table 1.3 SSCP Data Packet Format

0–9	10	11	12	13	14	...	...	...	...
SSCP Header	Data Type	Sequence Number		Data (variable length)			HMAC (variable length)		

In SSCP communication, encryption is an option for data confidentiality. In SSCP communication, to provide data confidentiality, SSCP supports AES-128 and AES-256 for encryption in AES CTR mode. SHA-1 and SHA-256 cryptographic HMAC algorithms provide data authenticity and integrity.

Streaming Encryption Protocol (SEP)

The Streaming Encryption Protocol (SEP) is used to encrypt information over untrusted communications channels when latency (delay introduced by the encryption process) is an issue. SEP uses the Advanced Encryption Standard (AES) cryptographic algorithm with a key length of 256 bits. The National Institute of Standards and Technology (NIST) has approved this algorithm as a secure means of encrypting data. The design of the random number generator the SEL-3044 uses for key generation ensures that all 1.2 • 10^{77} possible key values are equally likely. It is widely accepted throughout the cryptographic community that it is not realistically possible to mount a successful brute force (key guessing) attack on such a key space with presently available technology.

Key Management

- **System key (256 bits):** Your information technology (IT) professional or system administrator sets the system key. Use the system key to encrypt and securely transmit unique session keys (see the following). This key also provides a cryptographic authentication mechanism for rejecting session requests by unauthorized stations.
- **Session key (256 bits):** Use session keys to encrypt all protected user data prior to transmission. The SEL-3044 produces session keys at system startup and periodically during sessions. Session keys are generated through the use of an FIPS 186-2 compliant process that incorporates an integrated physical random number generator and a statistical data-whitening algorithm. Session keys are purely random and are not linked to the system key. The use of periodically changed session keys limits the amount of data the SEL-3044 encrypts with a single key value, thus strengthening the system against cryptanalytic attack. The SEL-3044 uses the system key to encrypt session keys prior to exchanging these keys among SEP peers.

Device Security

- **Strong Session Keys:** The SEL-3044 cryptography module incorporates a hardware random number generator and an FIPS-approved data whitener to guarantee that session keys contain the full key length of entropy (i.e., are completely random). This guarantees protection of encoded messages with a true cryptographic strength of 256 bits.

- **Decommissioning Procedure:** If necessary, you can reset the entire device to factory-default settings. This allows you to reinitialize the system key should you need to change the security parameters because of IT security procedures or a lost system key value.

Data Latency

SEP provides reliable and secure data communications while minimizing the communications delays (data latency) resulting from the addition of devices. *Figure 1.8* shows a local and a remote SEL-3025 Serial Shield communicating over a nonsecure network. Each SEL-3025 uses an SEL-3044 encryption card for all cryptographic operations. At time t_0 the local SEL-3025 begins receiving a single SCADA frame on its local interface (i.e., the local SEL-3025 begins receiving the first byte of the frame at this time). At time t1 the remote SEL-3025 has received and finished processing the first byte of the same SCADA frame and begins transmitting the byte to the protected device attached to its local interface. The time difference, t_1–t_0, represents the total communications delay resulting from the insertion of the two SEL-3025 transceivers into the data path. There are two sources for this introduction of latency: data buffering and transmission of cryptographic overhead resulting from the SEP protocol (cryptographic headers at the beginning of each frame).

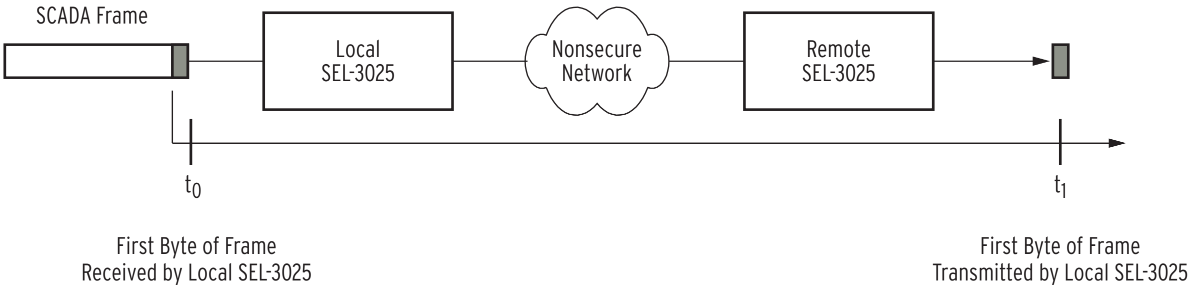

SCADA Frame
Local SEL-3025
Nonsecure Network
Remote SEL-3025
t_0
t_1
First Byte of Frame Received by Local SEL-3025
First Byte of Frame Transmitted by Local SEL-3025

Figure 1.8 Data Transmission Latency

The pair of transceivers introduces two byte times of latency to the communications path (one per device) as a result of buffering in the reception universal asynchronous receiver/transmitters (UARTs). For most common SCADA protocols, SEP will also add three bytes of cryptographic overhead to each frame. These two effects combine to introduce five byte times of communications latency. *Table 1.4* shows the approximate latency a pair of SEL-3025 transceivers introduces for an EIA-232 configuration with a single start bit and a single stop bit.

Table 1.4 Communications Latency

Data Rate, BPS	Latency (t_1 - t_0), Milliseconds
300	167
1200	42
2400	21
4800	10
9600	5.2
19200	2.6
38400	1.3

HTTPS Web Interface

The SEL-3025 uses Hypertext Transfer Protocol Secure (HTTPS) to provide a method to securely administer the device. Access to the HTTPS interface is through the Ethernet Management Port (ETH MGMT). Transport Layer Security (TLS) provides cryptographic functions in the Serial Shield HTTPS interface. Each SEL-3025 holds a server-side X.509 certificate to authenticate itself to incoming session requests while the user authenticates through an individually assigned username and password. This method establishes a mutually authenticated connection.

This HTTPS interface allows system operators to monitor the local and remote interface, to monitor channel health, and to program the system parameters of the device without removing the SEL-3025 from service or interrupting data transfer operations. This HTTPS interface also allows operators to use a remote management client, as seen in *Figure 1.9*, to monitor the channel health and program the system parameters of any other trusted SEL-3025 devices on the same serial network.

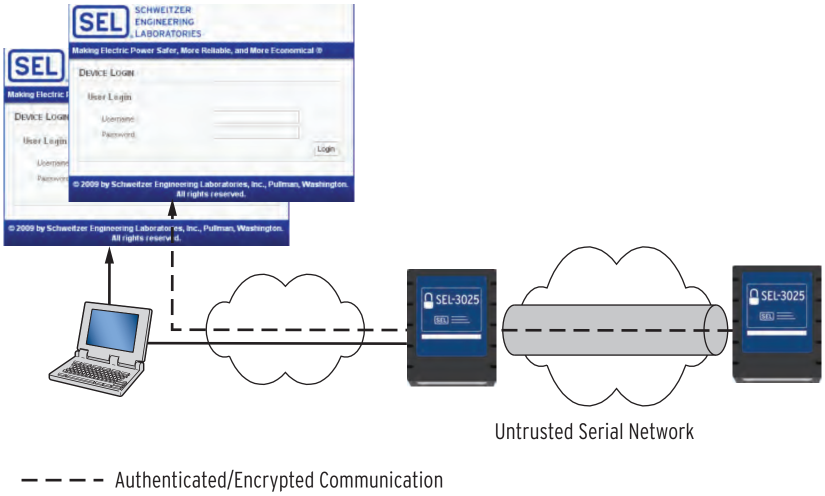

SEL SCHWEITZER ENGINEERING LABORATORIES
Making Electric Power Safer, More Reliable, and More Economical ®
Device Login
User Login
Username
Password
Login
© 2009 by Schweitzer Engineering Laboratories, Inc., Pullman, Washington. All rights reserved.
SEL-3025
SEL-3025
Untrusted Serial Network
Authenticated/Encrypted Communication

Figure 1.9 Nonintrusive HTTPS and Remote Management Client

X.509 Certificates

The SEL-3025 ships with a factory-installed X.509 certificate that the customer can change upon delivery. X.509 certificates are a part of the Internet's public key infrastructure (PKI). PKI involves two different, but mathematically related encryption and decryption keys, called public and private keys. A private key should only be known to its owner. As its name suggests, the matched public key can be distributed publicly.

When a private key is used to encrypt a message, only that message's public key can decrypt that message. The ability to decrypt the message with a specific public key provides a method for authenticating a sender. The decryption key is public, so it provides no confidentiality.

To obtain confidentiality with PKI, a sender must encrypt the message with the recipient's public key. The recipient's private key must be used to decrypt the message. This decryption provides for confidentiality, but not authentication, because the encryption key is public knowledge.

Combining the private key and public key systems can provide both confidentiality and authentication.

An X.509 certificate includes identifying information such as name, organization, country, etc. An X.509 certificate also includes an entity’s digital signature. This digital signature is encrypted with the entity’s private key. Only that entity knows its private key, and we can decrypt the digital signature with that entity’s public key, so we know to whom that X.509 certificate belongs. Please refer to *Appendix H: X.509* for additional information about X.509 certificates.

User-Based Accounts

The SEL-3025 has user-based accounts to improve the authentication, authorization, and accountability functions of the system. User-based accounts provide the ability to authenticate a user’s identity, rather than the user’s role. This authentication means that the system knows the identity of the person performing any action on the system, rather than the group to which that person belongs. Knowing the identity of a user makes event tracking and forensics much easier. User-based accounts also simplify password management.

Please refer to *Appendix D: User-Based Accounts* for additional information about user-based accounts.

Syslog

Syslog is a standard for forwarding log messages in an Internet Protocol (IP) network. The SEL-3025 logs all events in the Syslog format to provide for interoperability with other devices. More information on SEL-3025 logging is available in *Section 7: Settings and Commands* and *Section 8: Testing and Troubleshooting*. Please refer to *Appendix E: Syslog* for additional information about the Syslog format.

Secure Delivery and Deployment

SEL takes great care to ensure that the customer receives the SEL-3025 in a known secure state. We recommend in addition to the SEL precautions in place for delivery that the customer perform the following steps upon receiving the SEL-3025 transceiver.

Step 1. Inspect to make sure that the shipment packaging and seals have not been broken.

Step 2. Initialize the SEL-3025 in a secure place. We suggest that you are not networked or in an environment where those other than security officers can see settings.

Step 3. Use a known secure PC to initialize the SEL-3025.

Connections, Reset Button, and LED Indications

Figure 1.10 shows typical connections for the SEL-3025 Serial Shield.

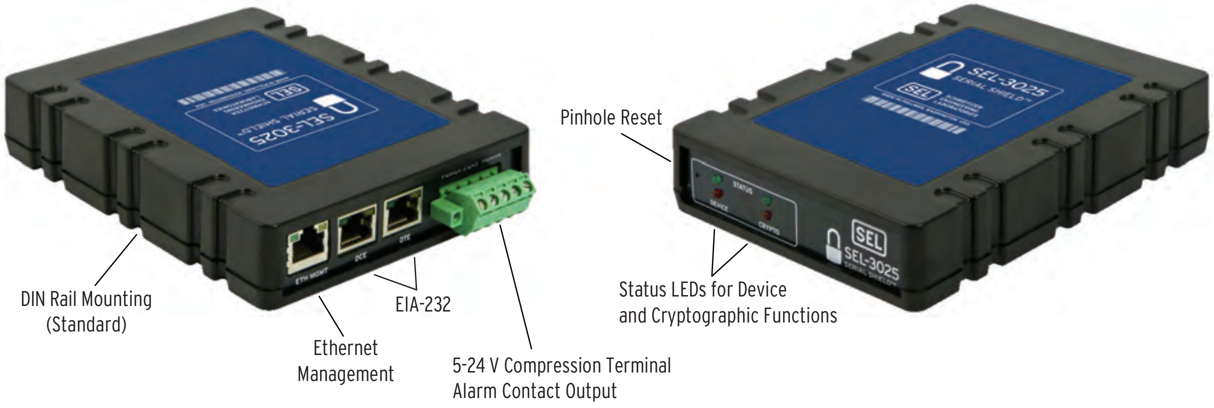


Figure 1.10 SEL-3025 Serial Shield

Mounting

The SEL-3025 is supplied with a mounting clip for attachment to a 35 mm Type O DIN rail attached to the underside of the unit. The clip can be detached by removing two screws.

For mounting multiple SEL-3025 units, order the Rack Mount Kit, part number 915900163. The kit includes a bracket that screws to the underside of the SEL-3025 to permit mounting of as many as 14 SEL-3025s on a 19" rack shelf. The rack shelf is SEL part number 925900160, a 19" shelf with mounting holes.

Power Supply Connections

You can apply 5 to 24 Vdc directly to the SEL-3025 power terminals, which are available as compression terminals. If the power source voltage is not within the 5 to 24 Vdc range, use an auxiliary power supply to provide 5 to 24 Vdc to the SEL-3025. See *Specifications* for power requirements.

Status LEDs

The SEL-3025 uses four light-emitting diodes (LEDs) to show the state of the device. Both the device and the cryptographic functions have one green and one red LED each. During normal operations, each of these indicators should be green. Red indicates a problem. The Ethernet, DCE, and DTE connectors on the back panel each have two LEDs to indicate data transmission to/from the SEL-3025. The Ethernet connector amber LED indicates that the network is connected, and the green LED indicates traffic on the network. For both the DCE and DTE connectors, the amber LED indicates data the SEL-3025 receives. The green LED indicates data the SEL-3025 transmits.

Refer to *Section 8: Testing and Troubleshooting* for more details.

Alarm Output Connections

The SEL-3025 has an alarm contact to alert you when its internal diagnostics fail, when a secure communications channel experiences errors, when a user logs onto the device, or when a user fails for three consecutive times to enter the password successfully. *Figure 1.11* shows the connections on the rear panel, including the alarm output connections.

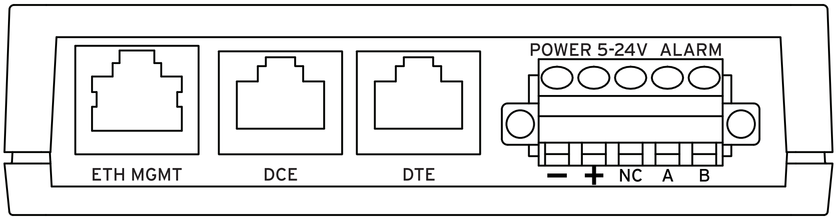


Figure 1.11 Rear Panel

The normally open alarm contact uses the connections **A** and **B**. Under normal operation it is closed, but it opens on alarm conditions. When the device is turned off, the alarm contact is open. The **NC** on the connector label denotes no connect, and this interface is not used internally.

The alarm contact is closed when you turn on the SEL-3025 and it has no diagnostic failures. For most diagnostic failures, the alarm contact opens and remains open. When a user successfully logs onto the SEL-3025 Serial Shield, the alarm contact pulses once (i.e., closed-open-closed). When a user fails three consecutive times to enter the password correctly, the SEL-3025 enters a lockout state for 30 seconds. During this time, that user cannot access the device. When lockout occurs, the SEL-3025 pulses the alarm contact for one second.

Serial Port Pinout Connection

The SEL-3025 has both a fully compliant EIA-232 DTE and a DCE serial port. SEL offers many cable configurations for use between the SEL-3025 and other devices.

The following tables list the serial port pinout descriptions for the DTE and DCE ports.

Table 1.5 RS-232/EIA-232 DCE Interface Pinout (RJ45)

Pin	Description
1	Data Set Ready/Ring Indicator (out)
2	Data Carrier Detect (out)
3	Data Terminal Ready (in)
4	Signal Ground
5	Receive Data (out)
6	Transmit Data (in)
7	Clear to Send (out)
8	Request to Send (in)

Table 1.6 RS-232/EIA-232 DTE Interface Pinout (RJ45)

Pin	Description
1	Data Set Ready/Ring Indicator (in)
2	Data Carrier Detect (in)
3	Data Terminal Ready (out)
4	Signal Ground
5	Receive Data (in)
6	Transmit Data (out)

Table 1.6 RS-232/EIA-232 DTE Interface Pinout (RJ45)

Pin	Description
7	Clear to Send (in)
8	Request to Send (out)

Ethernet Port Pinout Connection

The SEL-3025 uses a RJ45 Ethernet port capable of 10/100Mbps full duplex operation.

Table 1.7 Ethernet Management Port Pinout

Pin	Description
1	TX+ Transmit Data +
2	TX– Transmit Data –
3	RX+ Receive Data +
4	N/C
5	N/C
6	RX – Receive Data –
7	N/C
8	N/C

Reset Button

IMPORTANT: Pressing the RESET button erases all system configuration parameters and interrupts transmission of encrypted data until you reinitialize the SEL-3025 Serial Shield. See Initializing the SEL-3025 in Section 2: Installation.

Use the RESET button to reset the SEL-3025 to default settings and erase all stored data. Reset can only occur if the SEL-3025 is energized. You can access the RESET button through the small hole in the end of the SEL-3025 near the status LED. Use a paper clip or other similar device to press the RESET button for at least two seconds. This action resets the SEL-3025 to the factory-default state.

Software System Requirements

The SEL-3025 requires no proprietary software to configure or run. Perform all configuration and management of the SEL-3025 through the HTTPS web management interface. Because the SEL-3025 web management interface requires the use of strong cryptography, older browsers may not work. Use the following supported web browsers over an HTTPS session to access the web interface.

NOTE: Establishing a web session will take much longer when using a certificate with more than a 2048 bit key length. The Google Chrome browser cannot be used with 4096 bit certificates because it times out before connecting.

- ➤ Microsoft® Internet Explorer® 9 or greater
- ➤ Mozilla Firefox® 15 or greater
- ➤ Google Chrome® 10 or greater

General Safety and Care Information

General Safety Notes

The SEL-3025 is designed for restricted access locations. Limit access to qualified service personnel.

Do not install or operate the SEL-3025 in a condition other than what this manual specifies.

Cleaning Instructions

De-energize the SEL-3025 (by removing the power connection to both the power and alarm connection) before cleaning.

You can wipe down the case with a damp cloth. Use no solvent-based cleaners on plastic parts or labels.

Related Products

The SEL-3025 can be used with the following SEL products.

Plug-in Cryptographic Cards (SEL-3025 Ordering Option)

- **SEL-3045 Secure SCADA Card.** The SEL-3045 uses NIST-approved AES encryption and is FIPS 140-2 level 2 validated to secure remote engineering access communications with Secure SCADA Communication Protocol (SSCP).
- **SEL-3044 SEL Encryption Card.** The SEL-3044 uses NIST-approved AES encryption and is FIPS 140-2 level 2 validated to secure real-time data links with Streaming Encryption Protocol (SEP).

Remote Device Communications Encryption

- **915900225 PC Serial Security Kit.** Ideal for protecting engineering access that uses modems, the PC Serial Security Kit provides a USB card dock and PC software to allow a PC to use the SEL-3045 to encrypt a PC serial port for communicating with an SEL-3025.

Specifications

Compliance

ISO 9001:2008 Certified

UL Recognized to UL 294, 1076, and 1610 (File BP10155)

FIPS 140-2 level 2 Validation certificate 1488 and 1564

Indicators

Device Status:	Green and Red LEDs
Crypto Status:	Green and Red LEDs
EIA-232 communications:	Green and Yellow LEDs
Network (TCP/IP) communications:	Green and Yellow LEDs

Solid-State Output

100 mA continuous

250 Vdc or 120 Vac Operational Voltage

Maximum On Resistance:	50 Ω
Minimum Off Resistance:	10 MΩ
Insulation:	1500 Vdc
Wiring size:	14 AWG Max. 26 AWG Min. 0.4 mm Min. Insulation 105°C, 250 V Min.

Cryptographic Protocols

Authentication:	SHA-1, SHA-256
Encryption:	AES-128, AES-256
Key Exchange:	Diffie Hellman, AES Key Wrap
Management:	HTTPS, using X.509 certificates 1024 or 2048, Secure File Transfer

User-Based Accounts

Maximum Users:	32
Maximum Password Length:	128
Password Set:	All printable ASCII characters
User Roles:	Administrator, User Manager, Engineer, Monitor

Syslog

Storage for 2048 local Syslog messages.

Support for Syslog forwarding to two remote Syslog servers.

Serial Ports

Connectors:	RJ45 Female (DTE) RJ45 Female (DCE)
Data Rate:	1200 bps to 57600 bps
Interface:	EIA-232

Ethernet Port

Connector:	RJ45 Female 10/100BASE-T

Accessories

Power Adapter / Cable	The SEL 230-0604 power supply is designed to power the SEL-3025 from an AC source.
Communications Cables	For supporting data cables, use the SEL-5801 Cable Selector Program. Download the SEL-5801 Cable Selector Program for free at http://www.selinc.com.

Power Requirements

+5 to +24 Vdc:	<5 W

Operating Temperature Range

–40ºC to +85ºC (–40º to +185ºF)

0 to 95% humidity (noncondensing)

Dimensions

Height:	2.90 cm (1.14 in.)
Width:	11.43 cm (4.5 in.)
Depth:	16.22 cm (6.39 in.)

Type Tests

Electromagnetic Compatibility Emissions

Product Specific:	IEC 60255:2013; Section 7.1 CISPR 22:2008 CISPR 11:2010
Generic	FCC CFR 47:2008; Part 15 Severity Level: Class A

Electromagnetic Compatibility Immunity

Electrostatic Discharge:	IEC 60255-26:2013; Section 7.2.3 Severity Level: 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEC 61000-4-2:2008 Severity Level: 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEEE C37.90.3-2001 Severity Level: 2, 4, 8 kV contact; 4, 8, 15 kV air
Radiated RF:	IEC 60255-26:2013; Section 7.2.4 Severity Level: 10 V/m IEC 61000-4-3:2010 Severity Level: 10 V/m IEEE C37.90.2-2004 Severity Level: 35 V/m
Fast Transient/Burst:	IEC 60255-26:2013; Section 7.2.5 Severity Level: Zone A: 4 kV at 5 kHz, 2 kV at 5 kHz on communications ports IEC 61000-4-4:2012 Severity Level: 4 kV at 5 kHz, 2 kV at 5 kHz on communications ports

Surge Withstand Capability:	IEC 60255-26:2013; Section 7.2.6 Severity Level, Zone A: 2.5 kV peak common mode, 1.0 kV peak differential mode IEEE C37.90.1-2012 Severity Level: 2.5 kV oscillatory, 4 kV fast transient waveform
Conducted RF:	IEC 60255-26:2013; Section 7.2.8 Severity Level: 10 Vrms IEC 61000-4-6:2008 Severity Level: 10 Vrms

Environmental

Cold:	IEC 60068-2-1:2007 Severity Level: 16 hours at –40°C
Damp Heat, Cyclic:	IEC 60068-2-30:2005 Severity Level: 25° to 55°C, 6 cycles, Relative Humidity: 95%
Dry Heat:	IEC 60068-2-2:2007 Severity Level: 16 hours at +85°C
Mechanical:	IEC 60255-21-2:1988 Severity Level: Class 1 – Shock Withstand, Bump, and Class 2 – Shock Response IEC 60255-21-3:1993 Severity Level: Class 2 (Quake Response) IEC 60255-21-1:1988 Severity Level: Class 1 Endurance, Class 2 Response

Warranty

10 years

This page intentionally left blank

Section 2
Installation

Introduction

This section includes the following information:

- ➤ *Dimension Drawing*
- ➤ *Connecting to the SEL-3025*
- ➤ *Commissioning the SEL-3025*
- ➤ *Navigating the User Interface*

Dimension Drawing

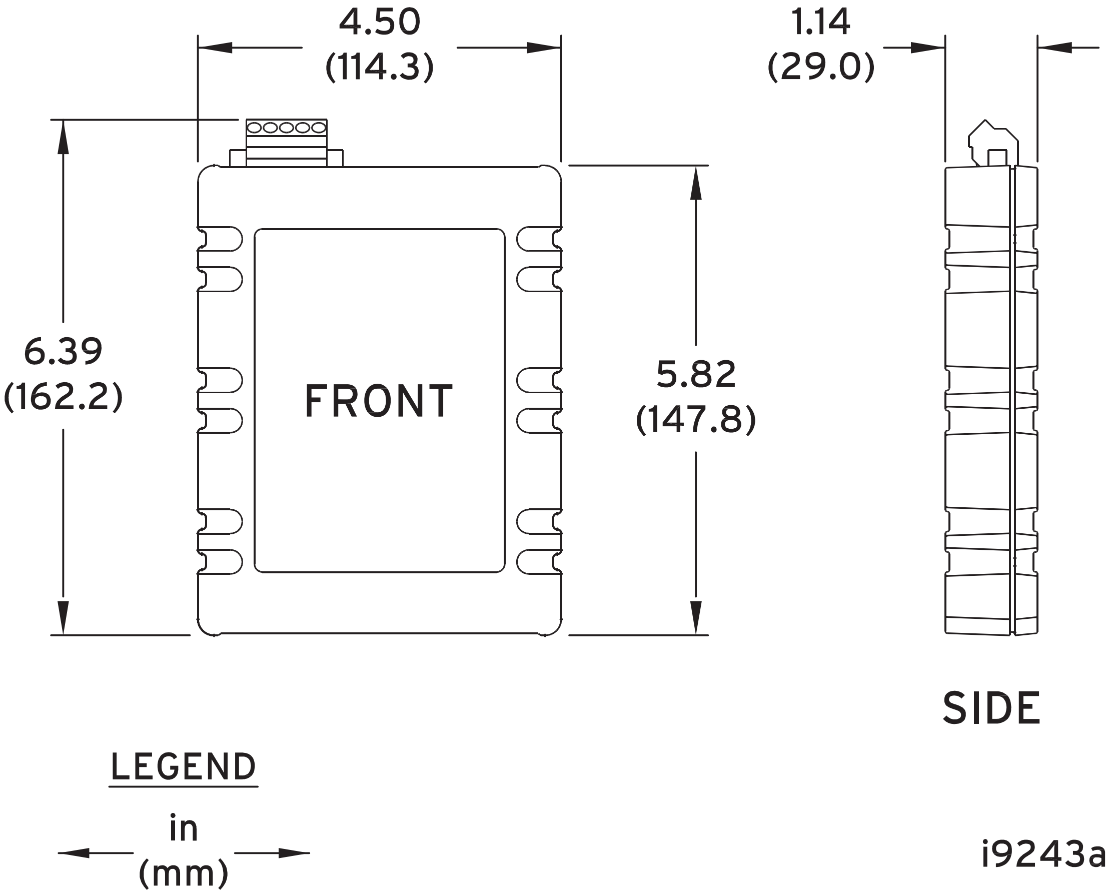


Figure 2.1 SEL-3025 Dimension Drawing

Connecting to the SEL-3025

The SEL-3025 Serial Shield® needs no special configuration software. The SEL-3025 includes an HTTPS web server for all management functions. You need only a standard web browser to connect to the SEL-3025. Tests have verified that the following web browsers work with the SEL-3025.

- Microsoft® Windows® Internet Explorer® 6, 7, 8
- Firefox® 2, 3, 4

For the initial connection to an SEL-3025, you will need the following:

- A computer with an RJ45 Ethernet port
- An uncommissioned SEL-3025
- One RJ45 Ethernet cable

The Physical Network

NOTE: The SEL-3025 is capable of autocrossover. This feature means that the SEL-3025 needs no hub or a crossover cable.

Connect the SEL-3025 to your computer, as shown in *Figure 2.2*. Using a standard RJ45 Ethernet cable, connect the Ethernet port of your computer directly to the **ETH MGMT** port of the SEL-3025. By default and following use of the recessed **RESET** button, the IP address on the **ETH MGMT** port is 192.168.1.2.

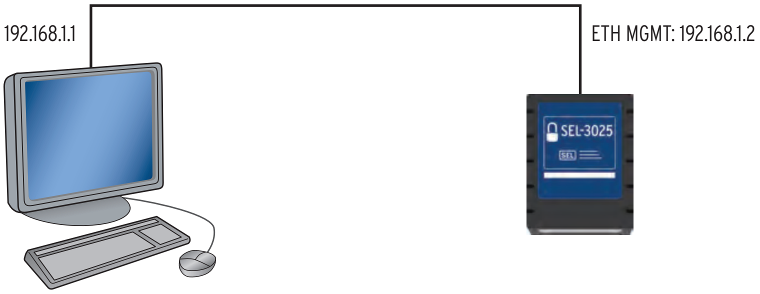


Figure 2.2 Commissioning Network

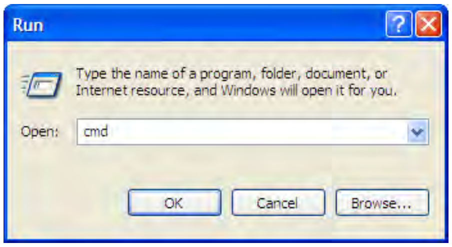
Configuring Microsoft Windows Networking

NOTE: Depending on your company's computer use policies and your user privileges, you may need the assistance of your IT department to configure networking on your workstation.

Confirm that your computer is configured to communicate on the 192.168.1.0/24 subnet. For a description of the Classless Inter-Domain Routing (CIDR) notation, please see *Appendix G: Classless Inter-Domain Routing (CIDR)*.

For additional information about Microsoft Windows networking, please see *Appendix F: Networking Fundamentals*.

Step 1. Start the Microsoft Windows Command Terminal. Use the Microsoft Windows **Run** function (from the **Start** menu) to run **cmd** (type **cmd** and click **OK**), as shown in *Figure 2.3*, to start the command terminal.

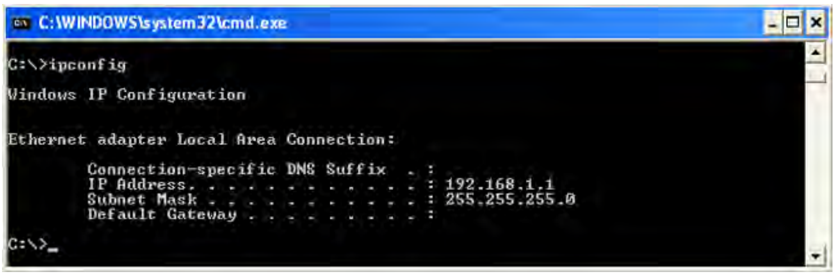

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

Figure 2.3 Open Terminal With Run Command

Step 2. In the command terminal, type **ipconfig <Enter>** as shown in *Figure 2.4*. This command will show the IP address and subnet mask for which your Ethernet connection is configured. The IP address must be in the 192.168.1.0/24 subnet (e.g., 192.168.1.1), and the subnet mask must match 255.255.255.0. If these values are correct, please skip to *Commissioning the SEL-3025*.

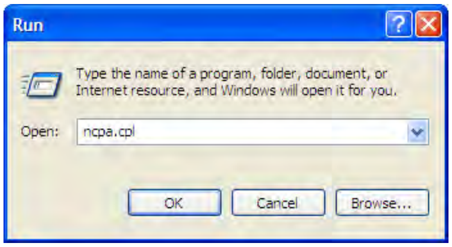


```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\>_
```

Figure 2.4 Windows IP Configuration

NOTE: Any IP address in the 192.168.1.0/24 subnet is acceptable except for 192.168.1.2, which is taken by the SEL-3025.

Step 3. If you need to configure your computer to communicate on the 192.168.1.0/24 subnet, then open Microsoft Windows Network Connections. Do this by typing **ncpa.cpl** in a command window or in the Windows **Run** dialog box, as shown in *Figure 2.5*.

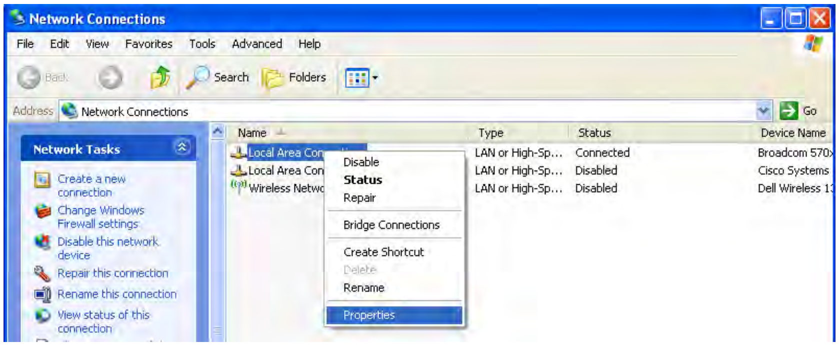


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: ncpa.cpl

Figure 2.5 Open Network Connections With Run Command

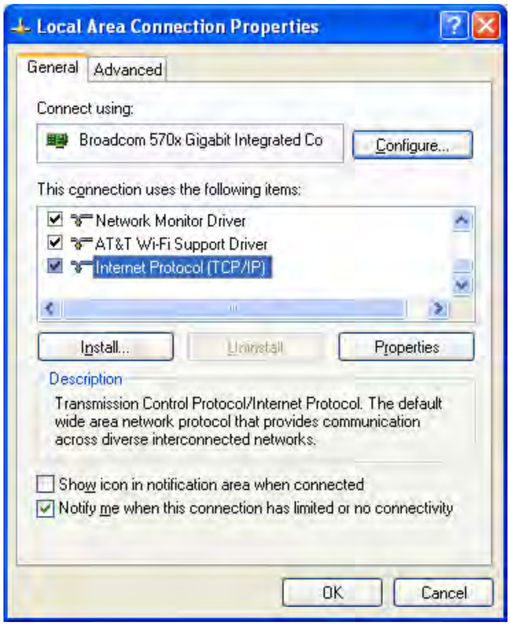
Step 4. Right-click on the connection you will be using to communicate with the SEL-3025 (Local Area Connection, for example), and select the **Properties** option.



Name	Type	Status	Device Name
Local Area Con	LAN or High-Sp...	Connected	Broadcom 570x
Local Area Con	LAN or High-Sp...	Disabled	Cisco Systems
Wireless Netwo	LAN or High-Sp...	Disabled	Dell Wireless 1

Figure 2.6 Open Connection Properties

Step 5. Select the **Internet Protocol (TCP/IP)** entry (usually the last listed) from the list in the **This connection uses the following items** area. Click the **Properties** button.



Local Area Connection Properties

General | Advanced

Connect using:

Broadcom 570x Gigabit Integrated Co

Configure...

This connection uses the following items:

☑ Network Monitor Driver
☑ AT&T Wi-Fi Support Driver
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

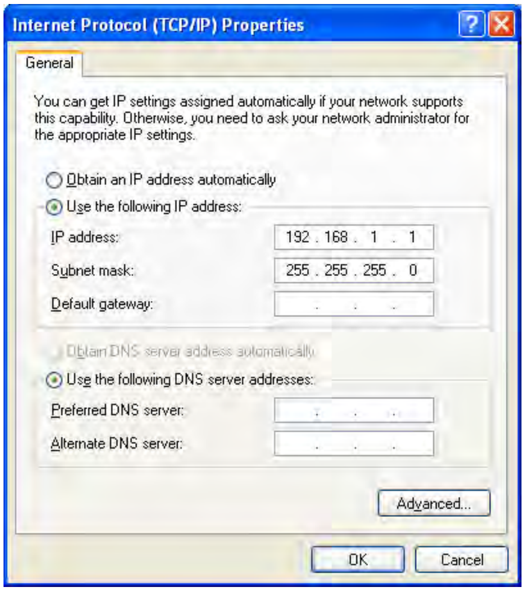
□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

OK | Cancel

Figure 2.7 Local Area Connection Properties

Step 6. Click the radio button labeled **Use the following IP address**.

Step 7. Enter **192.168.1.1** as the IP address and **255.255.255.0** as the subnet mask, as shown in *Figure 2.8*. Click the **OK** button.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

OK | Cancel

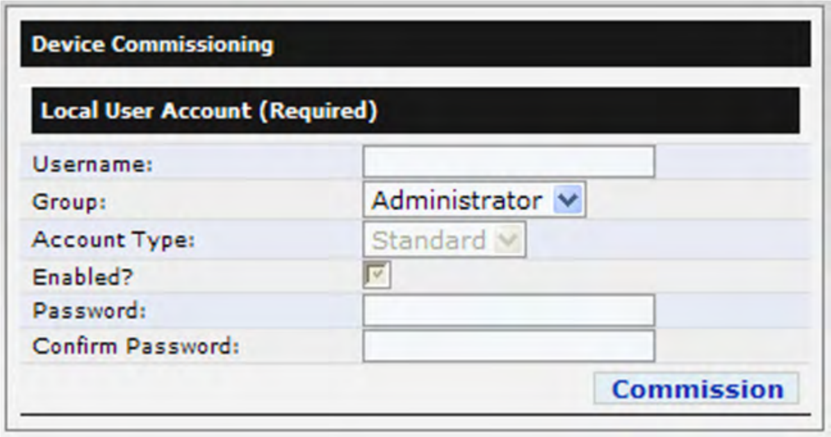
Figure 2.8 Internet Protocol (TCP/IP) Properties

Commissioning the SEL-3025

The SEL-3025 has a default IP address of 192.168.1.2 assigned to the ETH MGMT port. To connect to the SEL-3025, open your preferred web browser.

NOTE: Before the commissioning page loads, you will likely receive an error message stating that this site uses an invalid certificate. You must make an exception to accept this certificate. Your browser will provide you with the instructions for the exception.

Step 1. In your browser's address bar, enter **https://192.168.1.2** to open the SEL-3025 **Device Commissioning** Page.



Device Commissioning

Local User Account (Required)

Username:	
Group:	Administrator
Account Type:	Standard
Enabled?	☑
Password:	
Confirm Password:	

Figure 2.9 SEL-3025 Device Commissioning Page

NOTE: It is recommended that the default certificate be changed with your organization's issued certificate for this device. It is good practice to remove any default credentials. This certificate is the only default credential the SEL-3025 is manufactured to have.

NOTE: Usernames are unique on the SEL-3025. The same username cannot be used for multiple accounts. Once a username is taken, no other account can be created with that username unless the existing account is deleted. Usernames are not case sensitive.

NOTE: The SEL-3025 requires use of complex passwords. Passwords must be at least eight characters in length and require at least one character from each of the following character sets. Spaces are allowed.

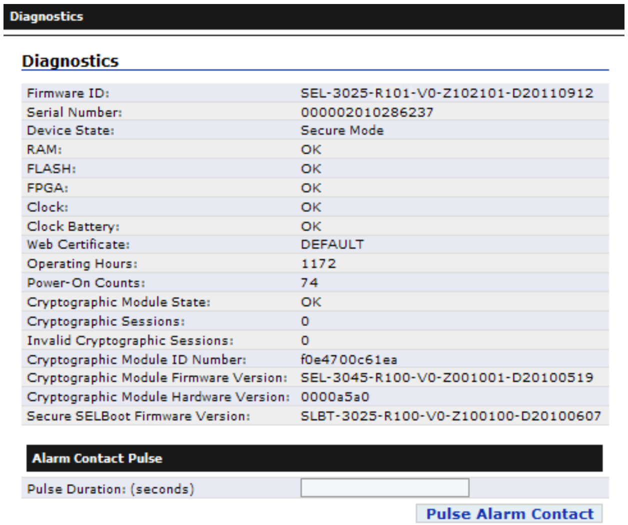
- ➢ Lowercase letters
- ➢ Uppercase letters
- ➢ Numbers
- ➢ Special characters (any printable character that is not alphanumeric)

Step 2. Enter the account information for an administrative user. This entry includes the username and password.

Step 3. Click the **Commission** button.

Navigating the User Interface

The SEL-3025 has an HTTPS interface to allow device administration without you needing to install any management software on your PC. Access this HTTPS interface by opening your favorite supported web browser and navigating to the SEL-3025 management address. By default, this address is https://192.168.1.2.



Diagnostics

Diagnostics

Firmware ID:	SEL-3025-R101-V0-Z102101-D20110912
Serial Number:	000002010286237
Device State:	Secure Mode
RAM:	OK
FLASH:	OK
FPGA:	OK
Clock:	OK
Clock Battery:	OK
Web Certificate:	DEFAULT
Operating Hours:	1172
Power-On Counts:	74
Cryptographic Module State:	OK
Cryptographic Sessions:	0
Invalid Cryptographic Sessions:	0
Cryptographic Module ID Number:	f0e4700c61ea
Cryptographic Module Firmware Version:	SEL-3045-R100-V0-Z001001-D20100519
Cryptographic Module Hardware Version:	0000a5a0
Secure SELBoot Firmware Version:	SLBT-3025-R100-V0-Z100100-D20100607

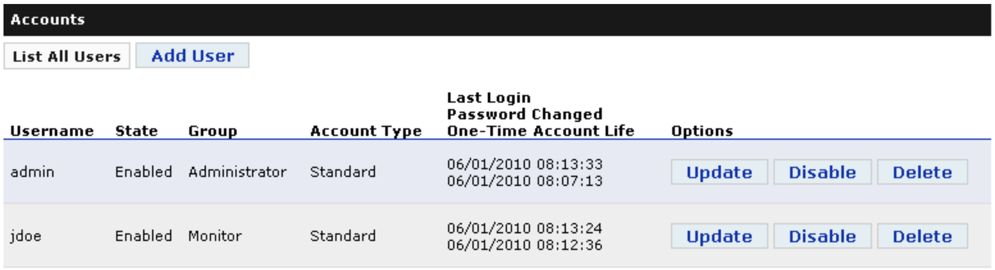
Alarm Contact Pulse

Pulse Duration: (seconds)

Figure 2.10 SEL-3025 Diagnostics Page

When you log in to the SEL-3025, the device presents you with the **Diagnostics** page as shown in *Figure 2.10*. The **Diagnostics** page gives a quick overview of SEL-3025 status. You can also access the **Diagnostics** page by clicking the SEL logo shown on the top left corner of every page. For more information about the **Diagnostics** page, please refer to *Section 8: Testing and Troubleshooting*.

The far left frame of the SEL-3025 web interface is the navigation panel. Selecting any link on this panel will take you to the associated page that includes all the settings and configurations for that part of the system. The navigation panel is always present on the web interface. Clicking on the **Accounts** link in the navigation panel displays the **Accounts** page as shown in *Figure 2.11*.



Accounts

Username	State	Group	Account Type	Last Login Password Changed One-Time Account Life	Options
admin	Enabled	Administrator	Standard	06/01/2010 08:13:33 06/01/2010 08:07:13	Update Disable Delete
jdoe	Enabled	Monitor	Standard	06/01/2010 08:13:24 06/01/2010 08:12:36	Update Disable Delete

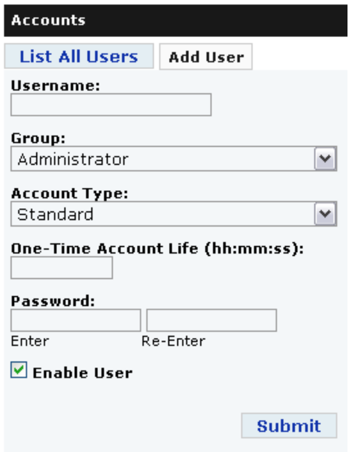
Figure 2.11 User Accounts

The **Accounts** page shown in *Figure 2.11* shows the main panel of the web interface. The main panel will change depending on which part of the system you are viewing. Many pages provide in the main panel a table such as that seen in *Figure 2.11*.

The main panel is where the device displays all configuration information. In *Figure 2.11*, we can see that this SEL-3025 is configured for two users: admin and jdoe. We can also see the status of each user account and details about the two users.

You can perform actions from the main panel. Each page has different buttons to perform actions specific to that page. Notice that the **Accounts** page has an **Add User** button above the table. There are also action buttons specific to each user in the table. Selecting any of these buttons will cause the SEL-3025 to perform the associated action.

Click the **Add User** button to display a dialog box such as in *Figure 2.12*. Use such dialog boxes for making configuration changes.



Username:

Group: Administrator

Account Type: Standard

One-Time Account Life (hh:mm:ss):

Password:
Enter
Re-Enter

☑ **Enable User**

Figure 2.12 Add User

Section 7: Settings and Commands provides detailed information about each of the webpages and their settings.

This page intentionally left blank

Section 3

Managing Users

Introduction

This section includes the following:

- ➤ *User-Based Accounts*
- ➤ *Adding a User*
- ➤ *Resetting a Password*
- ➤ *Removing a User*
- ➤ *Enabling or Disabling a User*
- ➤ *Changing a User Password*

User-Based Accounts

The SEL-3025 Serial Shield® has user-based access control to provide for greater authentication, authorization, and accountability. Individuals responsible for configuring, monitoring, or maintaining the SEL-3025 will have their own unique user accounts. User-based access controls allow flexibility for detailed auditing organized to answer, “Who did what and when?” This structure also eases the burden of password management for the operators by only requiring users to remember their own personal passwords. This system eliminates the need for each operator to remember a new password every time an employee leaves or no longer needs access as necessary in a global account structure.

Operators in the Administrator or User Manager group are authorized to create, delete, or modify accounts. The SEL-3025 logs changes to accounts and links changes to the username of the individual making them. You can disable each user account to help administer temporary accounts or strengthen security when employees are on extended leave. You can also use one-time accounts to allow short-term access to the SEL-3025. The **Accounts** page defines the one-time account lifetime. Make adjustments for each one-time account from the **Accounts** page by clicking the **Update** button for the user's account you want to change and then editing settings on the dialog box that displays.

The SEL-3025 presents different views of the **Accounts** page depending on your account type. A user in the Administrator or User Manager group will see a list of all presently installed user accounts. The account list shows an account’s username, group, and dates associated with account creation, last login, and last password change. You can configure as many as 32 accounts on the SEL-3025.

There are five actions an administrator or user manager can perform on this page: update user, enable user, disable user, delete user, and add user. Perform the update, enable, disable, and delete functions with the buttons associated with each individual account. You can access the add user function with the **Add User** button above the account list.

The update function allows an administrator or user manager to change settings, including the password associated with a particular account. The update function is necessary for resetting a forgotten password.

The **Enable**/**Disable** button will change depending on whether the account is presently enabled or disabled. Use this feature to disable the account of users who temporarily do not need to access this device. Disabling accounts prevents access to the SEL-3025 by individuals who do not need access. When these individuals again need to use the SEL-3025, reenable their accounts to restore access. If a user will never again need access to this device, remove that user account from the system with the **Delete** button.

Commissioning of the SEL-3025 configured an administrative-level account. Use this account to view, add, edit, enable, disable, or delete users from the SEL-3025.

The SEL-3025 allows assignment of different groups to users. To view, add, edit, enable, disable, or delete users from the SEL-3025, one must be logged in with an account that is a member of the Administrator or User Manager group. To edit settings, one must be logged in with an account that is a member of either the Administrator or Engineer group. The SEL-3025 logs any configuration changes to the system users. *Table 3.1* lists the SEL-3025 groups with a description of the privileges assigned to each group.

Table 3.1 SEL-3025 Device Groups

Group	Description
Monitor	User accounts assigned to the Monitor group can: 1) View logs and status information 2) View settings 3) Change their own passwords
Engineer	User accounts assigned to the Engineer group can: 1) Change settings 2) Upgrade firmware 3) View all information 4) Acknowledge logs 5) Change their own passwords
User Manager	User accounts assigned to the User Manager group can: 1) Manage User Accounts 2) View all information
Administrator	User accounts assigned to the Administrator group can perform all the actions that are allowed for User Manager and Engineer users. Users of this group are able to perform any action on the SEL-3025.

Adding a User

The SEL-3025 supports as many as 32 unique user accounts. Please follow the steps below to create a new user account.

Step 1. Log in to the SEL-3025 with an account belonging to either the Administrator or the User Manager group. The account that you created during commissioning is one such account.

Step 2. Select the **Accounts** link from the left frame of the webpage. The link will bring up the SEL-3025 **Accounts** page. From this page, an administrator or user manager user can view, add, edit, enable, disable, or delete other users.

Step 3. Click **Add User** to show the dialog box in which you would add a user (see *Figure 3.1*).

NOTE: Usernames are unique on the SEL-3025. You cannot use the same username for multiple accounts. Once you assign a username, you can create no other account with that username unless you delete the existing account. Usernames are not case sensitive and can contain as many as 128 characters.

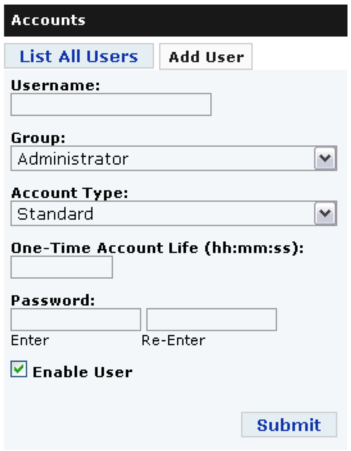
NOTE: The SEL-3025 requires use of complex passwords. Passwords must be at least eight following characters in length and require at least one character from each of the following character sets. Spaces are allowed.

- ➢ Lowercase letters
- ➢ Uppercase letters
- ➢ Numbers
- ➢ Special characters (any printable character that is not alphanumeric)

New users should change their password on their first login to the system. The change will ensure that they are the only individuals to know their passwords, and it will protect them from other users accessing their accounts.

Passwords should never be shared or written down. The effectiveness of any password relies on only one person knowing that password.

Step 4. Enter the Username, Group, Account Type, and Password of the new user. You will need to enter the Password twice to confirm that it is correct. New user accounts are enabled by default; you can uncheck the **Enable User** check box to disable a user account upon creation. Then, you can enable the account at a later date. Refer to *Section 7: Settings and Commands* for more information on user account settings.



Accounts

List All Users | Add User

Username:

Group: Administrator

Account Type: Standard

One-Time Account Life (hh:mm:ss):

Password: Enter Re-Enter

☑ Enable User

Submit

Figure 3.1 Add User Dialog Box

Step 5. Click the **Submit** button. This step will add the new user to the SEL-3025.

Resetting a Password

NOTE: If users forget their passwords, a user with administrator or user manager privileges must log in to the SEL-3025 and use the update user feature to reset the passwords. The first time users log in after a password reset, they should change their passwords. This method will ensure that they are the only individuals to know their passwords, and it will protect them from other users accessing their accounts.

The SEL-3025 provides a user with administrator or user manager privileges with the ability to edit account information for existing accounts. With this function, users can reset forgotten passwords, reassign group membership, and enable or disable an account. Please perform the following steps to reset an account’s password.

Step 1. Log in to the SEL-3025 with an account that is a member of the administrator or user manager group. The account you created during commissioning is one such account.

Step 2. Select the **Accounts** link from the left-hand frame of the webpage to display the **Accounts** page. From here, a user with administrator or user manager privileges can view, add, edit, enable, disable or delete other users.

Step 3. Click the **Update** button associated with the account that you want to edit. This step will open the dialog box from which you can update the user.

Step 4. To change the user’s password, enter the new password into the lower section of the dialog box and select the **Submit** button.

Removing a User

In the case where an employee leaves the company, you should remove the employee’s account to prevent security breaches. The SEL-3025 allows for the easy removal of user accounts. Please follow these steps to remove an account.

Step 1. Log in to the SEL-3025 with an Administrator or User Manager account. The account you created during commissioning is one such account.

Step 2. Select the **Accounts** link from the left frame of the webpage. This link will open the **Accounts** page from which you can edit user accounts. From here, a user with administrator or user manager privileges can view, add, edit, enable, disable, or delete other users.

Step 3. Click the **Delete** button associated with the account that you want to remove.

Step 4. Verify that the user to be deleted is the correct user.

Step 5. Once verified, click **Delete**. If this person is not the correct user, click **Cancel** to go back to the **Accounts** page.

Enabling or Disabling a User

If an employee takes an extended leave of absence or has a temporary change in duties, you should disable the employee’s account to prevent unauthorized access to the SEL-3025. Disabling the account will maintain the account information, while preventing unauthorized access to the system during the employee’s absence. You can then reactivate the account when the employee resumes normal duties. Please use the following steps to enable or disable a user’s account.

Step 1. Log in to the SEL-3025 with an account that is a member of the Administrator or User Manager group. The account you created during commissioning is one such account.

Step 2. Select the **Accounts** link from the left frame of the webpage. This link will open the **Accounts** page. From here, a user with administrator or user manager privileges can view, add, edit, enable, disable or delete other users.

Step 3. If an account is currently enabled, click the **Disable** button to disable the account. To enable an account that has been disabled, click the **Enable** button.

Changing a User Password

NOTE: The SEL-3025 requires use of complex passwords. Passwords must be at least eight characters in length and require at least one character from each of the following character sets. Spaces are allowed.

- Lowercase letters
- Uppercase letters
- Numbers
- Special characters (any printable character that is not alphanumeric)

Many organizations have policies requiring employees to change their system passwords at regular intervals. To accommodate these policies, users on the SEL-3025 can change their own passwords. Please use the following steps to change your password.

Step 1. Log in to the SEL-3025.

Step 2. Select the **Accounts** link from the left-hand frame of the webpage. This link will open the **Accounts** page. Users of the Monitor or Engineer group will only be able to see their own user information.

Step 3. Select the **Update** button associated with the user account to display the dialog box from which you can update users. From here, users can change their passwords by entering their new passwords as necessary.

Enter your new password twice, and click the **Submit** button to change your password.

This page intentionally left blank

Section 4

Using the PC Serial Security Kit to Protect Engineering Access Communication

Introduction

The 915900225 PC Serial Security Kit provides the hardware and software necessary for using your PC workstation to secure engineering access communications with remote SEL-3025 units. You will need to plug the SEL-3055 Card Dock into an available USB port on your computer and install the SEL-5025 Secure Port Service Software from the product CD.

If your SEL-3045 encryption card is already configured, you may not need to install configuration software. Otherwise, you will also need to install the ACSELERATOR QuickSet® SEL-5030 Software from the product CD before you can configure the card.

Set Up the Engineering Access Client

To use the PC Serial Security Kit, you will need to plug the SEL-3055 Card Dock into an available USB port on your computer and install the SEL-5025 Secure Port Service Software from the product CD.

If your SEL-3045 encryption card is already configured, you may not need to install configuration software. Otherwise, you will also need to install the ACSELERATOR QuickSet SEL-5030 Software from the product CD before you can configure the card. See *Section 5: Administering Engineering Access With ACSELERATOR QuickSet* for more information.

Install the SEL-5025 Secure Port Service Software

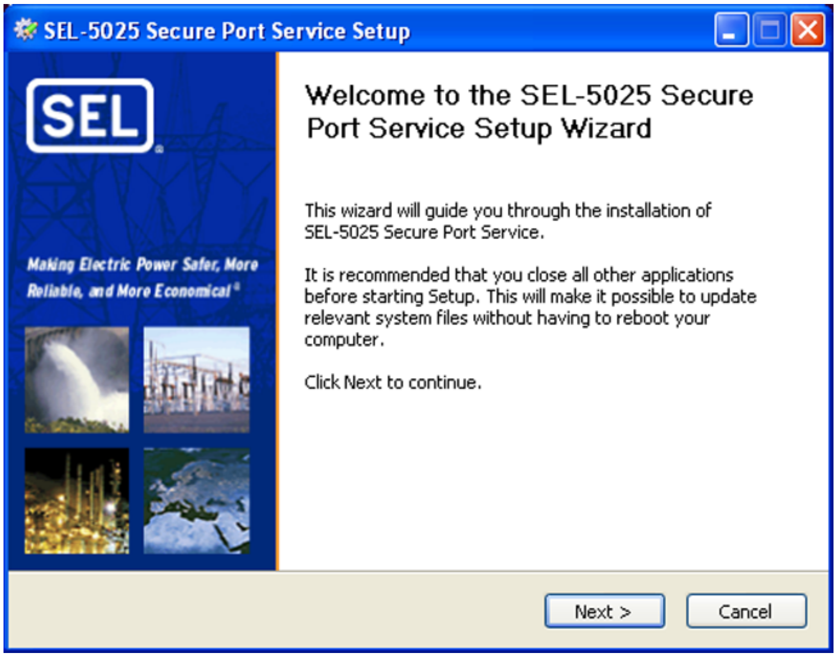
Step 1. Insert the CD into the drive.

Step 2. If Windows autorun is enabled, the installer will launch automatically. Otherwise, run **setup.bat** from the CD.

Step 3. On the installation page, click **Install SEL-5025 Secure Port Service**.

Step 4. The **SEL-5025 Secure Port Service Setup Wizard** (*Figure 4.1*) will guide you through the installation process. You must have 7.5 MB of available disk space for the SEL-5025 Secure Port Service Software.

NOTE: The SEL-5025 Secure Port Service software requires Microsoft .NET Framework Version 4 (http://www.microsoft.com/download/en/details.aspx?id=17851). If the .NET Framework Version 4 is not installed, you can install this software from the CD or have the installer download it from the Internet for you.


SEL-5025 Secure Port Service Setup
SEL
Making Electric Power Safer, More Reliable, and More Economical®
Next >
Cancel

Welcome to the SEL-5025 Secure Port Service Setup Wizard

This wizard will guide you through the installation of SEL-5025 Secure Port Service.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Figure 4.1 SEL-5025 Secure Port Service Software Installer

The default settings the wizard uses will install the SEL Secure Serial Port Service software in C:\Program Files\SEL\Secure Port Service\. The software includes the SEL-5025 Secure Port Service, as well as a tray application you can use for configuring the service and displaying its status. The default configuration for both the service and the tray application is to have these run automatically when your system starts. *Figure 4.2* shows the tray icon.

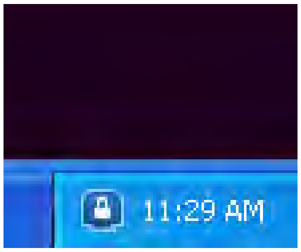


Figure 4.2 SEL-5025 Secure Port Service Software Tray Application Icon

TIP: You can find this service listed in the **Services** control panel applet (services.msc) as **SEL-5025 Secure Port Service**.

The SEL Secure Serial Port service adds a new virtual serial port to your computer. The Windows device manager (devmgmt.msc) lists the new port as **SEL Secured Communications Port** and assigns it to COM99 by default. You can use the tray application to configure the port number. This is the port to which your applications connect for secure communication with remote devices.

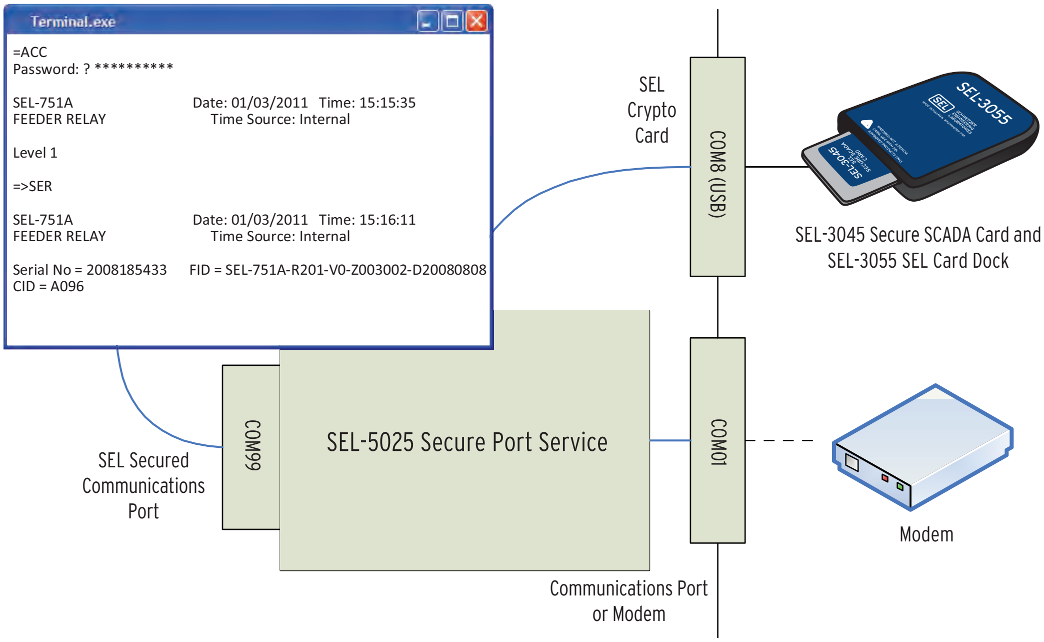
NOTE: The software creates and uses a second virtual serial port to communicate with the encryption card. This port is called "SEL-3045 Secure SCADA Card", and the software assigns to this port a port number greater than the numbers for the physical ports on the computer. You should not connect to this port.

Install the SEL-3055 Card Dock

Once you have installed the SEL-5025 Secure Port Service Software, plug the SEL-3055 card dock into an available USB port on your computer, and plug the SEL-3045 card into the dock.

Using the SEL-5025 Secure Port Service Software

The driver for the SEL-3055 Card Dock creates a serial port mapped to the USB port in which you have plugged the card dock and assigns it a port number greater than the numbers for the physical ports already on the computer. The SEL-5025 Secure Port Service Software creates a virtual (non-physical) serial port for communications applications to use. The service also assigns this port a port number greater than the port identification numbers on the computer, although you can change that assignment. *Figure 4.3* shows a typical situation, where a terminal application on the PC is using an external modem for secure communication. The modem is connected to the physical serial port, COM01, on the computer. The terminal program connects to the Secure Port Service virtual serial port, COM99, and is communicating normally. The Secure Port Service encrypts and decrypts data through the use of the SEL-3045 Secure SCADA Card in the card dock plugged into the USB port, which the service assigned to COM8.


Terminal.exe
SEL Crypto Card
COM8 (USB)
SEL-3055
SEL-3045 Secure SCADA Card and SEL-3055 SEL Card Dock
SEL Secured Communications Port
COM99
SEL-5025 Secure Port Service
COM01
Modem
Communications Port or Modem

```
=ACC
Password: ? **********

SEL-751A                    Date: 01/03/2011  Time: 15:15:35
FEEDER RELAY                   Time Source: Internal

Level 1

=>SER

SEL-751A                    Date: 01/03/2011  Time: 15:16:11
FEEDER RELAY                   Time Source: Internal

Serial No = 2008185433    FID = SEL-751A-R201-V0-Z003002-D20080808
CID = A096
```

Figure 4.3 Typical SEL-5025 Secure Port Service Software Connections

After you have installed the SEL-3055 card dock and software, you can use PC applications to encrypt communications to remote devices merely by selecting the new port when you choose the port you want to use for communication. Normally, your remote SEL-3025 units will have a consistent set of serial communications settings, and both this port and the physical serial port will have matching configurations.

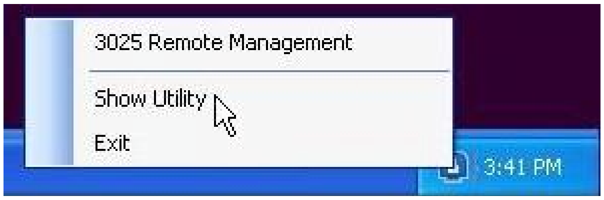
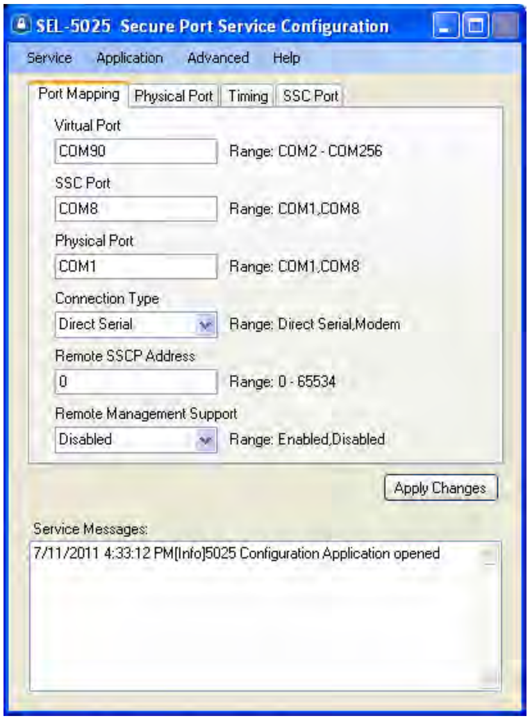


Figure 4.4 SEL-5025 Secure Port Service Software Tray Application Menu

Right-clicking on the icon in the tray (a blue icon with a white lock symbol) will open a context menu. Selecting **Show Utility** from this menu opens the application window, which displays the configuration application from which you can choose ports, configure physical communications ports, and view status messages. *Figure 4.5* shows the tray icon and the configuration application. You can also open this application window by double-clicking the tray icon. When configuration is complete, minimize the application to return it to the tray.



Virtual Port: COM90 Range: COM2 - COM256

SSC Port: COM8 Range: COM1,COM8

Physical Port: COM1 Range: COM1,COM8

Connection Type: Direct Serial Range: Direct Serial,Modem

Remote SSCP Address: 0 Range: 0 - 65534

Remote Management Support: Disabled Range: Enabled,Disabled

Service Messages:

```
7/11/2011 4:33:12 PM[Info]5025 Configuration Application opened
```

Figure 4.5 SEL-5025 Secure Port Service Software Tray Application

To configure the ports for communication, use the tray application (shown in *Figure 4.5*) to configure the speed, word format, and flow control options for the physical serial port to match your remote devices. Then use the communications program to select the secure port and configure its parameters to match exactly, as you would if you had connected directly to the physical port.

TIP: The **Remote Management Support** setting on the **Port Mapping** tab must match the setting for the remote device. To simplify the setup for engineering access, this setting should match for all SEL-3025 devices in your deployment that you will use for engineering access.

If you configure the **Connection Type** as **Modem**, the secure port will automatically keep communications in the clear (unencrypted) until a carrier is established, allowing you to communicate with your local modem for dialing purposes. It also detects the Hayes modem escape sequence, +++, which allows communications programs to regain control of the modem and hang up at the end of the session.

Section 5

Administering Engineering Access With ACSELERATOR QuickSet

Introduction

To use the SEL-3025 Serial Shield® to protect engineering access communications, you must use ACSELERATOR QuickSet® SEL-5030 Software to be able to provide encryption cards for members of your engineering staff and to configure each of your SEL-3025 serial shields to provide selected engineering personnel secure and traceable access. Through the use of ACSELERATOR QuickSet, you also reduce errors by simplifying the generation and management of the large and complex SSCP keys necessary for securing communication with a SEL-3025.

NOTE TO ADMINISTRATORS: The SEL-3045 and SEL-3025 are cryptographic devices. It is important to safeguard the deployment of cryptographic keys and protect key information from disclosure. SEL strongly recommends that you keep the computer and ACSELERATOR QuickSet installation you use for issuing SEL-3045 cards and for configuring SEL-3025 serial shields in a physically secure location and that you limit access strictly to those personnel responsible for SEL-3045 card deployment.

Figure 5.1 illustrates the architecture of a small sample engineering access deployment and demonstrates use of addresses and keys in a system. In the example, we have issued to three engineers encryption cards that uniquely identify and protect their communications with three protected devices. Alice, Bob, and Charlie each have a unique SSCP address and a unique SSCP key set.   They communicate with three protected devices by dial-up connection to remote modems.

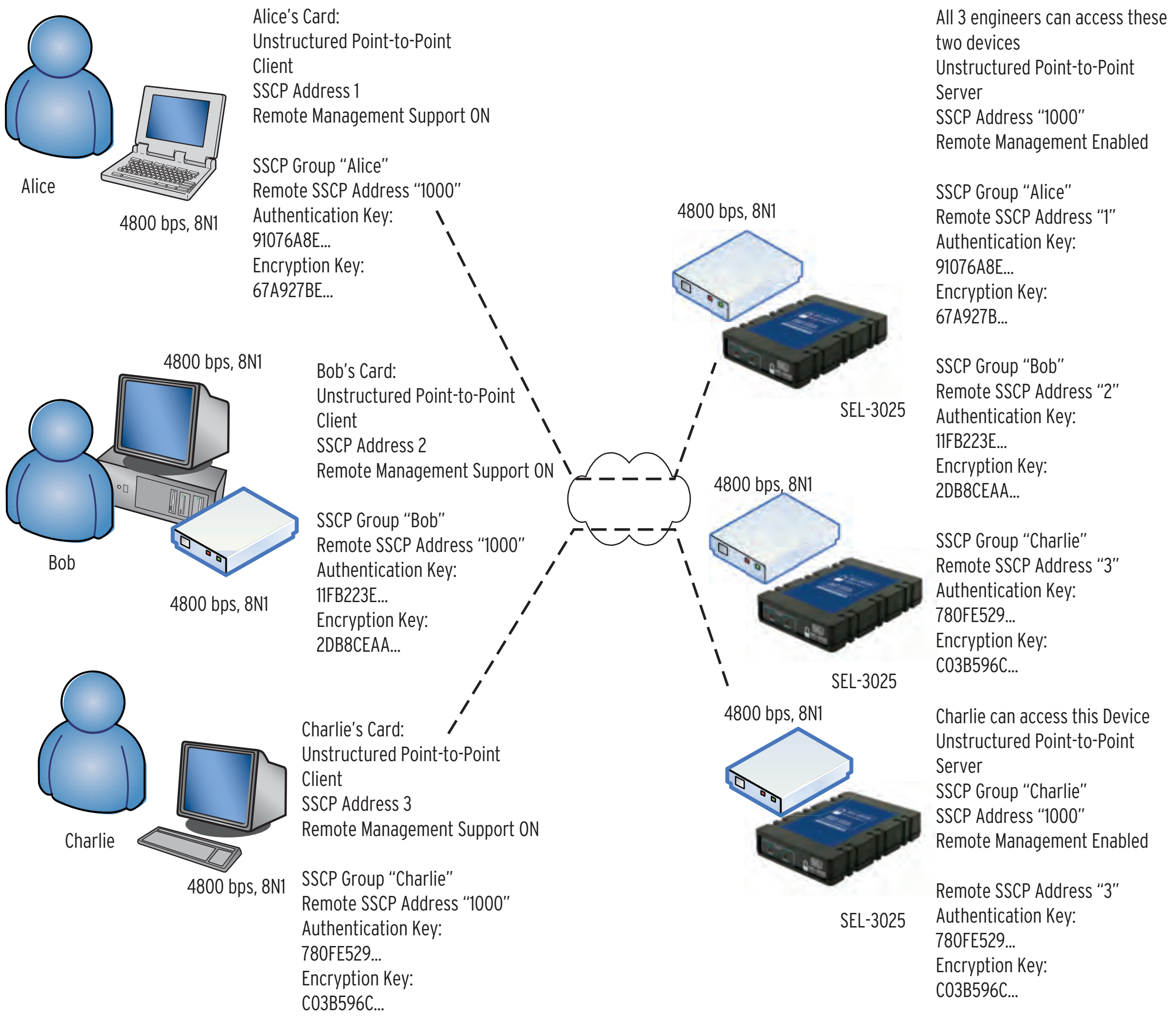


Figure 5.1 Engineering Access Architecture

TIP: Each SEL-3045 card in your deployment must have a unique address and pair of SSCP keys. To simplify deployment, each SEL-3025 transceiver you use for engineering access should have the same SSCP address, so that all cards only need to define a single SSCP group containing a single remote address and using their own SSCP key pair. Each of the SEL-3025 devices will have a separate SSCP group set up for every card with which they have authorization to communicate, configured with each card's SSCP key pair and SSCP address.

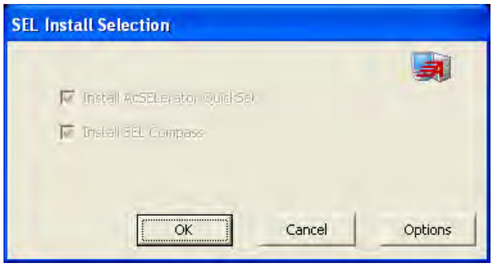
Configuration of the remote SEL-3025s permits all three engineers access to the top two devices, but only Charlie can access the one on the bottom. Note that all of the remote SEL-3025s have the same SSCP address assignment. This allows you to add more devices to the engineering access system and to grant access to other selected engineers without needing to reconfigure any engineer cards.

The configuration of these details—assignment of the SSCP addresses, generation of keys, and configuring cards and devices with the correct SSCP key and address information—is the job of ACSELERATOR QuickSet.

Installing ACSELERATOR QuickSet

Install SEL ACSELERATOR QuickSet from the Serial Security Products CD or through the use of SEL Compass software. You can also use SEL Compass to update your existing ACSELERATOR QuickSet installation to add support for the SEL-3045 and SEL-3025.

You can use ACSELERATOR QuickSet to configure many SEL products, including the SEL-3045 encryption card and the SEL-3025 Serial Shield. To install ACSELERATOR QuickSet, insert the CD and/or start **setup.bat**. On the installation webpage, click **ACSELERATOR QuickSet SEL-5030 Software**, which starts the ACSELERATOR QuickSet installer (*Figure 5.2*). You must have 211 MB of disk space available for ACSELERATOR QuickSet, SEL Compass, and the necessary support files.



☑ Install AcSELerator QuickSet
☑ Install SEL Compass

Figure 5.2 Starting ACSELERATOR QuickSet Installer

How to Use ACSELERATOR QuickSet to Configure a New SEL-3045 Secure SCADA Card

To run ACSELERATOR QuickSet, click the **Start** button, navigate to the **SEL Applications** group, and click on **ACSELERATOR QuickSet**.

Creating a New SEL-3045 User

ACSELERATOR QuickSet uses the User Manager to manage users and their credentials and the Device Manager to manage devices. For any user you have not already added, you will need to first use the User Manager to add that user for the card and then create a new SSCP credential for that user:

Step 1. In the main ACSELERATOR QuickSet window, use the menu bar to choose **Tools > Device Manager > User Manager**.

Step 2. If the engineering user does not already exist, click the **Create User** button to open the **Create User** dialog box. On the **User** tab, enter the **User Name**, **Full name**, and, optionally, a **Description** for the user. The **Password** entry is optional; it is unnecessary for using SSCP with the SEL-3025.

Step 3. Open the **Credentials** tab, and click **New** to open the **SSCP Credential** dialog box.

Step 4. Assign a **Group Name** to uniquely identify the user of the card. This name is normally the same as the **User Name** for the card holder.

TIP: You would usually use ACSELERATOR QuickSet to program a new card. You can restore a card to new condition by resetting it in the SEL-3055 Card Dock. To do this, plug the card into the dock, then insert the end of a paperclip or some similar instrument into the small **RESET** hole in the top of the reader and press gently until you feel a click. Hold the reset depressed for a couple of seconds and release it. If the card has reset successfully, the green LED on the reader will blink slowly.

Step 5. Click the **Auto Generate Keys** button to generate cryptographically random values for the card's SSCP keys.

Step 6. Click **OK** twice to return to the User Manager and then close the User Manager by clicking the inner (gray) **X** button in the top right corner of the User Manager window.

Setting up a New SEL-3045 for a User

TIP: If you will be administering multiple cards, you can use **Add > Location** from within Connection Explorer in the Device Manager window to create a folder to contain cards. You can then create cards by right-clicking on the folder and using **Add > Device**.

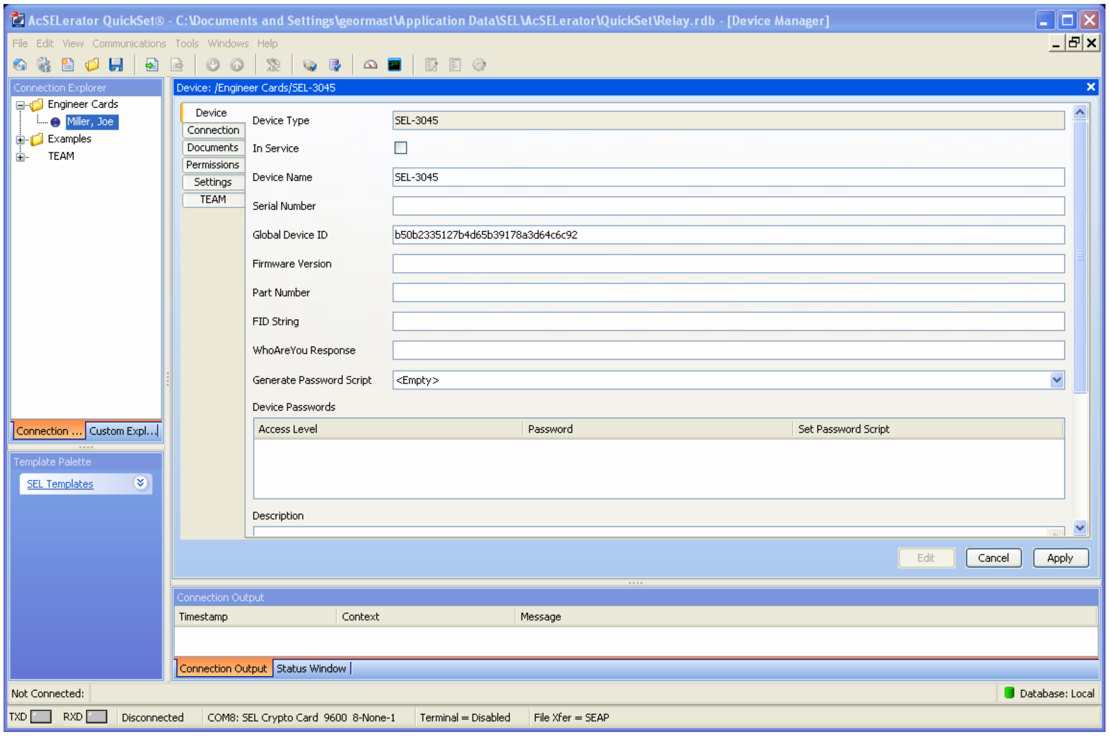
Use the Device Manager to add a new SEL-3045 to the view and associate the user with this view.

Step 1. In the main ACSELERATOR QuickSet window, use the menu bar to choose **Tools > Device Manager > Device Manager** or click either on the Device Manager label or corresponding icon under Settings in the Getting Started with QuickSet area.

Step 2. Right-click in Connection Explorer from within Device Manager where you want to create the new card, choose **Add > Device**, then choose SEL-3045 from the **Select Device Type** listing.

Step 3. Right-click on the new SEL-3045 device name within Connection Explorer and then rename the device to show the name or username of the card holder (Miller, Joe, for example).

Step 4. Double-click on this new card from within Connection Explorer in Device Manager to open the configuration area for that card. *Figure 5.3* shows a typical view of the Device Manager configuration area that would display after you double-click on the SEL-3045 device renamed Miller, Joe.


AcSELerator QuickSet® - C:\Documents and Settings\geormast\Application Data\SEL\AcSELerator\QuickSet\Relay.rdb - [Device Manager]

Device: /Engineer Cards/SEL-3045

Device Type: SEL-3045

In Service: □

Device Name: SEL-3045

Serial Number:

Global Device ID: b50b2335127b4d65b39178a3d64c6c92

Firmware Version:

Part Number:

FID String:

WhoAreYou Response:

Generate Password Script: <Empty>

Device Passwords

Access Level	Password	Set Password Script

Description

Timestamp	Context	Message

Not Connected:

Database: Local

TXD RXD Disconnected COM8: SEL Crypto Card 9600 8-None-1 Terminal = Disabled File Xfer = SEAP

Figure 5.3 Device Manager Showing SEL-3045

Configuring Communications to Your SEL-3045

Step 1. Set up communications with the card.

a. Click the **Edit** button so that you can change card settings.

b. Click the **Connection** tab from within the configuration area for the renamed SEL-3045.

c. Click the down-arrow that appears to the right of the **Device** drop-down list box, and choose the selection that ends with **SEL-3045 Secure SCADA Card**.

Creating Settings for Your SEL-3045

Step 2. Set the global settings for the card.

a. Click the **Settings** tab.

b. Click the **Global** node in the left pane of the configuration area.

c. The **Administrator Password** field will be colored red because its value is invalid. Enter a new password for administration of this card. This password must have at least eight characters, and it should contain both upper and lowercase letters, numbers, and special characters, such as punctuation.

TIP: The card's Administrator password would be necessary to read settings from the card through use of ACSELERATOR QuickSet or for updating settings. For most applications, where you reset cards before provisioning, and you provision cards just once, this password will be unnecessary. If this is the case, you can use a random value that you do not need to record.

d. Choose the **SSCPNETARCH Network Role** for the card. For engineering access, use **Master**.

e. Use the drop-down listing to the right of the **SSCPENBUFF Enable Data Buffering** text box to enable or disable data buffering.

f. Set the SSCP device address for this card. The address value should be unique in your system, so that log events relating to this SSCP address relate to a single identifiable card.

g. Click **Apply**.

Step 3. Set up SSCP credentials for access to remote SEL-3025s.

a. Click the **Permissions** tab.

b. Click **Add** to display a listing of users. Select from this listing the user you want, and click **OK**. This will add the user's name to a listing under the **Users and Group** heading in the **Permissions** tab.

c. Choose the correct card user for the card by selecting the user's name in the list and clicking **OK**.

d. Select the user's name from under the **Users and Groups** heading to add an Owner permission to the **Permissions** window.

e. Within the **Permissions** window, select the permission you just added and check the **Allow** check box at the end of that entry. This will create an SSCP group on the card that contains the user's SSCP credentials.

f. Click **Apply** to save all of these settings to the database.

Setting Up Your SEL-3045s for Engineering Access

Step 4. Set the remote SSCP address you will use for engineering access to your remote SEL-3025s

To do this, you must define at least one remote SEL-3025.

TIP: The first remote SEL-3025 need not be an actual device—it can be a template that you use for provisioning cards and which you can use to copy, rename, and edit to create actual remote SEL-3025s in your deployment.

To create an SEL-3025 for engineering access, perform the following steps:

a. In the main ACSELERATOR QuickSet window, choose **Tools > Device Manager > Device Manage**r from the menu bar.

b. Right-click in the **Connection Explorer** (left pane) window, choose **Add > Device**, then choose the SEL-3025 from the **Select Device Type** listing.

c. Right-click the new SEL-3025 in Connection Explorer and rename it. If this will be a template device, you might name it **3025 Template**.

d. Double-click on the new device to open a configuration area for the new 3025 Template device.

e. Click the **Settings** tab, click the **Edit** button, and then select **SSCP General Settings**. Set the **SSCPDEVADDR Device Address** to the value your engineering access SEL-3025s are using.

f. Click **Apply**.

Once you have set up an SEL-3025 for engineering access, perform the following steps:

g. Click the **Permissions** tab, click the **Add** button, select the new SEL-3045, and click **OK**. This will add the new user to the **Users and Groups** list.

h. Select the user in the list. This will cause the Pass Through permission for that user to display in the **Permissions** window. Check the **Allow** check box on that entry.

i. Click **Apply**.

This completes the setup of the SSCP groups for the card. The next steps will write the completed card configuration to the card.

Programming Your SEL-3045

Step 5. Send the settings data

a. In the Connection Explorer, right-click on the new **SEL-3045**.

b. From the menu, select **Device Tasks**, then **Send**.

c. You will be prompted for the administrator account password for the card. For a card that has been reset, enter **Administrator** for the password.

d. The data transfer will take a little longer than 10 seconds. When it completes, the status bar at the bottom of the Device Manager window will show the connection state as **Disconnected** (see *Figure 5.4*).

e. Remove the finished card from the card dock.

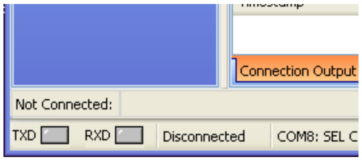


Figure 5.4 Status Bar When Programming Is Completed

How to Use ACSELERATOR QuickSet to Grant Engineering Access Through the SEL-3025

ACSELERATOR QuickSet easily grants users access to remote SEL-3025 devices in much the same way that it grants users pass through access to the SEL-3045.

Step 1. Set up communications with the SEL-3025

a. Use the menu bar to choose **Tools > Device Manager > Device Manager**.

b. Locate the target SEL-3025 device in the Connection Explorer.

c. Double-click the target SEL-3025 device to open the device configuration area.

d. Click the **Edit** button so that you can change settings.

e. Click the **Permissions** tab. The **Users and Groups** window shows a list of users for whom you could provide permission to that device. Initially, the window shows no users. Click the **Add** button to add a user to the device. This opens the **Select Users and Groups** window.

f. Choose the correct card user(s) from the list by selecting names in the list and clicking **OK**.

g. For the user(s) you added, select the user(s) in the **Users and Groups** window and then check the **Allow** check box at the end of the corresponding entry in the **Permissions** window.

h. Click **Apply** to save all of these settings to the database.

Step 2. Send the settings data

a. In the Connection Explorer, right-click on the target SEL-3025.

b. From the menu, select **Device Tasks**, then **Send**.

c. The software will prompt you for the administrator username and password for the device.

d. The data transfer will take a little longer than 10 seconds. When it completes, the status bar at the bottom of the Device Manager window will show the connection state as **Disconnected** (see *Figure 5.4*).

e. Close ACSELERATOR QuickSet.

This page intentionally left blank

Section 6
Job Done Examples

Introduction

This section contains Job Done® examples for the following applications:

- Example 1: *SEL-3025 Applied to Protect Engineering Access*
- Example 2: *SEL-3025 Applied in a Multidrop Network*
- Example 3: *SEL-3025 Applied in a Many-to-Many Network*
- Example 4: *SEL-3025 Applied To a Conitel 2100H Communications Link*

Job Done Example 1

SEL-3025 Applied to Protect Engineering Access

In this example, an engineering workstation is communicating via a point-to-point serial connection to a unit at a remote location. You must ensure that the data sent between the workstation and remote unit are secure. Data could be protected either by using two SEL-3025s or one SEL-3025 and the 915900225 PC Serial Security Kit. The PC Serial Security Kit applies cryptography to a serial port (or internal modem) on a PC, allowing it to communicate securely with a remote device through an SEL-3025 Serial Shield®. This example uses one SEL-3025 device to secure data sent between a remote device and a workstation equipped with the PC Serial Security Kit.

Identifying the Problem

Your objective is to secure the data between the engineering workstation and the remotely located unit. You decide for the following reasons that the SEL-3025 is the most cost-effective method for solving this problem:

- The SEL-3025 solution requires no modifications to your installed equipment, protocol, or software except for the addition of the SEL-3025 units and use of the 915900225 PC Serial Security Kit on the engineering workstation.
- The SEL-3025 setup is fast and easy.
- Identity-based access control prevents unauthorized use.

Defining the Solution

Figure 6.1 is a representation of the system this Job Done Example uses. For this example, we will assume that the communications infrastructure is already in place.

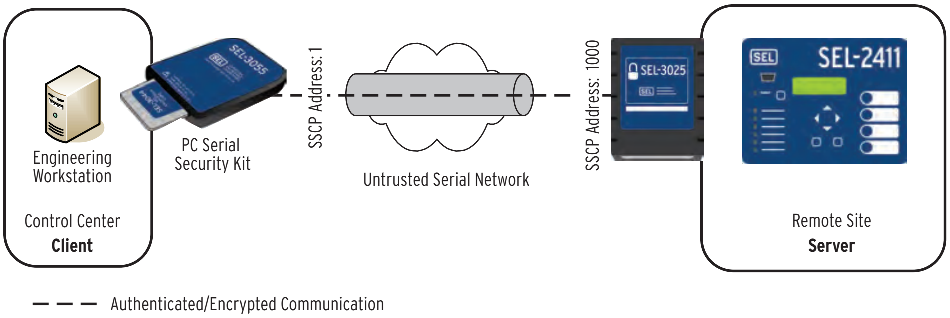


Figure 6.1 Point-to-Point Configuration

Table 6.1 defines the settings we will be applying to the Serial Shield devices in this example.

Table 6.1 SEL-3025 Address Settings

Setting	Engineering Access Remote Client	Server Serial Shield Device
IP Address	N/A	192.168.1.20/24
SSCP Device Address	1	1000
Network Architecture	Point-to-Point Client	Point-to-Point Server
Protocol	Unstructured Point-to-Point	Unstructured Point-to-Point

Setting Up the Engineering Access Client

The PC Serial Security Kit provides the hardware and software necessary for using your PC workstation to secure engineering access communications with remote SEL-3025 units. You will need to plug the SEL-3055 Card Dock into an available USB port on your computer and install the SEL-5025 Secure Port Service Software from the product CD.

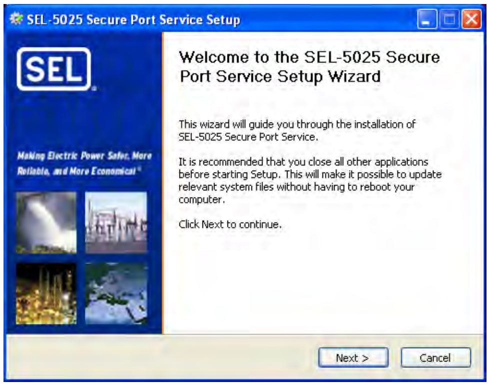
This example assumes that your SEL-3045 Secure SCADA Card is already configured, so you do not need to install configuration software. Otherwise, you would need to contact your system administrator or install ACSELERATOR QuickSet to provision your card. For detailed information about installing and using ACSELERATOR QuickSet, see *Section 4: Using the PC Serial Security Kit to Protect Engineering Access Communication*.

Install the SEL-5025 Secure Port Service Software

Step 1. Insert the CD into the drive.

Step 2. If Windows autorun is enabled, the installer will launch automatically. Otherwise, run **setup.bat** from the CD. On the installation webpage, click **Install SEL-5025 Secure Port Serial Service**.

Step 3. The SEL-5025 Secure Port Service Setup Wizard (*Figure 6.2*) will guide you through the installation process. You must have 7.5 MB of available disk space for the SEL-5025 Secure Port Service.


SEL-5025 Secure Port Service Setup
SEL
Making Electric Power Safer, More Reliable, and More Economical®
Next >
Cancel

Welcome to the SEL-5025 Secure Port Service Setup Wizard

This wizard will guide you through the installation of SEL-5025 Secure Port Service.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

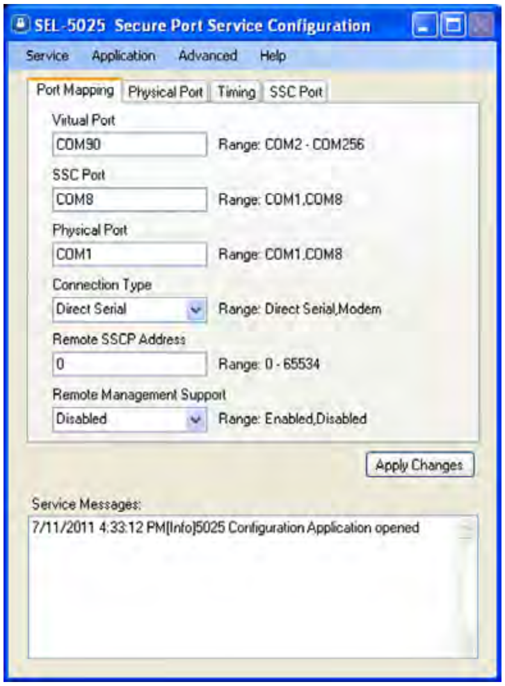
Figure 6.2 SEL-5025 Secure Port Service Setup Wizard

Install the SEL-3055 Card Dock

Step 1. Plug the SEL-3055 Card Dock into an available USB port on your computer.

Step 2. Plug the SEL-3045 Secure SCADA Card into the card dock.

Step 3. Wait for the green light on the card dock to illuminate.



Virtual Port: COM90 Range: COM2 - COM256

SSC Port: COM8 Range: COM1,COM8

Physical Port: COM1 Range: COM1,COM8

Connection Type: Direct Serial Range: Direct Serial,Modem

Remote SSCP Address: 0 Range: 0 - 65534

Remote Management Support: Disabled Range: Enabled,Disabled

Service Messages:

7/11/2011 4:33:12 PM[Info]5025 Configuration Application opened

Figure 6.3 SEL-5025 Secure Port Service Tray Application

Configuring the SEL-5025 Secure Port Service

Step 1. Double-click the **Secure Port Service** tray application icon in the tray area to open the configuration application. *Figure 6.3* shows the tray application window.

Step 2. On the **Port Mapping** tab, if you will be using a modem, set the connection type to **Modem**.

Step 3. On the **Port Mapping** tab, set the SSCP address to the address used by your engineering access SEL-3025 serial shields. If you have enabled remote management on your remote SEL-3025 serial shields, set **Remote Management Support** to **Enabled**.

TIP: The Remote Management Support setting on the Port Mapping tab must match the setting for the remote device. To simplify the setup for engineering access, this setting should match for all SEL-3025 devices in your deployment that you will use for engineering access.

Step 4. Click the **Physical Port** tab to configure the serial port to match the parameters expected by your modem or communications link.

Step 5. Close the configuration window.

Configure the Remote SEL-3025 Serial Shield

Once you have installed and configured the SEL-5025 Secure Port Service, if your system administrator configured your SEL-3045 card and the remote SEL-3025, your job is done. Otherwise, you will need to add an SSCP group to your SEL-3025 to enable secure communication.

Step 1. Log in to the Server Serial Shield by using the HTTPS web interface **https://<IP_Address>**, where <IP_Address> is the IP address configured for the device. Refer to *Section 2: Installation* for more information on device commissioning.

Step 2. On the **SSCP Settings > SSCP General** page, change the device address to match the remote SSCP address shown on the **Port Mapping** tab of the Secure Port Service configuration application (1000 in this example).

Step 3. On the **Serial Comms > System Communication** page, set the network architecture to **Point-to-Point Server** and the Trusted Interface (DCE) Protocol to **Unstructured Point-to-Point**.

Step 4. On the **SSCP Settings > SSCP Group** page, add a new SSCP group with the following settings.

a. Group Name: Your username

b. Remote SSCP Address: The SSCP address used by your SEL-3045 card (1 in this example)

c. Authentication Mode: **HMAC (SHA-256)**

d. Authentication Key: <<INSERT THE AUTHENTICATION KEY USED BY YOUR SEL-3045 CARD>>

e. Encryption Mode: **AES-256**

f. Encryption Key: <<INSERT THE ENCRYPTION KEY USED BY YOUR SEL-3045 CARD>>

g. HMAC Size: **10**

h. Max Sequence: **65535**

i. Key Exchange Interval: **30**

j. Encrypt Data: **Enabled** (checkmark ticked)

Verifying Cryptographic Settings

Step 1. Ensure that both **Enable Secure Protocol** and **Enable Remote Management** are checked on the **System Communications** page.

Step 2. Ensure that **Encrypt Data** is checked on both the **SSCP General** page and the **SSCP Groups** page for the server’s group.

Job Done Example 2

SEL-3025 Applied in a Multidrop Network

In this example, a master unit is using DNP3 to communicate to units at remote substations. You must ensure that the data sent between the master and remote units are secured. This example uses the SEL-3025 devices to secure data sent between a SCADA Master and remote devices.

Identifying the Problem

Your objective is to secure the data between the control center DNP3 SCADA Master and the remote substation units. You decide for the following reasons that the SEL-3025 is the most cost-effective method for solving this problem:

- The SEL-3025 solution requires no modifications to your installed equipment, protocol, or polling rate except for the additions of the SEL-3025 units.
- The SEL-3025 setup is fast.
- Management and logging are available from a central location.

Defining the Solution

NOTE: When using radios to communicate, you may need to set the Control Signal Mode of the Untrusted (DTE) Port to Push To Talk.

Figure 6.4 is a representation of the system this Job Done Example uses. For this example, we will assume that the DNP3 network and polling scheme are already in place.

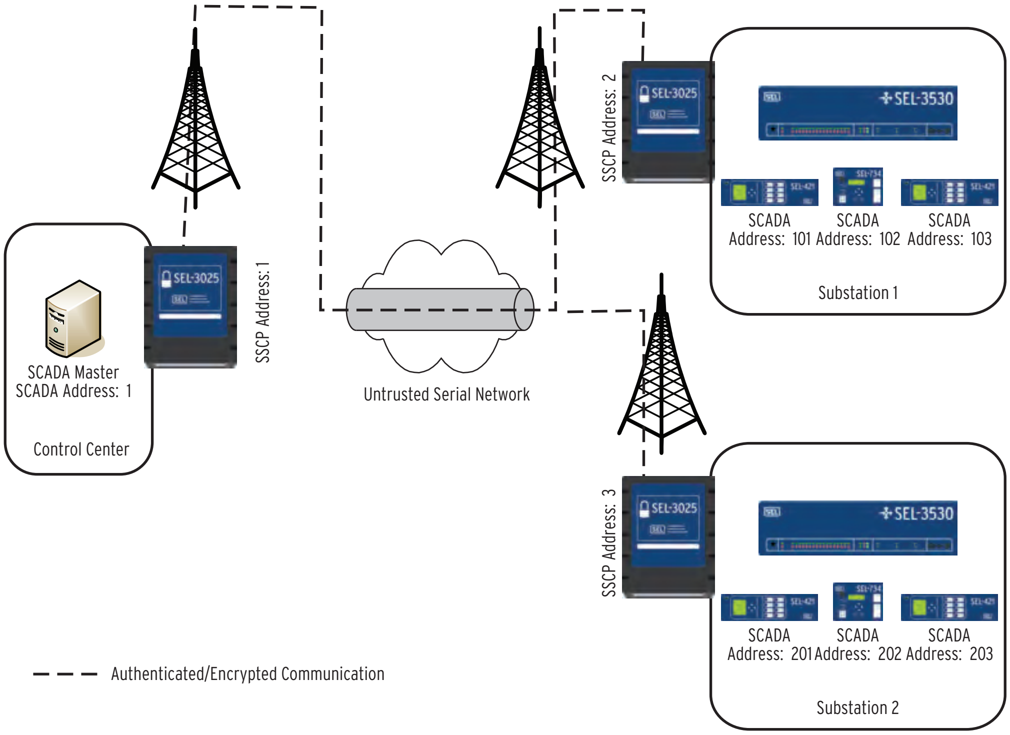


Figure 6.4 Multidrop Network

Table 6.2 defines the settings we will be applying to the Serial Shield devices in this example.

Table 6.2 SEL-3025 Address Settings

Setting	Master Serial Shield Device	Substation1 Serial Shield Device	Substation2 Serial Shield Device
SSCP Address	1	2	3
IP Address	192.168.1.10/24	192.168.1.20/24	192.168.1.30/24

Master Serial Shield Configuration

Step 1. Log in to the Master Serial Shield by using the HTTPS web interface https://<IP_Address>, where <IP_Address> is the IP address configured for the device during commissioning. Refer to *Section 2: Installation* for more information on device commissioning.

Step 2. Change the Device Address to **1** under **SSCP Settings** > **SSCP General**.

Step 3. Set the network architecture to **Point-to-Multipoint Client** under **Serial Comms** > **System Communication**.

Step 4. Create a new SSCP Group with the following settings:

a. Group Name: **Multidrop to Substations 1 and 2**

b. Remote SSCP Address: **2,3**

c. Authentication Mode: **HMAC (SHA-256)**

d. Authentication Key: <<INSERT>>

e. Encryption Mode: **AES-256**

f. Encryption Key: <<INSERT>>

g. HMAC Size: **10**

h. Max Sequence: **65535**

i. Key Exchange Interval: **30**

j. Encrypt Data: **Enabled** (checkmark ticked)

Step 5. Under **Serial Comms** > **Remote Address Mappings**, select **Update** for Remote SSCP Device Address **2**. Enter **101–103** for the Protected SCADA Addresses of the IEDs behind the remote SEL-3025 at Substation 1.

Step 6. Under **Serial Comms** > **Remote Address Mappings**, select **Update** for Remote SSCP Device Address **3**. Enter **201–203** for the Protected SCADA Addresses of the IEDs behind the remote SEL-3025 at Substation 2.

Remote Serial Shield Configuration for Substation 1

Step 1. Log in to the Substation1 Serial Shield by using the HTTPS web interface https://<IP_Address>, where <IP_Address> is the IP address configured for the device during commissioning. Refer to *Section 2: Installation* for more information on device commissioning.

Step 2. Change the Device Address to **2** under **SSCP Settings** > **SSCP General**.

Step 3. Set the network architecture to **Point-to-Multipoint Server** under **Serial Comms** > **System Communication**.

Step 4. Create a new SSCP Group with the following settings:

a. Group Name: **Multidrop to Control Center**

b. Remote SSCP Address: **1**

c. Authentication Mode: **HMAC (SHA-256)**

d. Authentication Key: <<INSERT>>

e. Encryption Mode: **AES-256**

f. Encryption Key: <<INSERT>>

g. HMAC Size: **10**

h. Max Sequence: **65535**

i. Key Exchange Interval: **30**

j. Encrypt Data: **Enabled** (checkmark ticked)

Step 5. Under **Serial Comms** > **Remote Address Mappings**, select **Update** for Remote SSCP Device Address **1**. Enter **1** for the Protected SCADA Addresses of the SCADA Master behind the remote SEL-3025 at the Control Center.

Remote Serial Shield Configuration for Substation 2

Step 1. Log in to the Substation2 Serial Shield by using the HTTPS web interface https://<IP_Address>, where <IP_Address> is the IP address configured for the device during commissioning. Refer to *Section 2: Installation* for more information on device commissioning

Step 2. Change the Device Address to **3** under **SSCP Settings** > **SSCP General**.

Step 3. Set the network architecture to **Point-to-Multipoint Server** under **Serial Comms** > **System Communication**.

Step 4. Create a new SSCP Group with the following settings:

a. Group Name: **Multidrop to Control Center**

b. Remote SSCP Address: **1**

c. Authentication Mode: **HMAC (SHA-256)**

d. Authentication Key: <<INSERT>>

e. Encryption Mode: **AES-256**

f. Encryption Key: <<INSERT>>

g. HMAC Size: **10**

h. Max Sequence: **65535**

i. Key Exchange Interval: **30**

j. Encrypt Data: **Enabled** (checkmark ticked)

Step 5. Under **Serial Comms** > **Remote Address Mappings**, select **Update** for Remote SSCP Device Address **1**. Enter **1** for the Protected SCADA Addresses of the SCADA Master behind the remote SEL-3025 at the Control Center.

Job Done Example 3

SEL-3025 Applied in a Many-to-Many Network

Use many-to-many network structures when there are many users with authorized access to many different endpoints. In this example, two engineering laptops need access to multiple devices.

Identifying the Problem

Your objective is to secure the data between each laptop and each of the remote devices. You decide for the following reasons that the SEL-3025 is the most cost-effective method for solving this problem:

- The SEL-3025 solution requires no modifications to your installed equipment or protocol, except for the additions of the SEL-3025 units.
- The SEL-3025 setup is fast.
- Management and logging are available from a central location.
- Identity-based access control prevents unauthorized use.

Defining the Solution

NOTE: The serial port of Remote Device 1 and 2 connecting to the respective SEL-3025 needs to be set to SEL ASCII for engineering access to work properly.

Figure 6.5 is a representation of the system this Job Done Example uses.

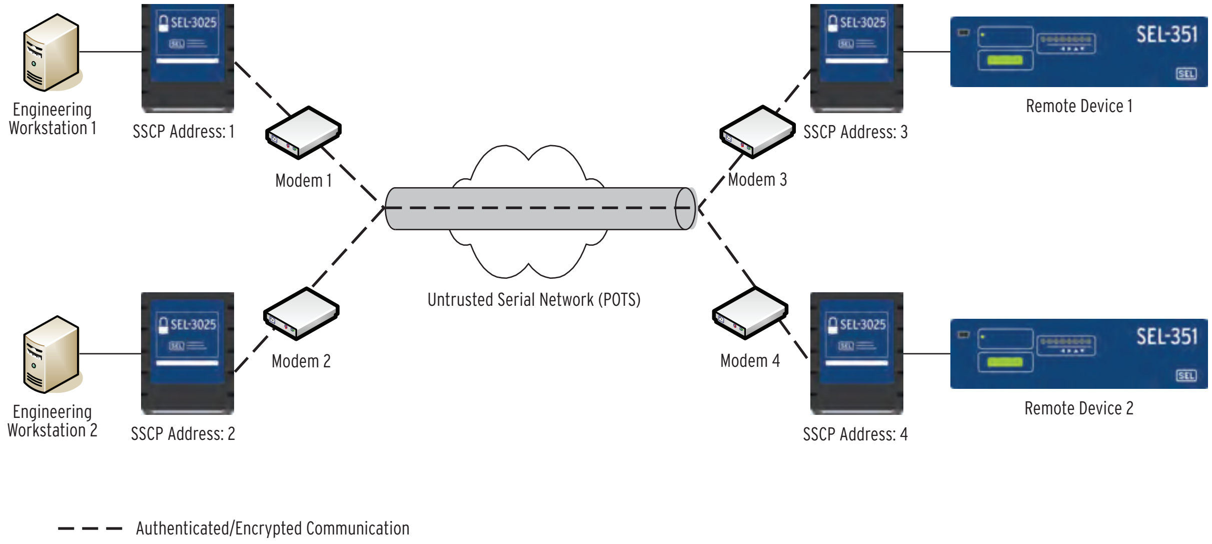


Figure 6.5 Many-to-Many Network

Table 6.3 defines the settings we will be applying to the Serial Shield devices in this example.

Table 6.3 SEL-3025 Address Settings

Setting	Engineering Workstation 1 Serial Shield Device	Engineering Workstation 2 Serial Shield Device	Remote Device 1 Serial Shield Device	Remote Device 2 Serial Shield Device
SSCP Address	1	2	3	4
IP Address	192.168.1.10/24	192.168.1.20/24	192.168.1.30/24	192.168.1.40/24

Serial Shield Configuration for Laptop 1

Step 1. Log in to the Engineering Workstation 1 Serial Shield by using the HTTPS web interface https://<IP_Address>, where <IP_Address> is the IP address configured for the device during commissioning. Refer to *Section 2: Installation* for more information on device commissioning.

Step 2. Change the Device Address to **1** under **SSCP Settings** > **SSCP General**.

Step 3. Set the network architecture to **Point-to-Point Client** under **Serial Comms** > **System Communication**.

Step 4. Set the Trusted Interface (DCE) Protocol to **Unstructured Point-To-Point** under **Serial Comms** > **System Communication**.

Step 5. Under **Serial Comms** > **AT Modem**, check **Enable AT Passthrough** and click **Save Settings**. Enable the **Multiple Remote Modems** setting and click **Save Settings**.

Step 6. Create a new SSCP Group with the following settings:

a. Group Name: **Engineering Access**

b. Remote SSCP Address: **3-4**

c. Authentication Mode: **HMAC (SHA-256)**

d. Authentication Key: <<INSERT>>

e. Encryption Mode: **AES-256**

f. Encryption Key: <<INSERT>>

g. HMAC Size: **10**

h. Max Sequence: **65535**

i. Key Exchange Interval: **30**

j. Encrypt Data: **Enabled** (checkmark ticked)

NOTE: The Connect String contains the phone number for Modem 3 in Figure 6.5. Replace the phone number to match your implementation.

Step 7. Under **Serial Comms** > **Remote Address Mappings**, select **Update** for Remote SSCP Device Address **3**. Enter **ATDT5095551003** for the Connect String.

NOTE: The Connect String contains the phone number for Modem 4 in Figure 6.5. Replace the phone number to match your implementation.

Step 8. Under **Serial Comms** > **Remote Address Mappings**, select **Update** for Remote SSCP Device Address **4**. Enter **ATDT5095551004** for the Connect String.

Serial Shield Configuration for Laptop 2

Step 1. Log in to the Laptop 2 Serial Shield by using the HTTPS web interface https://<IP_Address>, where <IP_Address> is the IP address configured for the device during commissioning. Refer to *Section 2: Installation* for more information on device commissioning.

Step 2. Change the Device Address to **2** under **SSCP Settings** > **SSCP General**.

Step 3. Set the network architecture to **Point-to-Point Client** under **Serial Comms** > **System Communication**.

Step 4. Set the trusted interface (DCE) protocol to **Unstructured Point-To-Point** under **Serial Comms** > **System Communication**.

Step 5. Under **Serial Comms** > **AT Modem**, check **Enable AT Passthrough** and click **Save Settings**. Enable the Multiple **Remote Modems** setting and click **Save Settings**.

Step 6. Create a new SSCP Group with the following settings:

a. Group Name: **Engineering Access**

b. Remote SSCP Address: **3-4**

c. Authentication Mode: **HMAC (SHA-256)**

d. Authentication Key: <<INSERT>>

e. Encryption Mode: **AES-256**

f. Encryption Key: <<INSERT>>

g. HMAC Size: **10**

h. Max Sequence: **65535**

i. Key Exchange Interval: **30**

j. Encrypt Data: **Enabled** (checkmark ticked)

NOTE: The Connect String contains the phone number for Modem 3 in Figure 6.5. Replace the phone number to match your implementation.

Step 7. Under **Serial Comms** > **Remote Address Mappings**, select Remote SSCP Device Address **3** from the drop-down list and select **View Settings**. Enter **ATDT5095551003** for the Connect String.

NOTE: The Connect String contains the phone number for Modem 4 in Figure 6.5. Replace the phone number to match your implementation.

Step 8. Under **Serial Comms** > **Remote Address Mappings**, select Remote SSCP Device Address **4** from the drop-down list and select **View Settings**. Enter **ATDT5095551004** for the Connect String.

Serial Shield Configuration for Remote Device 1

Step 1. Log in to the Remote Device 1 Serial Shield by using the HTTPS web interface https://<IP_Address>, where <IP_Address> is the IP address configured for the device during commissioning. Refer to *Section 2: Installation* for more information on device commissioning.

Step 2. Change the Device Address to **3** under **SSCP Settings** > **SSCP General**.

Step 3. Set the network architecture to **Point-to-Point Server** under **Serial Comms** > **System Communication**.

Step 4. Create a new SSCP Group with the following settings:

a. Group Name: **Engineering Access** (Workstation 1)

b. Remote SSCP Address: **1**

c. Authentication Mode: **HMAC (SHA-256)**

  d. Authentication Key: <<INSERT>>
  e. Encryption Mode: **AES-256**
  f. Encryption Key: <<INSERT>>
  g. HMAC Size: **10**
  h. Max Sequence: **65535**
  i. Key Exchange Interval: **30**
  j. Encrypt Data: **Enabled** (checkmark ticked)

Step 5. Create a new SSCP Group with the following settings:

  a. Group Name: **Engineering Access** (Workstation 2)
  b. Remote SSCP Address: **2**
  c. Authentication Mode: **HMAC (SHA-256)**
  d. Authentication Key: <<INSERT>>
  e. Encryption Mode: **AES-256**
  f. Encryption Key: <<INSERT>>
  g. HMAC Size: **10**
  h. Max Sequence: **65535**
  i. Key Exchange Interval: **30**
  j. Encrypt Data: **Enabled** (checkmark ticked)

Serial Shield Configuration for Remote Device 2

Step 1. Log in to the Remote Device 2 Serial Shield by using the HTTPS web interface https://<IP_Address>, where <IP_Address> is the IP address configured for the device during commissioning. Refer to *Section 2: Installation* for more information on device commissioning.

Step 2. Change the Device Address to **4** under **SSCP Settings > SSCP General**.

Step 3. Set the network architecture to **Point-to-Point Server** under **Serial Comms** > **System Communication**.

Step 4. Create a new SSCP Group with the following settings:

  a. Group Name: **Engineering Access** (Workstation 1)
  b. Remote SSCP Address: **1**
  c. Authentication Mode: **HMAC (SHA-256)**
  d. Authentication Key: <<INSERT>>
  e. Encryption Mode: **AES-256**
  f. Encryption Key: <<INSERT>>
  g. HMAC Size:**10**
  h. Max Sequence: **65535**
  i. Key Exchange Interval: **30**
  j. Encrypt Data: **Enabled** (checkmark ticked)

Step 5. Create a new SSCP Group with the following settings:

  a. Group Name: **Engineering Access** (Workstation 2)
  b. Remote SSCP Address: **2**
  c. Authentication Mode: **HMAC (SHA-256)**
  d. Authentication Key: <<INSERT>>

e. Encryption Mode: **AES-256**

f. Encryption Key: <<INSERT>>

g. HMAC Size: **10**

h. Max Sequence: **65535**

i. Key Exchange Interval: **30**

j. Encrypt Data: **Enabled** (checkmark ticked)

Job Done Example 4

SEL-3025 Applied To a Conitel 2100H Communications Link

In this application, a SCADA master and a remote slave are exchanging data via a leased-line modem link using the bit-based Conitel 2100H protocol. This example uses SEL-3025 Serial Shield devices with Streaming Encryption Protocol (SEP) to cryptographically secure the data while minimizing the latency the encryption introduces.

Identifying the Problem

Your objective is to secure the data between the two remote substation devices without affecting operation. You decide for the following reasons that the SEL-3025 with SEP is the most cost-effective method for solving this problem:

- The SEL-3025 solution requires no modifications to your installed equipment or protocols, except for the additions of the SEL-3025 units.
- The SEL-3025 setup is fast and simple.
- Streaming Encryption Protocol has the low latency necessary for real-time data.
- Management and logging are available from a central location.

Defining the Solution

Figure 6.6 is a representation of the system this Job Done Example uses. For this example, we assume that the SCADA Master, RTU, and modems are already in place. Your task is to add cryptographic protection to the link.

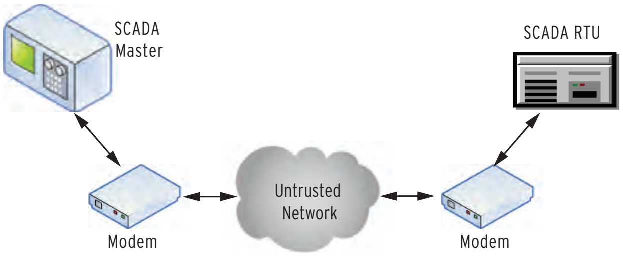


Figure 6.6 Real-Time SCADA Application

The SEL-3025 is a “bump-in-the-wire” encryption device; you insert one on each end of the communications link in line with the data you want to protect. Accordingly, you must insert an SEL-3025 between the SCADA equipment and the modem at each end of the setup. To do this, you must disconnect the cable between the modem and the equipment, and insert the SEL-3025, using additional cable(s). You would typically use a C609 cable. On each end, connect the modem to the DTE interface on the SEL-3025, and connect the DCE interface on the SEL-3025 devices to the SCADA equipment.

NOTE: For most installations, you can obtain information on the proper EIA-232 cable configuration from the SEL-5801 Cable Selector Program. Using the SEL-5801 software, you can choose a cable by application. The software provides the SEL cable number with wiring and construction information, so you can order the appropriate cable from SEL or construct one.

Figure 6.7 shows the system as modified by the addition of an SEL-3025 Serial Shield in the serial communications line to each modem.

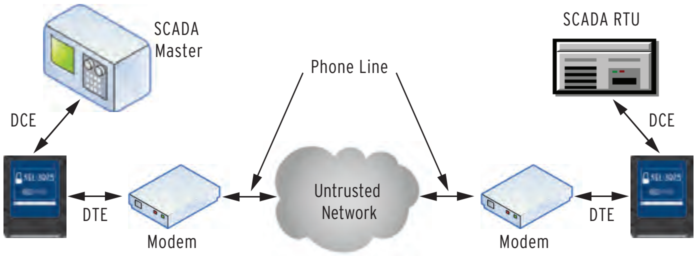


Figure 6.7 Real-Time Protection Application With SEL-3025 Encryption

It is convenient to set up the SEL-3025 on the bench before deploying it to the field. You must configure each unit individually with the correct settings to communicate with the unit on the other end of the communications link.

Connect an Ethernet cable to the ETH MGMT port of the unit you want to program. Reset the device, wait for the green LEDs to illuminate, and then use a web browser such as Internet Explorer or Firefox to navigate to https://192.168.1.2. This is a secure connection (https), but the certificate the device presents will be the default factory certificate, which will not match the URL. Because of this, the browser will present a warning dialog. You must manually continue opening the site to reach the initial **Device Commissioning** page. Your organization can issue a certificate for the device to eliminate the warning dialog. On the **Device Commissioning** page, you will need to set up the administrator account for the device, after which you will be able to continue with setup. Refer to *Section 2: Installation* for more information on device commissioning.

All that remains is to set up the communications parameters for the Serial Shield devices. *Table 6.4* shows the settings that we will apply to the Serial Shield devices in this example. Note that some device settings will change to appropriate values when you select Conitel 2100H as the trusted interface protocol, so you do not need to set them and they do not appear in the table.

Table 6.4 SEL-3025 Device Settings

Setting	SCADA Master	SCADA RTU (Slave)
IP Address	192.168.1.20/24	192.168.1.30/24
Network Architecture	Point-to-Point Client	Point-to-Point Server
Enable Secure Protocol	Yes	Yes
Enable Remote Management	Yes	Yes
Trusted Interface Protocol	Conitel 2100H	Conitel 2100H
Trusted (DCE) Port Baud Rate	Match modem speed (e.g., 9600 bps)	Match modem speed (e.g., 9600 bps)
Untrusted (DCE) Port Baud Rate	Match DCE speed	Match DCE speed
Data Buffering	No	No
SEP Device Address	1	2
SEP Group Name	JobDone4	JobDone4
Remote SEP Device Addresses	2	1
System Key	Any 64-hex-character key string (same for both units)	Any 64-hex-character key string (same for both units)

Remote Serial Shield Configuration for the Master Device

Step 1. Log in to the Master Serial Shield by using the HTTPS web interface and the IP address configured for the device. After reset, the URL is **https://192.168.1.2**. It can be set to its final value on the **Mgmt Network Interface** page. For this example, the device will be configured to be on **https://192.168.1.20**.

Step 2. Navigate to the **System Communication** page and set the **Network Architecture** to **Point-to-Multipoint Client**.

Step 3. Set the **Trusted Interface protocol** to **Conitel 2100H**.

Step 4. On both the **Trusted (DCE) Port** and **Untrusted (DTE) Port** pages, set the **Bits Per Second** to **9600** bps.

Step 5. On the **SEP General** page, set the **Device Address** to **1**.

Step 6. On the **SEP Group** page, create a new SEP Group with the following settings:

a. Group Name: **JobDone4**

b. Remote SEP Device Addresses: **2**

c. System Key: <<INSERT 64 KEY DIGIT KEY>>

Serial Shield Configuration for the Slave Device

Step 1. Log in to the Master Serial Shield by using the HTTPS web interface and the IP address configured for the device. After reset, the URL is **https://192.168.1.2**. It can be set to its final value on the **Mgmt Network Interface** page. For this example, the device will be configured to be on **https://192.168.1.30**.

Step 2. Navigate to the **System Communication** page and set the **Network Architecture** to **Point-to-Multipoint Server**.

Step 3. Set the **Trusted Interface protocol** to **Conitel 2100H**.

Step 4. On both the **Trusted (DCE) Port** and **Untrusted (DTE) Port** pages, set the **Bits Per Second** to **9600** bps.

Step 5. On the **SEP General** page, Set the **Device Address** to **2**.

Step 6. On the **SEP Group** page, create a new SEP Group with the following settings:

a. Group Name: **JobDone4**

b. Remote SEP Device Addresses: **1**

c. System Key: <<INSERT 64 HEX DIGIT KEY>>

Section 7
Settings and Commands

Introduction

This section explains the settings and commands of the SEL-3025 Serial Shield®.

- *Commissioning Page*
- *System*
  - *Date/Time*
  - *Usage Policy*
  - *File Management*
  - SELBOOT *Key*
  - *Web Server Certificate*
- *Users*
  - *Accounts*
  - *Account Settings*
- *Network*
  - *Management Network Interface*
  - *Syslog Settings*
- *Serial Communications*
  - *System Communication*
  - *AT Modem*
  - *Frame Synchronization*
  - *Trusted (DCE) Port*
  - *Untrusted (DTE) Port*
  - *Remote Address Mappings*
- *SSCP Settings*
  - *SSCP General*
  - *SSCP Group*
- *SEP Settings*
  - *SEP General*
  - *SEP Group*
  - *SEP Advanced*

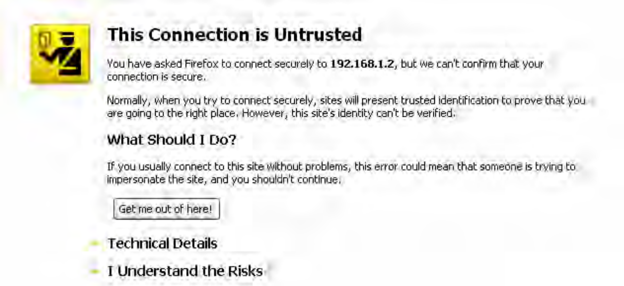
- *Remote Management*
  - *Remote Log In*
  - *Remote Ping*
  - *Secure Mode Initiation*
- *Reports*
  - *System Logs*
  - *Diagnostics*
  - *Serial Communications Status*
  - *Task List Report*
  - *Vector Reports*

Commissioning Page

The SEL-3025 commissioning page is available at the SEL-3025 default IP address: 192.168.1.2. You can only access the commissioning page when the SEL-3025 is unconfigured. The SEL-3025 is in an unconfigured state when received from the factory and after a factory-default reset. The SEL-3025 commissioning page is located at 192.168.1.2.

NOTE: You must enter the HTTPS prefix in the address bar to specify communication to Port 443. Without the HTTPS prefix, your web browser will default to communicating to Port 80 and the SEL-3025 will deny connection attempts.

The SEL-3025 authenticates itself to your web browser with a self-signed X.509 certificate. You must have this certificate to communicate over HTTPS. The self-signed certificate will probably cause your web browser to generate a security alert, similar to the one in *Figure 7.1*. This alert occurs because self-signed X.509 certificates are not considered secure, but use of such certificates is unavoidable during commissioning. If you get this security alert, you will need to add a security exception to your web browser. Your web browser will provide instructions for creating the security exception. You can eliminate this security alert by generating or installing a new certificate after commissioning.



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.1.2**, but we can't confirm that your connection is secure.

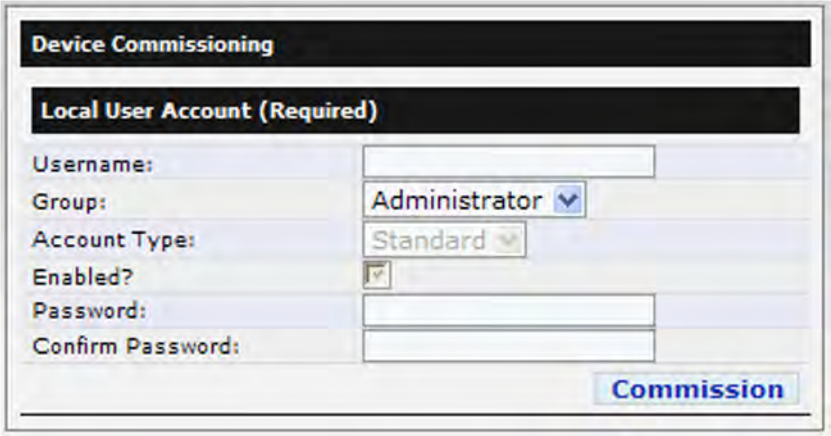
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Figure 7.1 Security Exception

Device commissioning requires you to create an account in the Administrator or User Manager group. An unconfigured SEL-3025 does not contain any accounts. This method ensures that only the user commissioning the SEL-3025 has the knowledge necessary to access it. The **Device Commissioning** page (*Figure 7.2*) provides username and password fields to create the initial administrative account. These are the only fields that require user input for commissioning.



Device Commissioning

Local User Account (Required)

Username:
Group: Administrator
Account Type: Standard
Enabled? ☑
Password:
Confirm Password:

Figure 7.2 Device Commissioning Page

Table 7.1 shows the configurable fields on the SEL-3025 **Device Commissioning** page, acceptable values for these fields, and brief descriptions of them. For more detailed information on each of the network configuration fields, see *Management Network Interface*.

Table 7.1 Commissioning Settings

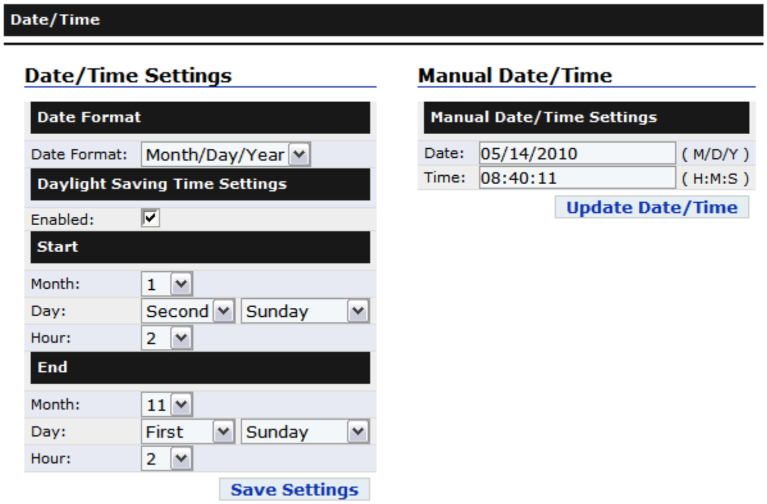
Field Name	Values	Description
Username	as many as 128 characters	The username for the initial account on this system. All usernames on this system must be unique. Usernames are not case sensitive.
Password	8 to 128 characters	Passwords must consist of at least eight characters and have characters from each of the following character sets: lowercase letters, uppercase letters, digits, and nonalphanumeric characters. Passwords must be entered twice to ensure correctness.

System

Date/Time

The date and time functions of the SEL-3025 allow for time stamping of system events. The SEL-3025 has an internal clock that must be set manually. The SEL-3025 contains a battery that will maintain the internal clock for 10 years in case of power loss.

To set the date and time, enter the date and time in their respective fields in the formats indicated, and then select the **Update Date/Time** button. If you want to use Daylight-Saving Time and have the SEL-3025 update the clock automatically, you must enable **Daylight Saving Time Settings** and configure the **Start** and **End** parameters. For example, in the year 2010, Daylight-Saving Time began in the United States at 2:00 a.m. on the second Sunday of March, and ended at 2:00 a.m. on the first Sunday of November. *Figure 7.3* depicts the date and time settings for the SEL-3025.



Date Format: Month/Day/Year

Enabled: ☑

Start — Month: 1; Day: Second Sunday; Hour: 2

End — Month: 11; Day: First Sunday; Hour: 2

Date: 05/14/2010 (M/D/Y)

Time: 08:40:11 (H:M:S)

Figure 7.3 Date and Time Settings

The device logs all configuration changes to the system date or time.

The SEL-3025 provides three options for the date format. These options are provided for compatibility with your existing system. To choose the date format, select the format you want from the **Date Format** drop-down box. The SEL-3025 defaults to a date format of month/day/year. After selecting the appropriate date format, click the **Save Settings** button.

Usage Policy

The SEL-3025 presents a usage policy to all users accessing the login page. This policy notifies users of what constitutes appropriate use of this machine, what actions are taken to ensure the device is not used inappropriately, and what actions will be taken if abuse is discovered. The SEL-3025 comes with the following default usage policy.

> *This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such activity to law enforcement officials.*

The usage policy is customizable and can include any message of as many as 1000 characters in length. Select the **Usage Policy** link from the navigation panel to modify the usage policy.

Only a user with administrator or user manager privileges can perform changes to the usage policy. The SEL-3025 logs all configuration changes to the usage policy.

File Management

Use the **File Management** page to upgrade firmware for the SEL-3025. Refer to *Appendix B: Firmware Upgrade Instructions*. The **File Management** page is also used to import or export SEL-3025 settings. Refer to *Appendix C: Importing or Exporting Settings*.

SELBOOT Key

SEL-3025 firmware uses cryptographic key signatures. SELBOOT Keys verify the integrity of the signed firmware. You need to upgrade the SELBOOT Keys only if any of the public-private key pairs have been compromised. The SELBOOT **Key** page allows a user to upload new SELBOOT public key files through the web interface over an Ethernet connection.

Web Server Certificate

You must authenticate HTTPS connections to confirm that the server you are communicating with is the correct server. This authentication is through X.509 certificates. By default, the SEL-3025 has a self-signed X.509 certificate that can cause your web browser to issue a security alert. This security alert will require you to create security exception before authentication can continue.

To prevent this security alert from appearing, install a certificate authority (CA)-signed X.509 certificate on your web browser and set as the web server certificate. To configure the web server certificate on your SEL-3025, paste the text of a base64 encoded X.509 SSL certificate into the **Certificate** text box on the Web Server Certificate page, and click **Import Certificate**. Because the SEL-3025 cannot create the certificate request, the certificate data you provide must also include the encoded private key information.

For more information on X.509 certificates, see *Appendix H: X.509*.

Users

Accounts

Use the **Accounts** page to add, remove, and update local user accounts of the SEL-3025. Refer to *Section 3: Managing Users* for more information regarding accounts of the SEL-3025.

Account Settings

Use the **Account Settings** page to define an account inactivity timeout, one-time account life, and the behavior of the alarm contact for user logins. *Table 7.2* lists the options for account settings.

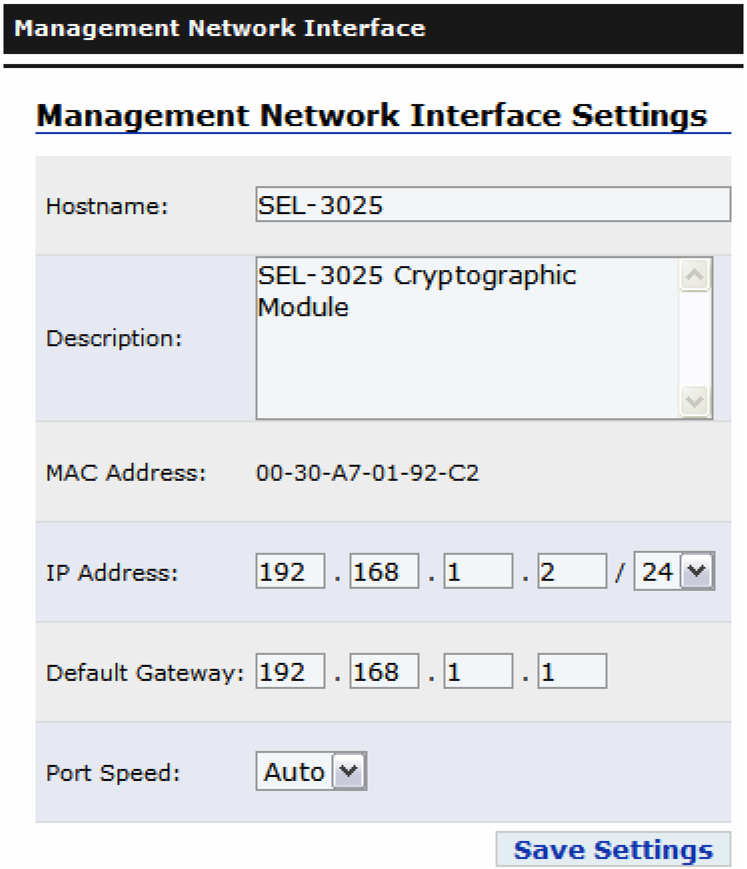
Table 7.2 Account Settings

Field Name	Values	Description
Account Inactivity Timeout	1–120 minutes	The amount of time a user’s session is inactive before the SEL-3025 terminates the session.
One-Time Account Life	1–72 hours	The amount of time a one-time account is valid. The account is removed from the SEL-3025 once this value has been reached.
Logon Alarm	Yes / No	Indicates whether the alarm should be pulsed for successful user login.

Network

Management Network Interface

The **Management Network Interface** page provides the configuration options for the network settings for the ETH MGMT port. Configure the IP address in CIDR notation. Refer to *Appendix G: Classless Inter-Domain Routing (CIDR)* for more information regarding CIDR notation.



Management Network Interface

Management Network Interface Settings

Hostname: SEL-3025

Description: SEL-3025 Cryptographic Module

MAC Address: 00-30-A7-01-92-C2

IP Address: 192 . 168 . 1 . 2 / 24

Default Gateway: 192 . 168 . 1 . 1

Port Speed: Auto

Figure 7.4 Management Network Interface

Table 7.3 Management Network Interface Settings (Sheet 1 of 2)

Field Name	Values	Description
Hostname	2 to 32 characters	The unique name that is to be used to identify this device on the webpages and in Syslog messages. The host name must begin with a letter and can contain letters, digits, and hyphens (-). This host name defaults to SEL-3025-<device serial number>.
Description	As many as 255 characters	A user-defined description of the usage or purpose of this SEL-3025 (optional).
MAC Address	Read-only value of MAC address of the ETH MGMT interface.	Read-only value of MAC address of the ETH MGMT interface.
IP Address	www.xxx.yyy.zzz/aa	A unique IP address used to communicate to this SEL-3025. Class D and Class E addresses are not allowed. This address defaults to 192.168.1.2/24.

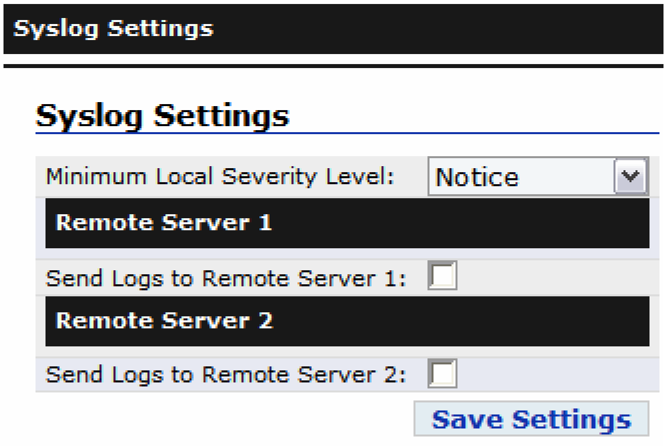
Table 7.3 Management Network Interface Settings (Sheet 2 of 2)

Field Name	Values	Description
Default Gateway	www.xxx.yyy.zzz	Defines the IP address of the default router that is used to transfer packets to another network. Class D and Class E addresses are not allowed. If this address is left blank and a packet is destined for another network, that packet will be dropped (optional).
Port Speed	Auto/10/100	Defines the port speed of the ETH MGMT network interface. This speed is used when connecting the SEL-3025 to another network device. The speed defaults to Auto, which is usually the most appropriate option.

Syslog Settings

Syslog is a specification that describes both the method and format in which logs are locally stored and routed to a collector. The SEL-3025 can send its log information to two destinations and will store at least 2,048 event logs locally in nonvolatile memory. Each destination, including the local memory, has a configurable severity level filter. The SEL-3025 logs all configuration changes to Syslog. For more information about Syslog, refer to *Appendix E: Syslog*.

The SEL-3025 logs many different types of events such as system startup, login attempts, and configuration changes. Selecting the **Syslog Settings** link from the navigation panel will display a screen similar to *Figure 7.5*. From the **Syslog Settings** page you can configure the minimum local severity level, as well as configure remote Syslog destinations. The **Minimum Local Severity Level** setting indicates the minimum severity that a Syslog message must have before the SEL-3025 can store that message locally or send it to a remote Syslog destination. You can set the minimum severity level at **Informational**, **Notice**, **Warning**, or **Error** for both local and remote Syslog destinations. Select the appropriate logging threshold for your needs. Setting the threshold too low can result in the generation of many logs that are not relevant to your business needs. Setting the threshold too high can result in the SEL-3025 not recording important messages. The logging threshold is set at **Notice** by default.


Syslog Settings

Syslog Settings

Minimum Local Severity Level: Notice

Remote Server 1

Send Logs to Remote Server 1: □

Remote Server 2

Send Logs to Remote Server 2: □

Figure 7.5 Syslog Settings

Below the **Minimum Local Severity Level** setting are settings for remote Syslog destinations. These destinations are the Syslog servers that will store and process the Syslog messages remotely. You can configure as many as two destinations. To configure a Syslog destination, enable remote logging for the destination you are configuring and enter the configuration parameters to match your environment. See *Table 7.4* for descriptions of the Syslog destination settings.

Table 7.4 Syslog Destination Settings

Setting	Values	Description
IP Address	www.xxx.yyy.zzz	The IP address of the Syslog destination.
Port	1–65535	The Syslog UDP port number is 514 by default. This port number must match the configuration of your Syslog server.
Minimum Severity Level	Informational, Notice, Warning, Error	The minimum severity level that a message must have to be forwarded to this destination.

Serial Communications

System Communication

The system communication settings define how the SEL-3025 will operate within the serial network. The **Network Architecture** setting defines what role the SEL-3025 will have when communicating with other SEL-3025 devices in the serial network. *Table 7.5* lists the options for system communication settings with a brief description of each.

Table 7.5 System Communication Settings (Sheet 1 of 2)

Setting	Values	Description
Network Architecture	Point-to-Point Client Point-to-Point Server Point-to-Multipoint Client Point-to-Multipoint Server	The network architecture role the SEL-3025 will fill. See *Figure 7.6* and *Figure 7.7*.
Enable Secure Protocol	Yes / No	Enable or disable the secure protocol. If set to No, the SEL-3025 will be in pass-through mode and all data are sent unencrypted and unauthenticated.
Enable SEL Remote Management	Yes / No	Enable or disable remote management features.

Table 7.5 System Communication Settings (Sheet 2 of 2)

Setting	Values	Description
Trusted Interface (DCE) Protocol	Protocols available with SSCP cryptographic card installed: DNP3 Modbus® RTU Unstructured Point-to-Point Custom Delay-Delimited Protocols available with SEP cryptographic card installed: DNP3 Modbus RTU Tejas Conitel 2100H Van Comm Redac 70H Unstructured Point-to-Point Custom Delay-Delimited Delay-Delimited Bit-based	The protocol that will be used by devices connected to the trusted interface (DCE).
Untrusted Interface (DTE) Protocol	SSCP or SEP	Display only. This setting is determined by the type of encryption card installed.

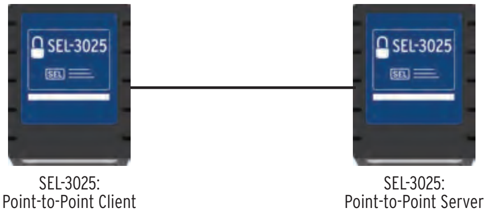


Figure 7.6 Point-to-Point Network Architecture

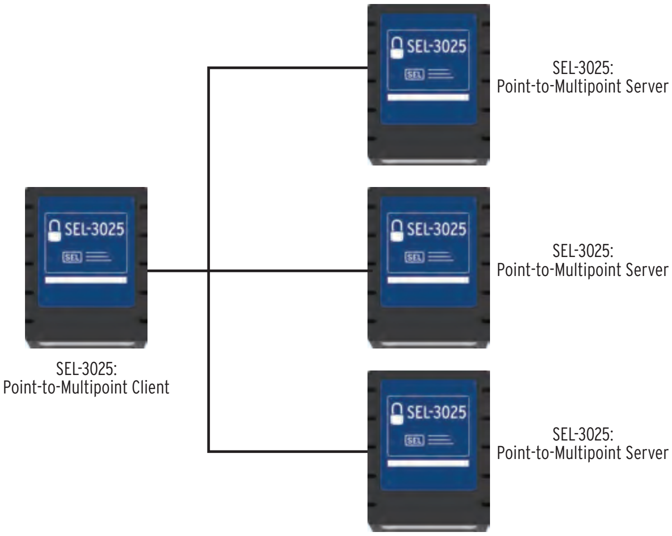

SEL-3025
SEL-3025:
Point-to-Multipoint Server
SEL-3025
SEL-3025:
Point-to-Multipoint Client
SEL-3025
SEL-3025:
Point-to-Multipoint Server
SEL-3025
SEL-3025:
Point-to-Multipoint Server

Figure 7.7 Point-to-Multipoint Network Architecture

AT Modem

Many DCE devices, such as modems, must receive Hayes AT commands to establish communications and configure parameters. To support these devices, the SEL-3025 must support a means to pass Hayes AT commands through the SEL-3025 to the DCE device without encryption. We refer to this as AT Passthrough, which you can enable by selecting the Enable AT Passthrough check box. *Table 7.6* lists the options for the AT Modem setting of the SEL-3025.

Table 7.6 AT Modem Settings

Setting	Values	Description
Enable AT Passthrough	Yes / No	Enable or disable AT passthrough.
Multiple Remote Modems	Yes / No	Indicates whether connections may be formed with multiple different remote modems.
Enable Hangup Sequence	Yes / No	Enable or disable use of "+++" as a hangup sequence.
Enable Status Messages	Yes / No	Enable or disable the device to send informative messages out of the trusted port when modem connections are established or lost.

Frame Synchronization

Use the frame synchronization settings to synchronize serial frames passing through the SEL-3025. *Table 7.7* lists frame synchronization setting options for the SEL-3025.

Table 7.7 Frame Synchronization Settings (Sheet 1 of 2)

Setting	Values	Description
Frame Timeout	1 to 60000 ms	Timeout for frame synchronization activities. Used to determine when to discard an incomplete frame.
Minimum Interframe Deadtime	1.0 to 2000.0 character times or 1 to 20000 bit times	Delay that is applied to delay-delimited protocols. This setting is configurable if the Trusted Interface Protocol is set to Unstructured Point-to-Point or Custom Delay-Delimited.
Maximum Frame Length	2 to 8192 characters	Maximum frame length for frame synchronization activities. If the number of bytes defined is buffered without completing a frame, the frame is considered completed.
Destination Address Location	1 to 8192 bytes	Location of the SCADA address within the protocol. NOTE: This setting applies only when the Trusted Interface Protocol is set to Custom Delay-Delimited.

Table 7.7 Frame Synchronization Settings (Sheet 2 of 2)

Setting	Values	Description
Destination Address Length	1 or 2 bytes	Length of the SCADA address. NOTE: This setting applies only when the Trusted Interface Protocol is set to Custom Delay-Delimited.
Conitel Synchronization Mark Time	8 to 128 bit times	Duration of synchronization mark that is used to indicate the start and middle of a Conitel 2100H frame.
Remote Management Frame Timeout	1 to 30 seconds	Timeout used for remote management frames.

Trusted (DCE) Port

The **Trusted (DCE) Port** settings page provides configuration options for the SEL-3025 serial port connected to the trusted device. *Table 7.8* lists the options for the trusted (DCE) port settings of the SEL-3025.

NOTE: Some of these settings may not be available for editing, depending on the protocol being used.

Table 7.8 Trusted (DCE) Port Settings

Setting	Values	Description
Bits Per Second	1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 48000, 57600	The rate at which this port will transmit data.
Data Bits	6, 7, 8	The number of data bits in each character.
Stop Bits	1, 2	The number of stop bits sent at the end of each character.
Parity	None, Odd, Even	The method of detecting errors in transmission.
Control Signal Mode	None, Full Duplex, Half Duplex	This setting controls which type of flow control is used.
Carrier Detect Control Mode	Constant, Switched, Passthrough	This setting defines the way the carrier detect signal is controlled. This setting is not applicable when the SEL-3025 is configured in AT Passthrough mode.
Pre-Transmit CD Hold Time	0 to 500 character times or 5000 bit times	Amount of time to hold CD asserted before sending first bit of transmission. Only applicable when Carrier Detect Control Mode is set to Switched.
Post-Transmit CD Hold Time	0 to 500 character times or 5000 bit times	Amount of time to hold CD asserted before sending last bit of transmission. Only applicable when Carrier Detect Control Mode is set to Switched.

Untrusted (DTE) Port

The **Untrusted (DTE) Port** settings page provides configuration options for the SEL-3025 serial port connected to a DCE device, such as a modem. *Table 7.9* lists the options for the untrusted (DTE) port settings of the SEL-3025.

NOTE: Pre-Transmit and Post-Transmit RTS Hold Time values only apply when the Control Signal Mode is set to either "Half Duplex Flow Control" or "Push To Talk".

Table 7.9 Untrusted DTE Port Settings

Setting	Values	Description
Bits Per Second	1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 48000, 57600	The rate at which this port will transmit data.
Control Signal Mode	None, Full Duplex, Half Duplex, Push To Talk	This setting controls which type of flow control is used.
Pre-Transmit RTS Hold Time	0 to 500 character times or 5000 bit times	The amount of time to hold the Request To Send (RTS) signal asserted before sending the first byte of the transmission.
Post-Transmit RTS Hold Time	0 to 500 character times or 5000 bit times	The amount of time to hold the Request To Send (RTS) signal asserted after sending the last byte of the transmission.

Remote Address Mappings

NOTE: You will only be able to enter either SCADA addresses or connect strings. This is dependent on the configuration of the SEL-3025 based on the serial network.

Use remote address mappings to identify which remote SEL-3025 is associated with different SCADA addresses or modem connections. The settings on this page provide the mappings between SSCP addresses and SCADA addresses or modem connections, depending on the mode for which the SEL-3025 is configured. To configure the remote address napping on the SEL-3025 with SSCP Address 1 for the example in *Figure 7.8*, you would select **Remote SSCP Device Address 2** and enter **10** as the protected SCADA address. *Table 7.10* lists the options for the remote address mappings.

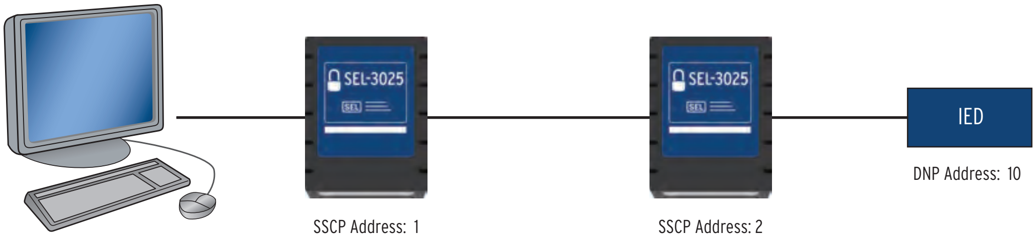


Figure 7.8 Remote Address Mapping

Table 7.10 Remote Address Mappings Settings (Sheet 1 of 2)

Setting	Values	Description
Remote SSCP Device Address	Read-only list of the SSCP addresses of remote devices.	The remote SSCP address of the SEL-3025 protecting the IED behind the trusted (DCE) port.
Protected SCADA Address	0–65535	A comma-separated list of SCADA addresses that are protected by the SEL-3025 with the selected SSCP address. Example: 1,3,10–20,35, 185–203,215

Table 7.10 Remote Address Mappings Settings (Sheet 2 of 2)

Setting	Values	Description
Connect String	String with as many as 40 characters.	Connect string that can be used in “many-to-many” network (point-to-point with multiple possible remotes) to determine which remote SEL-3025 is at the other end of the connection. This string applies to modem connections only and to use of an unstructured protocol. You must have the “Enable AT Passthrough” option selected with “Multiple Remote Modems”, and be using an unstructured protocol (e.g., Unstructured Point To Point), to use connect strings. Examples of connect strings include the following: ATDT5095551234 5095551234
SSCP Address of Single Remote Address	0–65534	SSCP address that is used when multiple remote SSCP device addresses exist but SCADA addresses or connect strings cannot be used. This setting is used when multiple remote SSCP device addresses are defined, the network architecture setting is point-to-point, and the multiple remote modems setting is not enabled.

SSCP Settings

SSCP General

The SSCP general settings define the parameters the SEL-3025 will use to communicate using the SSCP protocol. These settings are applied when creating new SSCP groups. If you prefer to use different default group settings when creating new SSCP groups, change the settings here. These settings do not apply to existing groups. *Table 7.11* lists the options for the SSCP general settings.

Table 7.11 SSCP General Settings (Sheet 1 of 2)

Setting	Values	Description
Data Buffering	Yes / No	This setting controls whether to enable or disable data buffering when no secure session is available.
Device Address	0–65534	SSCP address of the local SEL-3025. This address must be unique within the serial network to which this SEL-3025 is connected.
Encryption Mode	AES-128, AES-256	The encryption protocol used to protect the confidentiality of the data.
Encrypt Data	Yes / No	This setting controls whether or not to encrypt the data.

Table 7.11 SSCP General Settings (Sheet 2 of 2)

Setting	Values	Description
Authentication Mode	SHA-1, SHA-256	The authentication protocol used to protect the integrity of the data.
HMAC Size	4–20 (with SHA-1) 4–32 (with SHA-256)	The number of bytes in the hash-based authentication code (HMAC) appended to the end of the payload.
Max Sequence	100–65535	The maximum sequence number used in transmitted communication.
Key Exchange Interval	1–60 seconds	The minimum time interval between preshared key exchanges. This setting is used to prevent excessive amounts of traffic during a key exchange.

SSCP Group

The SSCP group settings define the parameters the SEL-3025 will use to communicate with remote SEL-3025 serial shields listed in the SSCP group settings as remote SSCP device addresses.

Table 7.12 SSCP Group Setting (Sheet 1 of 2)

Setting	Values	Description
Group Name	1–32 characters	Name of the SSCP device group
Remote SSCP Addresses	0–65534	A comma-separated list of SSCP addresses of the remote SEL-3025 devices with which this SEL-3025 will communicate. Example: 1,3,10–20,35,185–203,215
Authentication Mode	SHA-1, SHA-256	The authentication protocol used to protect the integrity of the data.
Authentication Key	40 hexadecimal (0–9, A–F) characters (SHA-1) 64 hexadecimal (0–9, A–F) characters (SHA-256)	Master authentication key for remote devices in the group.
Encryption Mode	AES-128, AES-256	The encryption protocol used to protect the confidentiality of the data.
Encryption Key	32 hexadecimal (0–9, A–F) characters (AES-128) 64 hexadecimal (0–9, A–F) characters (AES-256)	Master encryption key for remote devices in the group.
HMAC Size	4–20 (with SHA-1) 4–32 (with SHA-256)	The number of bytes in the HMAC appended to the end of the payload.
Max Sequence	100–65535	The maximum sequence number used in transmitted communication.

Table 7.12 SSCP Group Setting (Sheet 2 of 2)

Setting	Values	Description
Key Exchange Interval	1–60 seconds	The minimum time interval between pre-shared key exchanges. This setting is used to prevent excessive amounts of traffic during a key exchange.
Encrypt Data	Yes / No	This setting controls whether or not to encrypt the data.

SEP Settings

SEP General

The SEP general settings define the parameters the SEL-3025 will use for communication with Streaming Encryption Protocol (SEP). *Table 7.13* lists SEP general settings options.

Table 7.13 SEP General Settings

Setting	Values	Description
Data Buffering	Yes / No	Buffer data when no secure session is available. This setting applies to the local device.
Sequence Size	1 to 8 Default 3	Number of bytes dedicated to transmission of the sequence number and the OOB/IB control bit. The actual number of bits is (8*'Sequence Size'- 1).
Device Address	0 to 65534 Default 0	SEP address of the local device. This address must be unique.

SEP Group

Table 7.14 SEP Group Settings

Setting	Values	Description
Group Name	1–32 characters	Name of the SEP device group.
Remote SEP Device Addresses	0–65534	Comma-separated list of the SEP addresses of the remote SEL-3025 devices with which this SEL-3025 will communicate.
System Key	64 hexadecimal (0–9, A–F) digits	Shared encryption key used by all members of the group.

SEP Advanced

The SEP advanced settings are parameters that you do not normally need to modify from their default values. You would normally modify these settings on instructions from SEL product support to meet the requirements of unusual applications.

Table 7.15 SEP Advanced Settings

Setting	Values	Description
Max Response Time	10 to 60000 ms Default 1000	The maximum time that the device will wait for complete acquisition of a reply to an IB or OOB message.
Key Validation Max Confidence	1 to 32 frames Default 5	The minimum number of consecutive frames that can fail decryption validation before the device initiates a rekey request with the remote device.
Sequence Anomaly Threshold	1 to 32 frames Default 10	The maximum difference between the sequence the device last received and the current sequence for which the device will accept the current frame and update the next expected sequence number.
Sequence Anomaly Acceptance Threshold	1 to 32 frames Default 10	The maximum consecutive sequence anomalies the device will reject before accepting the frame and updating the next expected sequence number.
Sequence Rejection ReKey Threshold	1 to 32 frames Default 20	The maximum consecutive frames that the device will reject because of sequence mismatches before invalidating the decryption key.
Session Use Timeout	1 to 86400 seconds Default 60	The time that a decryption session can proceed without use before the device initiates a key status cycle. If a slave device is unresponsive, the master device continues to initiate a key status cycle at this frequency until it receives a response.
Synchronization Mode	Pattern-based with Escaping, Delay-delimited, Bit-based	The frame synchronization on SEP frames. The default value is delay-delimited.

Remote Management

NOTE: Enabling remote management adds another byte to the SSCP header.

The remote management functionality of the SEL-3025 allows operators to securely manage other SEL-3025 devices even if the Ethernet network is not extended out to remote sites. The remote management web interface consists of the following pages: **Remote Log In**, **Remote Ping**, and **Secure Mode Initiation**. The remote management pages are available based on the operating mode of the SEL-3025, cryptographic module status, network architecture, and if remote management is enabled on the device. The master SEL-3025 must have the **Enable Remote Management** setting enabled and a network architecture where the device is a client (point-to-point client, point-to-multipoint client). The slave SEL-3025 device(s) must have the **Enable Remote Management** setting enabled and a network architecture where the device is a server (point-to-point client, point-to-multipoint server). In *Figure 7.9*, the SEL-3025 device connected to the Ethernet network is configured as a point-to-point client. The remote SEL-3025 at Substation 1, configured as a point-to-point server, is not connected to an Ethernet network. Through use of the remote management functionality of the SEL-3025, you can still manage the remote device through the SEL-3025 at the Control Center. The Operator Workstation connects through the Ethernet network to the SEL-3025 at the Control Center and logs on through the HTTPS web interface. From the user interface, the operator navigates to the **Remote Log In** page and connects to the SEL-3025 at Substation 1 over the untrusted serial network.

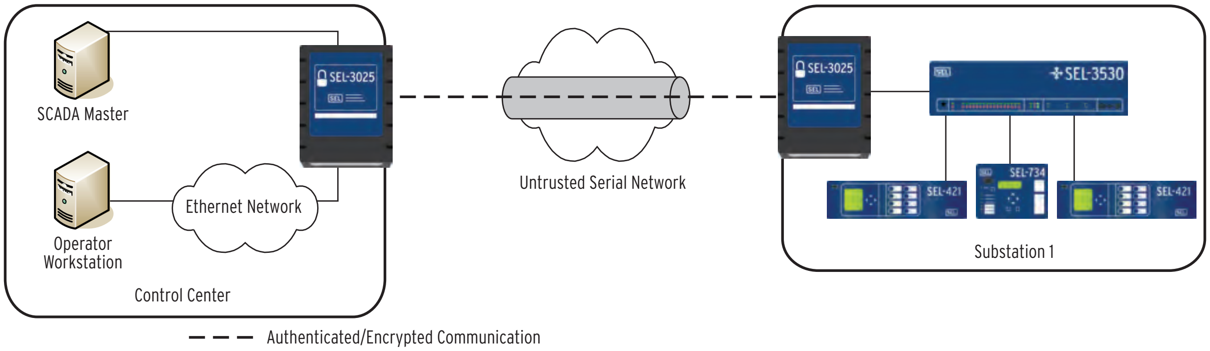


Figure 7.9 Remote Management Example

Remote Log In

NOTE: SCADA messages will be dropped during the user session when a user successfully logs on to a remote device through the Remote Log In page. Normal serial data processing will resume after the user logs out of the remote management session.

The **Remote Log In** page allows users to manage remote SEL-3025 devices over the serial communications network. The SEL-3025 devices communicating must have the **Enable Secure Protocol** setting enabled, have an SSCP group with the remote SSCP address, and be configured to encrypt data to use the remote log in feature. Sensitive information, such as usernames and passwords, must pass over the serial communications channel and must have encryption to ensure data confidentiality. The remote SEL-3025 uses usernames, passwords, and privileges to determine which users can log in to the device as well as what authorization level an authenticated user shall have.

Remote Ping

The **Remote Ping** page allows users to query the connection status of a remote SEL-3025 device.

The SEL-3025 devices communicating must have the **Enable Secure Protocol** setting enabled and have an SSCP group with the remote SSCP address to use the remote ping feature. Encryption is optional when you use the remote ping feature.

Secure Mode Initiation

Customers may need to put SEL-3025 devices in service with their cryptographic functionality disabled. When all devices are installed and it is time to enable the system security, significant time and effort may be necessary to directly access each unit. If Ethernet connectivity is not widely available, this may even require significant travel. Even with Ethernet availability, accessing every device may take a long time and is prone to human error. As devices are enabled, communications links are lost until the matching device at the other end of the line is also enabled.

NOTE: Increase the Remote Management Frame Timeout value if your serial network has high latency.

Secure mode initiation, or SMI, allows all SEL-3025 devices on a single serial network to be enabled quickly and conveniently in an automated fashion. Similar to the other remote management functions, the SMI interface is available through the HTTPS web interface on a master SEL-3025 with the **Enable Remote Management** setting enabled and a network architecture where the device is a client (point-to-point client, point-to-multipoint client). SMI changes the security state from pass-through mode to secure mode, so the master SEL-3025 device must also have the **Enable Secure Protocol** setting disabled for the SMI process to initiate the transition from pass-through mode to secure mode.

Reports

System Logs

The SEL-3025 uses the Syslog message format to record event data. The SEL-3025 has storage for 2048 of these messages. The SEL-3025 can also forward Syslog messages to two destinations.

A message can have seven different severity ratings, ranging from informational to emergency. There are five possible facilities on the SEL-3025: Kernel, System Daemon, Security/Authorization, Clock Daemon, and Log Audit. The **Tag Name** field indicates which part of the system generated the message. The **Time Stamp** and **Message** fields include the time stamp of when the message was generated and the message description.

Select the system logs link from the navigation panel to show the internal system logs.

Event messages in the SEL-3025 have two states: unacknowledged and acknowledged. These two states exist to make identification of abnormal event generation easier. Large numbers of unacknowledged messages can indicate high levels of activity on the SEL-3025.

Message acknowledgment also assists with log documentation. In your periodic examination of logs, acknowledge existing logs. When you examine logs in the future, the previously acknowledged logs will limit the logs of concern to only those logs the SEL-3025 generated since the last examination.

You can filter the SEL-3025 system logs to track certain events. Configure the filters with the form above the system logs list.

Click the **ACK** button to acknowledge selected system logs. You cannot remove system logs from the SEL-3025 without issuing a factory-default reset.

Diagnostics

The **Diagnostics** page contains information that may be useful for troubleshooting the SEL-3025. The **Diagnostics** page contains two actions that a user with administrator or engineer privileges can perform; *Table 7.16* lists these actions.

Table 7.16 Diagnostics Page Actions

Setting	Description
Clear Status Failures	The **Clear Status Failures** button is used to clear status failures.
Pulse Alarm Contact	The **Pulse Alarm Contact** button is used to manually pulse the alarm contact. Pulse duration is configurable from 1–30 seconds.

For more information about the **Diagnostics** page, please refer to *Section 8: Testing and Troubleshooting*.

Serial Communications Status

The serial communications status report contains information that can be useful for troubleshooting the SEL-3025. The SEL-3025 stores serial communications error counters in volatile memory and clears these counters upon a power cycle or restart.

For more information about the **Serial Communications Status** page, please refer to *Section 8: Testing and Troubleshooting*.

Task List Report

Use the task list report to determine the status of system resources. Use this information primarily for troubleshooting the device with the SEL factory.

Access to the **Task List Report** webpage is available for users in the Administrator and Engineer groups.

Vector Reports

The vector report is a textual display of data that represent the processor and memory state if an exception were to occur within the firmware. Use this information primarily for troubleshooting the device with the SEL factory.

Access to the **Vector Report** webpage is available for users in the Administrator and Engineer groups.

This page intentionally left blank

Section 8

Testing and Troubleshooting

Introduction

This section provides guidelines for testing and troubleshooting the SEL-3025 Serial Shield®.

- *Testing Philosophy*
- *Indicator Lights*
- *Diagnostics Page*
- *Troubleshooting*
- *Factory Assistance*

Testing Philosophy

We can divide SEL-3025 testing into three categories: acceptance, commissioning, and maintenance testing. We differentiate the categories both by when they take place in the life cycle of the transceiver and by test complexity. The following paragraphs describe when you should perform each type of test, the goals of testing at that time, and the functions that you need to test at each point.

This information is intended as a guideline for testing an SEL-3025.

Acceptance Testing

Perform acceptance testing when qualifying an SEL-3025 for use in a serial communications system that requires data authentication with optional data encryption.

Goals of Acceptance Testing

- Ensure that the SEL-3025 meets published critical performance specifications.
- Ensure that the SEL-3025 meets the requirements of the intended application.
- Improve your familiarity with SEL-3025 capabilities.

What to Test

Perform acceptance testing on all setting parameters critical to your intended application.

SEL performs detailed acceptance testing on all SEL-3025 models and versions. Any SEL-3025 we ship meets published specifications. It is important for you to perform acceptance testing on an SEL-3025 if you are unfamiliar with SEL-3025 operating theory or settings. Such testing helps you ensure that SEL-3025 settings are correct for your application.

Commissioning Testing

Perform commissioning testing when you install a new SEL-3025.

Goals of Commissioning Testing

- Ensure that power connections are correct.
- Ensure that the alarm output connection is correct.
- Ensure that the SEL-3025 functions with your settings according to your expectations.

What to Test

Perform commissioning testing on the Ethernet port, serial ports, and your alarm output.

SEL performs a complete functional check of each SEL-3025 before shipment. SEL-3025 commissioning tests should verify that the power supply, serial cables, and alarm output (if used) are connected properly. Commissioning testing should also ensure proper configuration and operation of the HTTPS management interface.

Maintenance Testing

The SEL-3025 does not require regular maintenance testing. If you use the alarm output, you can use the HTTPS management interface to run the **Pulse** command to verify functionality between the SEL-3025 and a connected device.

Indicator Lights

The SEL-3025 has extensive self-test capabilities. You can determine the status of your SEL-3025 with the indicator lights located on the front of the device. *Table 8.1* and *Table 8.2* summarize the operation of the indicator lights.

Table 8.1 SEL-3025 Indicator Lights

Indicator Light	Green Condition	Red Condition
DEVICE	Normal operations	A diagnostics failure has occurred with the device that is not related to the cryptographic functionality.
CRYPTO	Normal operations	A diagnostics failure has occurred with the device that is specifically related to the cryptographic functionality.

Table 8.2 SEL-3025 Indicator Lights (Blink Rate)

Indicator Light	Blink Rate (seconds)	State
CRYPTO (green)	OFF	Secure protocol is disabled via device configuration.
CRYPTO (green)	0.25	Secure protocol is not being applied because the modem is disconnected.
DEVICE (red)	0.25	A firmware failure has occurred.

In addition to the front-panel indicators, the SEL-3025 features activity LEDs on all three of the I/O connectors on the rear panel.

The amber LED on the Ethernet connector indicates the cable is connected to a live network. The green LED indicates traffic on the network.

On the DCE and DTE connectors, the amber LED indicates data the SEL-3025 received on that connector. The green LED indicates data the SEL-3025 transmitted on that connector.

Table 8.3 Serial Port Connector Indicators

Indicator Light	Meaning
DCE amber	The SEL-3025 is receiving data on the trusted interface (in the clear) from a PC or a device.
DCE green	The SEL-3025 is sending data to a PC or connected device on the trusted interface.
DTE amber	The SEL-3025 is receiving data from the distant cryptographic transceiver on the untrusted interface.
DTE green	The SEL-3025 is sending data to the distant cryptographic transceiver on the untrusted interface.

Diagnostics Page

While the SEL-3025 status indicator lights are useful for getting status information at a quick glance, they will only alert you to normal versus abnormal operating conditions. For more detailed diagnostics information, visit the **Diagnostics** page by selecting the **Diagnostics** link from the navigation panel.

Table 8.4 Diagnostics Page (Sheet 1 of 2)

Field Name	Description
Firmware ID	Firmware version of the SEL-3025.
Serial Number	Serial number assigned to the SEL-3025.
Device State	Current state of the device.
RAM	RAM status.
FLASH	Code and data flash status.
FPGA	FPGA status.
Clock	Real-time clock status.
Clock Battery	Real-time clock battery status.

Table 8.4 Diagnostics Page (Sheet 2 of 2)

Field Name	Description
Web Certificate	Web certificate status. “DEFAULT” indicates the default SEL certificate is being used. “OK” indicates a certificate has been uploaded and is being used.
Operating Hours	Number of hours the SEL-3025 has been operating.
Power-On Counts	Number of times the SEL-3025 has been turned on.
Cryptographic Module State	The state of the cryptographic functionality of the SEL-3025.
Cryptographic Sessions	The number of cryptographic sessions currently in use.
Invalid Cryptographic Sessions	The number of cryptographic sessions that are currently identified as “invalid”.
Cryptographic Module ID Number	Identification number of the module that provides cryptographic functionality.
Cryptographic Module Firmware Version	Firmware version of the module that provides cryptographic functionality.
Cryptographic Module Hardware Version	Hardware version of the module that provides cryptographic functionality.
Secure SELBoot Firmware Version	Firmware version of Secure SELBoot

Troubleshooting

Inspection Procedure

Complete the following procedure before disturbing the SEL-3025. After you finish the inspection, refer to *Table 8.5*.

Step 1. If Ethernet is installed and the HTTPS web management interface is configured for the network, check that the web interface is accessible.

Step 2. Measure and record the power supply voltage at the power input terminals.

Step 3. Record the state of the light indicators.

Table 8.5 Troubleshooting Procedure

Problem	Possible Causes	Solution
The DEVICE and CRYPTO indicator lights are dark.	Input power is not present.	Verify that input power is present.
The login page is inaccessible.	Input power is not present.	Verify that input power is present.
	HTTP connections to the SEL-3025 are being attempted to Port 80.	Prefix the IP address with https:// in your web browser.
	The computer trying to connect to the web interface is not on the correct network.	Configure the IP address of the management computer to the same network as the SEL-3025.

Table 8.5 Troubleshooting Procedure

Problem	Possible Causes	Solution
	Network errors are preventing communication.	Verify the physical and logical connection between the management computer and the SEL-3025. If the active scripting setting is disabled in Internet Explorer, you may receive an error with res://ieframe.dll/ as the URL in the address bar. Enable active scripting in your Internet Explorer browser settings, or attempt to access the login page with a different web browser.
No Syslog messages.	Unable to reach the Syslog server.	Ensure that the Syslog server IP address is valid and reachable, or that a network gateway is configured and available to route the Syslog traffic.
A user cannot log on.	The user's password is incorrect.	Wait 30 seconds for the account to unlock and try again. Have an administrator or user manager change the password if the user cannot remember the correct password.
	The user's account has been locked because of repeated incorrect passwords.	Wait 30 seconds for the account to unlock and try again.
No data communication between units.	SSCP Setup is incorrect.	On the client unit, on the navigation bar in the **Remote Mgmt** group, click **Remote Ping**. Most SSCP setup errors will result in display of "Ping timeout: no response from remote device." If this occurs, check the SSCP addresses and that the key material matches on the two units. If the ping result is "Ping successful: response received," SSCP is set up correctly, and the problem is most likely in cabling and interconnections.
	Trusted Interface Protocol is incorrect.	Set the **Trusted Interface Protocol** on the **System Communication** settings page to match the data the SEL-3025 is handling. In a point-to-point configuration, you should be able to use either the actual protocol (e.g., DNP3) or Unstructured Point-to-Point. In a point-to-multipoint application, the SEL-3025 will be associating SSCP peer addresses with protocol addresses, so setting the protocol to match is important.
	Data are being lost because data buffering is not turned on.	Check the **Data Buffering** check box on the **SSCP General** settings page under **SSCP General**. Enabling data buffering stops the SEL-3025 from flushing data from queues when it switches to secure mode. Under some circumstances, flushing data can cause the SEL-3025 to discard the now incomplete data for the first frame.

Serial Communications Status Page

The **Serial Communications Status** page contains information that may be useful for troubleshooting the SEL-3025. Errors appearing on this page may indicate mismatched serial settings between devices connected to the respective ports.

The SEL-3025 stores serial communications error counters in volatile memory and clears these counters upon a power cycle or restart.

Task List Page

Use the SEL-3025 task list page to determine the status of the threads and system resources within the firmware. Use this page primarily during factory assistance.

To access the **Task List Report** webpage, log in to the SEL-3025 as an administrator or engineer user and click on the **Tasklist** link on the navigation menu.

Vector Report

The **Vector Report** webpage provides information about the processor and memory state if an exception occurs. You can access the **Vector Report** webpage by logging on as an administrator or engineer user and clicking on the **Vectors** link on the navigation menu. The SEL-3025 can store the last two vector reports. You can save vector reports by clicking **Save As** from your web browser. You can then send this saved file to SEL for analysis.

Factory Assistance

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 USA
Phone: +1.509.332.1890
Fax: +1.509.332.7990
Internet: www.selinc.com
Email: info@selinc.com

Appendix A

Firmware and Manual Versions

Firmware

This manual covers SEL-3025 Serial Shield® devices containing firmware bearing the firmware version numbers listed in *Table A.1*. This table also lists a description of modifications and the instruction manual date code that corresponds to firmware versions. The most recent firmware version is listed first.

Table A.1 Firmware Revision History

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3025-R110-V0-Z104104-D20150107 SEL-3025-R109-V0-Z102102-D20150107	➤ Resolved the handling of unrecognized Ethertype frames that can cause Ethernet to stop responding. ➤ Removed support for weaker cryptographic algorithms for the web management interface. ➤ Increased the supported key size range for certificates. ➤ Resolved the security vulnerability detailed in CVE-2014-3566 POODLE. ➤ Updated System Logs webpage to display correct page numbering and improve page navigation. ➤ Updated the operations of the password confirmation field when adding users.	20150107
SEL-3025-R106-V0-Z104102-D20120406	➤ Added setting Data Buffering options when using point-to-multipoint mode with bit protocols, which had been disallowed.	20120406
SEL-3025-R105-V0-Z102101-D20120406	➤ Changed to firmware supporting manufacturing processes to simplify initialization of flash memory.	
SEL-3025-R104-V0-Z103102-D20111205	➤ Changed secure protocol to SEP for real-time SCADA applications, added support for settings import and export, changed framing for Conitel and other bit-based protocols.	20111205
SEL-3025-R103-V0-Z102101-D20111205	➤ Added support for settings import and export, removed support for bit-based protocols (available with SEP cryptographic protocol).	
SEL-3025-R102-V0-Z101100-D20100806	➤ Switched Carrier support and corrected Conitel protocol.	20100806
SEL-3025-R101-V0-Z100100-D20100715	➤ Initial version.	20100715

Instruction Manual

The date code at the bottom of each page of this manual reflects the creation or revision date.

Table A.2 lists the instruction manual release dates and a description of modifications. The most recent instruction manual revisions are listed at the top.

Table A.2 Instruction Manual Revision History (Sheet 1 of 2)

Revision Date	Summary of Revisions
20151009	**Section 1** ➤ Clarified alarm output connections information. ➤ Updated *Specifications*.
20150107	**Preface** ➤ Updated *Safety Information.* **Section 1** ➤ Updated for FIPS 140-2. ➤ Updated *Specifications*. ➤ Updated browser requirements. **Section 2** ➤ Added a note to *Commissioning the SEL-3025.* **Appendix A** ➤ Updated for firmware versions R109 and R110.
20140602	**Section 1** ➤ Updated *Specifications*.
20120406	**Section 1 and Section 6** ➤ Removed FIPS 140-2 certification because of change from version certified. **Appendix A** ➤ Updated for firmware versions R105 and R106.
20111205	**Section 1** ➤ Added comparison information for SSCP and SEP ordering options. **Section 4** ➤ Added description and instructions for the PC Serial Security Kit. **Section 5** ➤ Added description of SEL-3045 configuration using ACSELERATOR QuickSet. **Section 6** ➤ Added SEP application example (Job Done 4). ➤ Changed application example (Job Done 1) to engineering access using PC Serial Security Kit. **Section 7** ➤ Added *SEP Settings*. ➤ Added *Table 7.13: SEP General Settings*. **Section 8** ➤ Added *Table 3.8: Serial Port Connector Indicators*. ➤ Added additional information to *Table 8.5: Troubleshooting Procedure*. **Appendix A** ➤ Updated for firmware versions R103 and R104.

Table A.2 Instruction Manual Revision History (Sheet 2 of 2)

Revision Date	Summary of Revisions
20100806	**Section 5** ➤ Added Carrier Detect Control Mode, Pre-Transmit CD Hold Time, and Post-Transmit CD Hold Time settings (*Table 5.8: Trusted (DCE) Port Settings*). **Appendix A** ➤ Updated for firmware version R102.
20100715	➤ Initial version.

This page intentionally left blank

Appendix B
Firmware Upgrade Instructions

Introduction

SEL occasionally offers firmware upgrades to improve the performance of your SEL-3025. Updating of settings and firmware occurs in nonvolatile memory, so it is unnecessary for you to open your unit. These instructions provide step-by-step procedures for upgrading the SEL-3025 by uploading files from a personal computer into the SEL-3025. The SEL-3025 logs all firmware updates.

SEL-3025 updates can be for the SEL-3025 itself, for the cryptographic card inside the SEL-3025, or for the program loader called Secure SELBOOT. To perform an update, you will need the appropriate upgrade file(s) and you will need to be logged in with an administrator account on the SEL-3025.

These instructions cover the following upgrades:

➤ *Upgrading SEL-3025 Firmware From Version R103 or Higher*

➤ *Upgrade Procedure: Version R102 to the Latest SSCP Release for Engineering Access*

➤ *Upgrade Procedure: Version R102 to the Latest SEP Release for SCADA Protection*

➤ *Upgrade Procedure for the Cryptographic Card*

➤ *Converting the SEL-3025 Between SSCP and SEP Protocols*

About Firmware Files

The SEL-3025 firmware files contain cryptographic signatures to enable the SEL-3025 to recognize official SEL upgrades. The SEL-3025 will not process any uploaded upgrade files that it cannot verify as being produced by SEL.

About the Upgrade Procedures

If you are upgrading the SEL-3025 to firmware version R103 or higher from firmware version R102 or lower, you must upgrade Secure SELBOOT to version R101 or higher before you perform the firmware upgrade. If your device is at SELBOOT version R102 or higher, it should not be downgraded to any version of SELBOOT lower than R102. You must also use the serial port, with a terminal emulator program capable of performing Xmodem file transfers. Note that upgrading SELBOOT firmware is a critical operation. If a loss of power interrupts this operation before it completes, you may need to return your unit to SEL for service. Upgrading SELBOOT typically takes about 15 seconds.

If the upgrade will change the secure protocol used by your SEL-3025 (e.g. upgrading to the latest SEP release from R102), you must first upgrade the cryptographic card in your SEL-3025. You can perform this upgrade through use of the Web Management interface of the SEL-3025. After upgrading the card, if upgrading from a version lower than R103, you must then upgrade Secure SELBOOT to version R101 or higher before you finally perform the firmware upgrade. To perform Secure SELBOOT and firmware upgrades, you must use the serial port, with a terminal emulator program capable of performing Xmodem file transfers. Note that upgrading SELBOOT firmware is a critical operation. If a loss of power interrupts the operation before it completes, you may need to return your unit to SEL for service.

Upgrading SEL-3025 Firmware From Version R103 or Higher

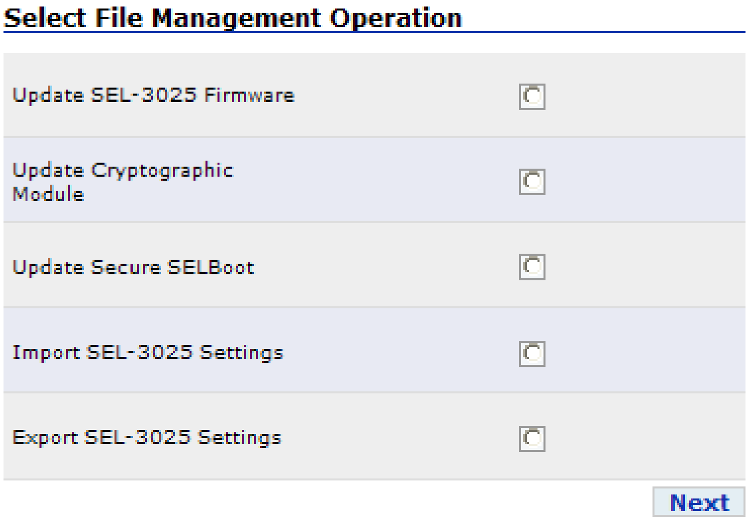
Use this procedure if your SEL-3025 is already running R103 or higher firmware, and the upgrade will not change the secure protocol. If the upgrade will change your unit between SSCP and SEP protocols, see the section *Converting the SEL-3025 Between SSCP and SEP Protocols*. If you logged in as an administrator or engineer, you can use the web interface to upgrade firmware. Perform the following steps to upgrade your SEL-3025:

Use the Management Web Interface to Upgrade the SEL-3025

If you logged in as an administrator or engineer, you can use the web interface to upgrade firmware from version R103 or higher. Perform the following steps to upgrade your SEL-3025.

Step 1. Use an account in the Administrator or Engineer group to log in to the Ethernet Management interface of the SEL-3025. Accounts not assigned to one of these groups cannot perform firmware upgrades.

Step 2. Select the **File Management** link from the navigation panel to display the **File Management** page on your computer screen.



Select File Management Operation

Update SEL-3025 Firmware	○
Update Cryptographic Module	○
Update Secure SELBoot	○
Import SEL-3025 Settings	○
Export SEL-3025 Settings	○

Figure B.1 File Management Page

Step 3. Select the upgrade type (SEL-3025 firmware, Cryptographic Module, Secure SELBOOT, or SEL-3025 Settings).

Step 4. Click the **Next** button.

Step 5. On the next page, either type in the full path to the upgrade file, or click the **Browse** button to locate it.

Step 6. Click the **Send File** button to install the upgrade. The SEL-3025 will verify the file and then install it. Depending upon the type of upgrade performed, you may need to re-establish the browser connection to the Ethernet Management Port and log in again.

Upgrade Procedure: Version R102 to the Latest SSCP Release for Engineering Access

This procedure upgrades your SSCP-protocol SEL-3025 to the most recent firmware release. Use this procedure for units you have deployed for engineering access applications such as protection of dialup modems. This procedure first upgrades Secure SELBOOT and then the SEL-3025 firmware.

Use the Serial Port to Upgrade Secure SELBOOT

To upgrade Secure SELBOOT to version R101, perform the following steps:

Step 1. Remove power from your SEL-3025.

Step 2. Use an SEL-C609 or equivalent cable to connect the PC serial port to the trusted (DCE) interface.

Step 3. Set the PC terminal emulation program to 9600 bits per second, 8 bits, no parity, 1 stop bit, with no flow control.

Step 4. Enter SELBOOT mode by applying power to the SEL-3025 while pressing and holding the reset button. If you have successfully entered SELBOOT mode, the front-panel LEDs will flash alternately.

Step 5. Press **<Enter>** and verify that you receive a !> prompt. If you do not, go back to *Step 2*

Step 6. Set the SEL-3025 data rate to 115200 bps by typing **BAUD 115200 <Enter>**.

Step 7. Change the terminal program data rate to 115200 bps, press **<Enter>** again, and verify that you receive the prompt.

Step 8. Type **REC BOOT <Enter>** at the prompt. The device will prompt you to confirm that you want to erase the existing firmware.

Step 9. Type **Y** at the prompt, press **<Enter>**, and then follow the instructions on the screen.

Step 10. Press the spacebar and then use Xmodem protocol to send the upgrade file.

Your computer screen will display three messages: `Erasing SELboot, Writing SELboot`, and `Restarting SELboot`. You should then see the front-panel LEDs flash alternately.

Step 11. Change the terminal program data rate to 9600 bps, press **<Enter>** again, and verify that you receive the prompt.

Once you have upgraded Secure SELBOOT, you can proceed with upgrading the SEL-3025 firmware. To load the upgrade firmware perform the following steps.

Use the Serial Port to Upgrade the SEL-3025 Firmware

Step 1. Connect a terminal emulator program to Secure SELBOOT as described in *Use the Serial Port to Upgrade the SEL-3025 Firmware*.

Step 2. Set the SEL-3025 data rate to 115200 bps by typing **BAUD 115200 <Enter>**.

Step 3. Change the terminal program data rate to 115200 bps, press **<Enter>** again, and verify that you receive the prompt.

Step 4. Type **REC <Enter>** at the prompt. The device will prompt you to confirm that you want to erase the existing firmware.

Step 5. Type **Y** at the prompt, press **<Enter>**, and then follow the instructions.

Step 6. Press the spacebar and then use Xmodem protocol to send the firmware upgrade file.

Your computer screen will display two messages: `Erasing firmware` and `Erase successful`. You should then see the front-panel LEDs flash alternately.

Do not disturb the device until after your computer screen displays the message `Upload completed successfully. Attempting a restart.` and one or both front-panel LEDs illuminate.

The upgrade is complete.

Upgrade Procedure: Version R102 to the Latest SEP Release for SCADA Protection

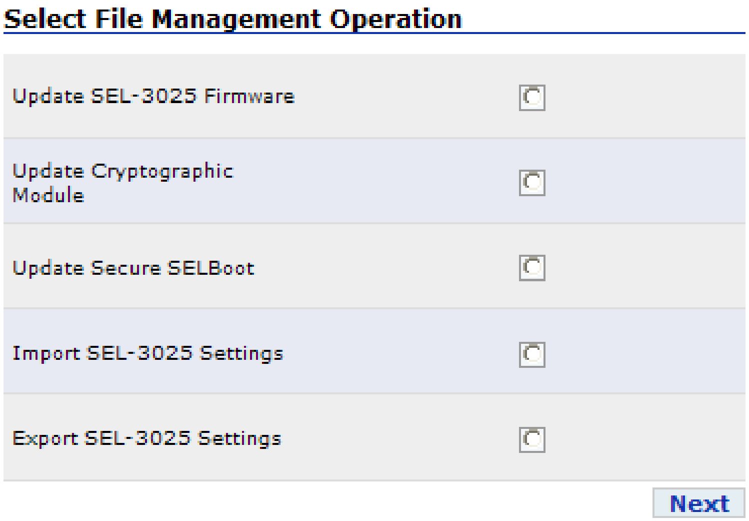
This procedure changes your SSCP-protocol SEL-3025 to use the SEP protocol, with the most recent firmware release. Use this procedure for units you intend for SCADA applications. This procedure updates the firmware of the cryptographic card inside the SEL-3025. It also upgrades Secure SELBOOTand the SEL-3025 firmware.

Upgrade the Cryptographic Card

Step 1. Use an account in the Administrator group to log in to the Ethernet Management interface of the SEL-3025.

Accounts not assigned to this group cannot perform cryptographic card updates.

Step 2. Select the **File Management** link from the navigation panel to display the **File Management** page on your computer screen.



Select File Management Operation

Update SEL-3025 Firmware	○
Update Cryptographic Module	○
Update Secure SELBoot	○
Import SEL-3025 Settings	○
Export SEL-3025 Settings	○

Figure B.2 File Upgrade Page

Step 3. Select the **Update Cryptographic Module** check box.

Step 4. Click the **Next** button.

Step 5. Click the **Browse** button to display a file browser window.

Step 6. Navigate to the location of the upgrade file and select it.

Step 7. Click the **Send File** button. The file download will take about a minute.

When the download is complete, your computer screen will display `Transferring file to Cryptographic Module` while the new firmware file is being loaded onto the card. This will take about two minutes.

Step 8. Wait for the card update operation to complete.

When the transfer is complete, the SEL-3025 will restart to complete the card upgrade process. During this process, the front-panel LEDs will be unlit. Do not disturb the unit until one or more front-panel LEDs illuminate, after about one minute.

Use the Serial Port to Upgrade Secure SELBOOT

To upgrade Secure SELBOOT to version R101, perform the following steps:

Step 1. Remove power from your SEL-3025.

Step 2. Use an SEL-C609 or equivalent cable to connect the PC serial port to the trusted (DCE) interface.

Step 3. Set the PC terminal emulation program to 9600 bits per second, 8 bits, no parity, 1 stop bit, with no flow control.

Step 4. Enter SELBOOT mode by applying power to the SEL-3025 while pressing and holding the reset button. If you have successfully entered SELBOOT mode, the front-panel LEDs will flash alternately.

Step 5. Press **<Enter>** and verify that you receive a !> prompt. If you do not, go back to *Step 2*.

Step 6. Set the SEL-3025 data rate to 115200 bps by typing **BAUD 115200 <Enter>**.

Step 7. Change the terminal program data rate to 115200 bps, press **<Enter>** again, and verify that you receive the prompt.

Step 8. Type **REC BOOT <Enter>** at the prompt. The device will prompt you to confirm that you want to erase the existing firmware.

Step 9. Type **Y** at the prompt, press **<Enter>**, and then follow the instructions on the screen.

Step 10. Press the spacebar, and then use Xmodem protocol to send the upgrade file.

Your computer screen will display three messages: `Erasing SELboot`, `Writing SELboot`, and `Restarting SELboot`. You should then see the front-panel LEDs flash alternately.

Step 11. Change the terminal program data rate to 9600 bps, press **<Enter>** again, and verify that you receive the prompt.

Once you have upgraded Secure SELBOOT, you can proceed with upgrading the SEL-3025 firmware. To load the upgrade firmware perform the following steps.

Use the Serial Port to Upgrade the SEL-3025 Firmware

Step 1. Connect a terminal emulator program to Secure SELBOOT as described in *Use the Serial Port to Upgrade Secure SELBOOT*.

Step 2. Set the SEL-3025 data rate to 115200 bps by typing **BAUD 115200 <Enter>**.

Step 3. Change the terminal program data rate to 115200 bps, press **<Enter>** again, and verify that you receive the prompt.

Step 4. Type **REC <Enter>** at the prompt. The device will prompt you to confirm that you want to erase the existing firmware.

Step 5. Type **Y** at the prompt, press **<Enter>**, and then follow the instructions.

Step 6. Press the spacebar and then use Xmodem protocol to send the firmware upgrade file.

Your computer screen will display two messages: `Erasing firmware` and `Erase successful`. You should then see the front-panel LEDs flash alternately.

Do not disturb the device until after your computer screen displays the message `Upload completed successfully. Attempting a restart.` and one or both front-panel LEDs illuminate.

The upgrade is complete.

Upgrade Procedure for the Cryptographic Card

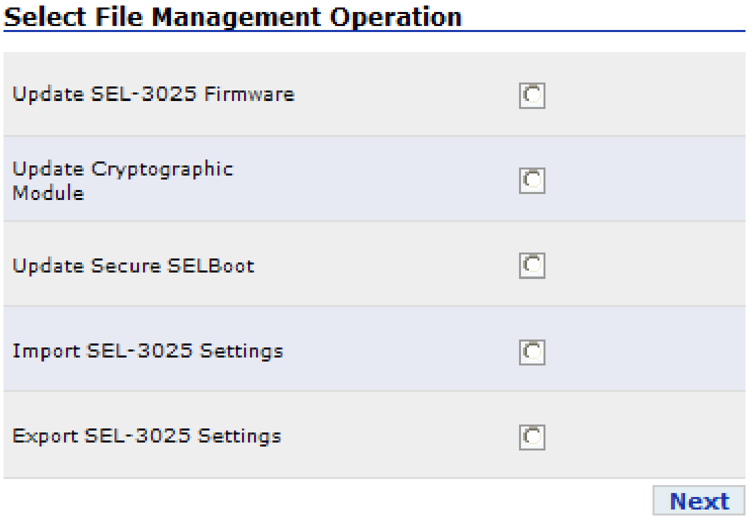
If your SEL-3025 unit has been upgraded to firmware release R103 or higher, you can use the SEL-3025 Web Management interface to load updates to the cryptographic card firmware. You can perform cryptographic card updates to upgrade the performance of the card or to change the secure protocol the card uses (convert an SEL-3045 to an SEL-3044 or vice versa).

Upgrade the Cryptographic Card

Step 1. Use an account in the Administrator group to log in to the Ethernet Management interface of the SEL-3025.

Accounts not assigned to this group cannot perform cryptographic card upgrades.

Step 2. Select the **File Management** link from the navigation panel. This will show the **File Management** page.



Select File Management Operation

Update SEL-3025 Firmware	○
Update Cryptographic Module	○
Update Secure SELBoot	○
Import SEL-3025 Settings	○
Export SEL-3025 Settings	○

Figure B.3 File Upgrade Page

Step 3. Select the **Update Cryptographic Module** check box.

Step 4. Click the **Next** button.

Step 5. Click the **Browse** button to display a file browser window.

Step 6. Navigate to the location of the upgrade file and select it.

Step 7. Click the **Send File** button. The file download will take about a minute.

When the download is complete, your computer screen will display `Transferring file to Cryptographic Module` while the new firmware file is being loaded onto the card. This will take about two minutes.

Step 8. Wait for the card update operation to complete.

When the transfer is complete, the SEL-3025 will restart to complete the card upgrade process. During this process, the front-panel LEDs will be unlit. Do not disturb the unit until one or more front-panel LEDs illuminate, after about one minute.

Converting the SEL-3025 Between SSCP and SEP Protocols

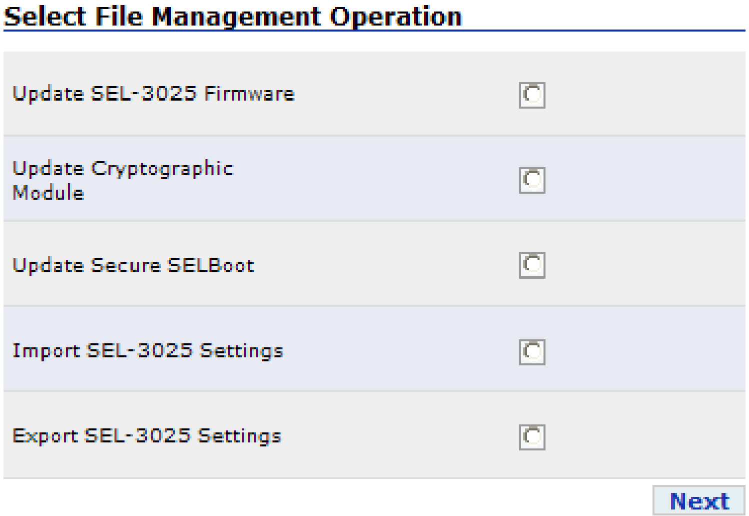
This procedure changes the secure protocol your SEL-3025 uses. It updates the firmware of the cryptographic card inside the SEL-3025, and it upgrades Secure SELBOOT and the SEL-3025 firmware. You can obtain update files for converting the SEL-3025 by contacting your SEL customer service representative.

Upgrade the Cryptographic Card

Step 1. Use an account in the Administrator group to log in to the Ethernet Management interface of the SEL-3025.

Accounts not assigned to this group cannot perform cryptographic card updates.

Step 2. Select the **File Management** link from the navigation panel. This will show the **File Management** page.



Select File Management Operation

Update SEL-3025 Firmware ○

Update Cryptographic Module ○

Update Secure SELBoot ○

Import SEL-3025 Settings ○

Export SEL-3025 Settings ○

Next

Figure B.4 File Upgrade Page

Step 3. Select the **Update Cryptographic Module** check box.

Step 4. Click the **Next** button.

Step 5. Click the **Browse** button to show a file browser window.

Step 6. Navigate to the location of the upgrade file and select it.

Step 7. Click the **Send File** button. The file download will take about a minute.

When the download is complete, your computer screen will display `Transferring file to Cryptographic Module` while the new firmware file is being loaded onto the card. This will take about two minutes.

Step 8. Wait for the card update operation to complete.

When the transfer is complete, the SEL-3025 will restart to complete the card upgrade process. During this process, the front-panel LEDs will be unlit. Do not disturb the unit until one or more front-panel LEDs illuminate, after about one minute.

Use the Serial Port to Upgrade SEL-3025 Firmware

Step 1. Remove power from your SEL-3025.

Step 2. Use an SEL-C609 or equivalent cable to connect the PC serial port to the trusted (DCE) interface.

Step 3. Set the PC terminal emulation program to 9600 bits per second, 8 bits, no parity, 1 stop bit, with no flow control.

Step 4. Enter SELBOOT mode by applying power to the SEL-3025 while pressing and holding the reset button. If you have successfully entered SELBOOT mode, the front-panel LEDs will flash alternately.

Step 5. Press **<Enter>** and verify that you receive a !> prompt. If you do not, go back to *Step 2*.

Step 6. Set the SEL-3025 data rate to 115200 bps by typing **BAUD 115200 <Enter>**.

Step 7. Change the terminal program data rate to 115200 bps, press **<Enter>** again, and verify that you receive the prompt.

Step 8. Type **REC <Enter>** at the prompt. The device will prompt you to confirm that you want to erase the existing firmware.

Step 9. Type **Y** at the prompt, press **<Enter>**, and then follow the instructions on the screen.

Step 10. Press the spacebar and then use Xmodem protocol to send the new firmware file.

Your computer screen will display two messages: `Erasing firmware` and `Erase successful`. You should then see the front-panel LEDs flash alternately.

Do not disturb the device until after your computer screen displays the message `Upload completed successfully. Attempting a restart`. and one or both front-panel LEDs illuminate.

The conversion is complete.

This page intentionally left blank

Appendix C
Importing or Exporting Settings

Introduction

The SEL-3025 Serial Shield® allows you to store settings information in a settings file. Settings files are XML files that contain device version, configuration, and settings data.

Importing Settings

Importing settings allows you to set some or all configuration settings of the SEL-3025 from a file. Perform the following steps to import a settings file into the SEL-3025.

Step 1. Navigate to the **File Management** page.

Step 2. Check **Import** SEL-3025 **Settings**

Step 3. Click **Next**.

Step 4. Type the path to the settings file, or use the **Browse** button to locate it.

Step 5. Click **Send File**.

The **File Upload** page will show the status of the import operation as the operation receives, verifies, and applies settings to your SEL-3025. Verification and application of settings occur in an order that minimizes any chance of the current device settings changing if the import operation fails. Should there be such a failure, however, certain types of errors in the cryptographic groups information can result in removal of all users except the logged-in user.

Exporting Settings

By exporting settings, you can save some of the configuration settings of the SEL-3025. You may find it handy to export your device settings to include them in a request for technical assistance.

NOTE: For security reasons, you cannot export passwords and encryption keys, and these are absent from the exported settings file. If you need keys and passwords in your settings file, you can use a text editor to edit the file and insert those values manually.

Perform the following steps to export your SEL-3025 device settings to a file.

Step 1. Navigate to the **File Management** page.

Step 2. Check **Export** SEL-3025 **Settings**.

Step 3. Click **Next**.

Step 4. Click the **Receive File** button. The XML settings file will replace the page.

Step 5. Click **Save As** from your browser to save the file. By default, the file name will be SET_ALL.XML.

Appendix D
User-Based Accounts

Introduction

Local accounts are the engineering access accounts that reside on SEL products. SEL has historically used global accounts such as ACC and 2AC and a password associated with each to control access to SEL devices. With global accounts, every user has the same login credentials (username and password), which weakens the security of the system. To strengthen authentication, authorization, and accountability, this SEL product uses a user-based account structure.

Benefits of User-Based Accounts

User-based accounts allow for a stronger security posture than global accounts. One of the drawbacks of global accounts is that when an individual's privileges are revoked, either everyone who uses that account is temporarily without access or there exists an unauthorized individual with secret knowledge that individual can use or sell for malicious purposes. User-based accounts correct this problem with the ability to disable or remove one individual's account without affecting access for anyone else.

Similarly, when password changes are required, either because of a compromised system, routine maintenance, or regulatory requirements, users will not need to remember several new and different global passwords. They will only need to remember their own personal password changes. This increases security by reducing the need to write passwords down and by reducing the chance that an unauthorized individual might obtain an active password.

Three key parts of strong access control are authentication, authorization, and accountability. Authentication is the process of verifying that users are whom they claim to be. This is very difficult to do reliably with global accounts because of the nature of shared passwords. User-based accounts allow for the reliable authentication of individual users of a system. This creates more trust that those who access the system really are whom they claim to be.

Authorization is the process of granting privileges to users of a system. You can perform authorization with global accounts when the accounts are organized into access roles, such as with ACC and 2AC. However, unless you have a large number of roles (and, therefore, a large number of shared passwords), it is difficult to assign privileges granularly to global accounts. You can use user-based accounts to assign specific privileges to users of a system.

Accountability is the idea that individual users can be held responsible for their actions on a system. The lack of authentication with global accounts creates too much opportunity to cast doubt on one's activities, making accountability difficult to enforce. The ability to clearly authenticate a user to the individual level allows all actions to be assigned to specific users. Accountability is very important to event tracking and forensic investigations.

Administration of User-Based Accounts

This product comes unconfigured from the factory. This means that there are no user accounts installed. To access the product, you must create an initial account through the commissioning page. This account is authorized to add, remove, enable, and disable system users. Only the individual who creates this account should have knowledge of this account password.

It is possible to create other accounts that are able to manage users. This device supports as many as 32 unique user accounts. Only those users with a need to manage user accounts should be a member of the User Manager or Administrator group.

The SEL-3025 stores user accounts in nonvolatile memory. This allows the device to maintain account status through power cycles and other unexpected events.

Acceptable Use Banner

Prior to logging on to this SEL product, any potential user will see a use banner. The use banner is a programmable message indicating what constitutes appropriate use of this device and potential consequences for abusing this device. The default use banner for SEL products is the same as the recommended use banner for the National Institute of Standards and Technology:

> *This system is for the use of authorized users only. Individuals using this system without authority or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such activity to law enforcement officials.*

Logging on With SEL User-Based Accounts

Upon connection to this SEL product, a user will see a use banner and a login prompt. The login prompt includes fields for entering a username and the password associated with that username. To log in to this SEL product, the user must enter a valid username and the appropriate password. Usernames are case insensitive and unique to each individual with authority to access the device. Users who enter valid usernames and matching passwords will have access to the device.

If the SEL-3025 determines a username or password to be invalid, then it rejects the access attempt and provides an alert to the user. This alert will inform the user that the login credentials were incorrect. After three failed login attempts within a one-minute period, this SEL product will disallow access attempts with the locked username for 30 seconds. Additionally, this device will pulse the alarm contact for one second to provide an alert to the control center that a failed login attempt has occurred. These security features are designed to prevent and slow down password guessing attacks. Login failure can happen for three reasons: the username was invalid, the password was incorrect, or the user's account is disabled. Please check the spelling of the username and password if an access attempt fails. If you are certain that you entered the username and password correctly, please contact your system administrator to verify that your account has not been disabled.

Passphrases

Passphrases provide a user the ability to create strong and easy-to-remember passwords that protect access to a system. A strong passphrase includes many different characters from many different character sets. Longer passphrases provide greater security than shorter passphrases. SEL user-based accounts support complex passphrases that must include at least one character from each of the following character sets.

- Uppercase letters
- Lowercase letters
- Digits
- Special characters

Additionally, passphrases must be at least eight characters in length. This SEL product supports passphrases as long as 128 characters. Spaces are allowed in passphrases.

Users with administrative access can set or change passphrases for any user of the system. Users without administrative access can only change their own passphrases. For protection of your account, this SEL product will never display, transmit, or store a passphrase in clear text.

This page intentionally left blank

Appendix E
Syslog

Introduction

The syslog protocol, as defined in RFC 3164, provides a means for a device to send system event notification messages across IP networks to remote syslog servers. Syslog is commonly used to send system logs such as security events, system events, and status messages useful in troubleshooting, auditing, and event investigations. The syslog packet size is limited to 1024 bytes and is formatted into three parts: **PRI**, **HEADER**, and **MSG**.

1. **PRI**: The priority part of a syslog packet is a number enclosed in angle brackets that represents both the facility and severity of the message. We can calculate the priority value by multiplying the facility numerical code by 8 and adding the numerical value of the severity. For example, a kernel message (facility=0) with a severity of emergency (severity=0) would have a priority of 0. Also, a “local use 4” message (facility=20) with a severity of Notice (severity=5) would have a priority value of 165. In the PRI part of the syslog message, we would place these values between the angle brackets as <0> and <165>, respectively.

The severity code (see *Table E.1*) is a number indicative of a message’s importance.

Table E.1 Syslog Message Severities

Numerical Code	Severity
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

The facility code (see *Table E.2*) defines the application group in which the message originated.

NOTE: Various operating systems have been found to use facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages that seem to be similar.

NOTE: Various operating systems have been found to use both facilities 9 and 15 for clock (cron/at) messages.

Table E.2 Syslog Message Facilities

Numerical Code	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons
4	Security/authorization messages (note 1)
5	Messages generated internally by syslogd
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon (note 2)
10	Security authorization messages (note 1)
11	FTP daemon
12	NTP subsystem
13	Log audit (note 1)
14	Log audit (note 2)
15	Clock daemon (note 2)
16	Local use 0 (local0)
17	Local use 1 (local1)
18	Local use 2 (local2)
19	Local use 3 (local 3)
20	Local use 4 (local 4)
21	Local use 5 (local5)
22	Local use 6 (local6)
23	Local use 7 (local7)

2. **HEADER**: The header of a syslog packet contains the time stamp and the source of the message. The IP address or the hostname defines the source of the message originator. Time stamps are based on the time of the originating host, so it is critical to have time synchronized across devices for the entire network to perform log analysis and event correlation accurately.
3. **MSG**: The message part of a syslog packet contains the source program that triggered the message and the human-readable body of the message.

The following is a sample syslog message. This particular message shows an invalid login attempt on July 09, 2009 at 08:17:29 to “myhostname” for user root from the IP address 192.168.1.1.   The priority of this message is 34.

<34>Jul 09 2009 08:17:29 myhostname Invalid login attempt by: root at 192.168.1.1

We can divide the syslog message into each respective part, as the following table shows.

PRI	HEADER	MSG
<34>	Jul 09 2009 08:17:29 myhostname	Invalid login attempt by: root at 192.168.1.1

Remote Syslog Servers

The SEL-3025 stores syslog messages locally, but it can also send syslog messages to remote syslog servers. The local buffers are circular in nature, so newer messages overwrite older messages after the buffer is filled. Support for multiple remote syslog servers provides the added benefits of centralized logging including larger storage capacity, centralized event analysis and correlation, and archiving of event logs. In the following figure, remote devices are configured to send syslog messages to the remote syslog server on the other end of the virtual private network (VPN) tunnel. Syslog-compatible devices can send logs to the central syslog server in this example for centralized logging, reporting, and event correlation. The syslog protocol uses User Datagram Protocol (UDP) Port 514 to send syslog messages to remote syslog servers.

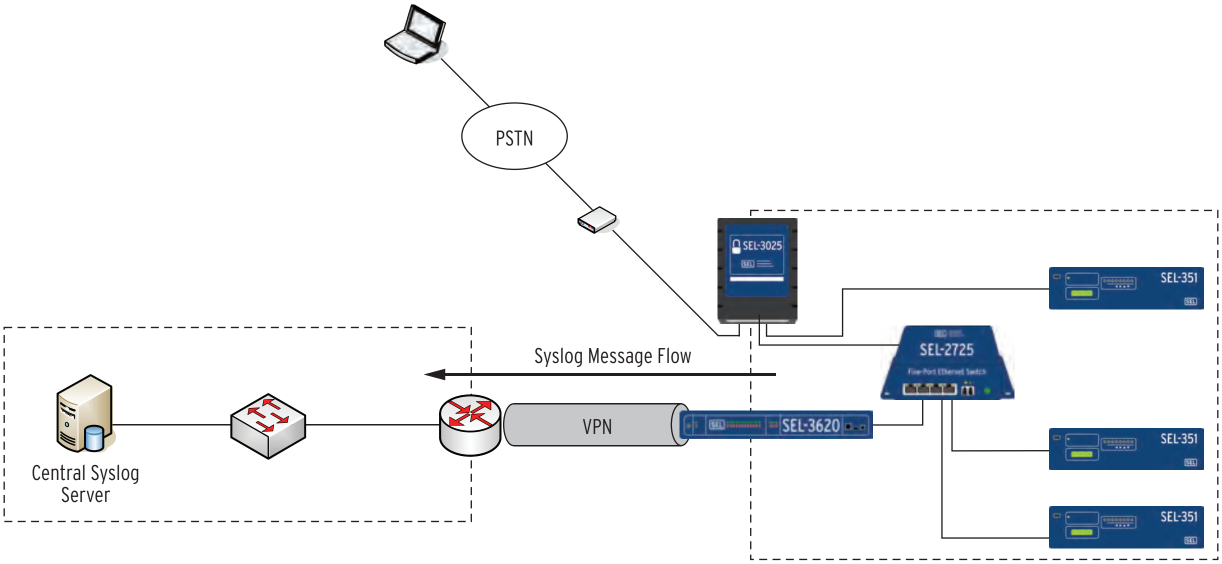


Figure E.1 Central Syslog Server

Open Source Syslog Servers

Most Linux and UNIX distributions include a native syslog server that can provide a central syslog server solution. Syslog-ng (http://balabit.com) is also an excellent solution with added functionality that you can use if you do not include it already in your distribution.   Syslog server solutions for Microsoft Windows are typically commercial or have limited features if they are available at no charge.

SEL-3025 Syslog Events

The SEL-3025 records and time-stamps all events in the Syslog Format, consistent with the syslog description from RFC 3164.

The following tables provide a listing of all the events that the SEL-3025 logs and the record that it generates with each of these events.

Log messages may contain words or phrases in brackets such as <username>. This notation indicates that the SEL-3025 will replace the word or phrase inside the brackets with a value of the field it is logging, in this case, the username of the user who performed an action.

Table E.3 System Events

Message	Tag Name	Severity	Facility
Device Power Up	Startup	Notice	Log Audit
Device Restarted	Startup	Notice	Log Audit
Device Shutting Down	Shutdown	Notice	Log Audit
Pushbutton reset has been performed	Pushbutton Reset	Notice	Log Audit

Table E.4 User Account Events

Message	Tag Name	Severity	Facility
User account <new account user name> created by <username>.	User Management	Notice	Security/ Authorization
User account <deleted account username> deleted by <username>.	User Management	Notice	Security/ Authorization
Password changed for <username> by <username2>.	User Management	Notice	Security/ Authorization
<access> user <username> group changed to <new_access> by <username2>.	User Management	Notice	Security/ Authorization
<type> user <username> changed to <new_type> by <username2>.	User Management	Notice	Security/ Authorization
User <username> enabled by <username2>.	User Management	Notice	Security/ Authorization
User <username> disabled by <username2>.	User Management	Notice	Security/ Authorization
Device commissioned with user <username>.	User Management	Notice	Security/ Authorization
Login successful for <username>.	User Management	Notice	Security/ Authorization
Logout successful for <username>.	User Management	Notice	Security/ Authorization
Session timed-out for <username>.	User Management	Notice	Security/ Authorization
Login failed.	User Management	Notice	Security/ Authorization
User <username> has been locked out due to 3 failed login attempts.	User Management	Warning	Security/ Authorization

Table E.5 Remote Management Events

Message	Tag Name	Severity	Facility
Login successful for <username>.	Remote Management	Notice	Security/ Authorization
Logout successful for <username>.	Remote Management	Notice	Security/ Authorization
Session timed-out for <username>.	Remote Management	Notice	Security/ Authorization
Login failed.	Remote Management	Notice	Security/ Authorization

Table E.6 Cryptographic Module Events

Message	Tag Name	Severity	Facility
Cryptographic Module Failure	Crypto System	Emergency	System Daemon
SSCP key exchange with <addr> (<sscp group>)	Crypto System	Notice	System Daemon
SSCP OOB <type> <action> to address <addr> (<sscp group>)	Crypto System	Informational	System Daemon
SSCP Data message rejected from address <addr> due to an <cause>	Crypto System	Notice	System Daemon
SSCP <type> rejected from address <addr> due to an <cause>	Crypto System	Notice	System Daemon
SEP key exchange with <Addr>	Crypto System	Notice	System Daemon
SEP OOB <Type> <Action> with address <Addr>	Crypto System	Informational	System Daemon
SEP IB message rejected with address <Addr> due to an <Cause>	Crypto System	Notice	System Daemon
SEP OOB message rejected with address <Addr> due to an <Cause>	Crypto System	Notice	System Daemon

Table E.7 Settings Events

Message	Tag Name	Severity	Facility
Settings (<class>) modified by <username>	Settings Management	Notice	Log Audit
Settings import initiated	Settings Management	Notice	Log Audit
Settings import successful	Settings Management	Notice	Log Audit
Settings import failed: <reason>	Settings Management	Error	Log Audit
Settings export initiated	Settings Management	Notice	Log Audit
Settings export successful	Settings Management	Notice	Log Audit
Settings export failed: Internal Error	Settings Management	Error	Log Audit
Time/date changed from <original time stamp> to <new time stamp> by <user name>	Date Time	Informational	Clock Daemon
Time adjusted from <original> to <new> to conform to Daylight Savings Time change	Date Time	Informational	Clock Daemon

Table E.8 Diagnostics

Message	Tag Name	Severity	Facility
Cryptographic Module Failure.	Diagnostics	Emergency	Kernel Messages
FPGA Failure.	Diagnostics	Emergency	Kernel Messages
RAM Failure. <location>	Diagnostics	Emergency (if shutting down). Alert (if restarting).	Kernel Messages
Code Flash Failure. Expected <expected>, Actual <actual>.	Diagnostics	Emergency	Kernel Messages
Real Time Clock Failure.	Diagnostics	Warning	Kernel Messages
Real Time Clock Battery Voltage Low.	Diagnostics	Warning	Kernel Messages
Data Flash Failure. <location>	Diagnostics	Emergency (if disabling serial data processing). Error (if serial data processing still functional).	Kernel Messages

Table E.9 Firmware Upgrade Events

Message	Tag Name	Severity	Facility
SEL-3025 Network Firmware Upgrade started by <username>.	Upgrade	Warning	Security/ Authorization
SEL-3025 Network Firmware Upgrade successful.	Upgrade	Notice	Security/ Authorization
SEL-3025 Network Firmware Upgrade failed.	Upgrade	Error	Security/ Authorization
Cryptographic Module Network Firmware Upgrade started by <username>.	Upgrade	Warning	Security/ Authorization
Cryptographic Module Network Firmware Upgrade successful	Upgrade	Notice	Security/ Authorization
Cryptographic Module Network Firmware upgrade failed	Upgrade	Error	Security/ Authorization
SEL-3025 SELBOOT key upgrade successful	Upgrade	Notice	Security/ Authorization
SEL-3025 SELBOOT key upgrade failed	Upgrade	Error	Security/ Authorization
SEL-3025 SELBOOT firmware upgrade successful	Notice	Notice	Security/ Authorization
SEL-3025 SELBOOT upgrade failed	Upgrade	Error	Security/ Authorization

Table E.10 Certificate Management

Message	Tag Name	Severity	Facility
Certificate upload error by user <username>.	Certificate Management	Notice	Security/ Authorization
Certificate uploaded by user <username>.	Certificate Management	Notice	Security/ Authorization

Table E.11 Communications

Message	Tag Name	Severity	Facility
Modem connected	Communications	Notice	Security/ Authorization
Modem disconnected	Communications	Notice	Security/ Authorization

Appendix F
Networking Fundamentals

Introduction

A telecommunications network can be as simple as two devices linked together for the purpose of information sharing or as complex as the Internet involving many devices serving a multitude of purposes. In either case, networking devices need a common model for interconnectivity across a diverse set of communications media, manufacturer equipment, protocols, and applications. The International Standards Organization (ISO) developed the Open Systems Interconnection (OSI) model to serve this purpose. The OSI model has been in use for decades as a reference model that describes the fundamental concepts and approach to interconnecting heterogeneous systems by abstracting the model into seven logical layers. This appendix provides an introduction to networking fundamentals and illustrates how device communication occurs across disparate networks.

OSI Model

The OSI model consists of seven conceptual layers, as shown in *Figure F.1*. Each layer is relatively independent of the other layers and only needs to know how to communicate with the adjacent layers. This independence has allowed manufacturers to develop implementations at their respective OSI layers and still be interoperable with implementations at completely different layers. For example, a program interfacing at the Application Layer does not need to know if the data being transmitted will traverse over an Ethernet, serial, or radio physical medium.

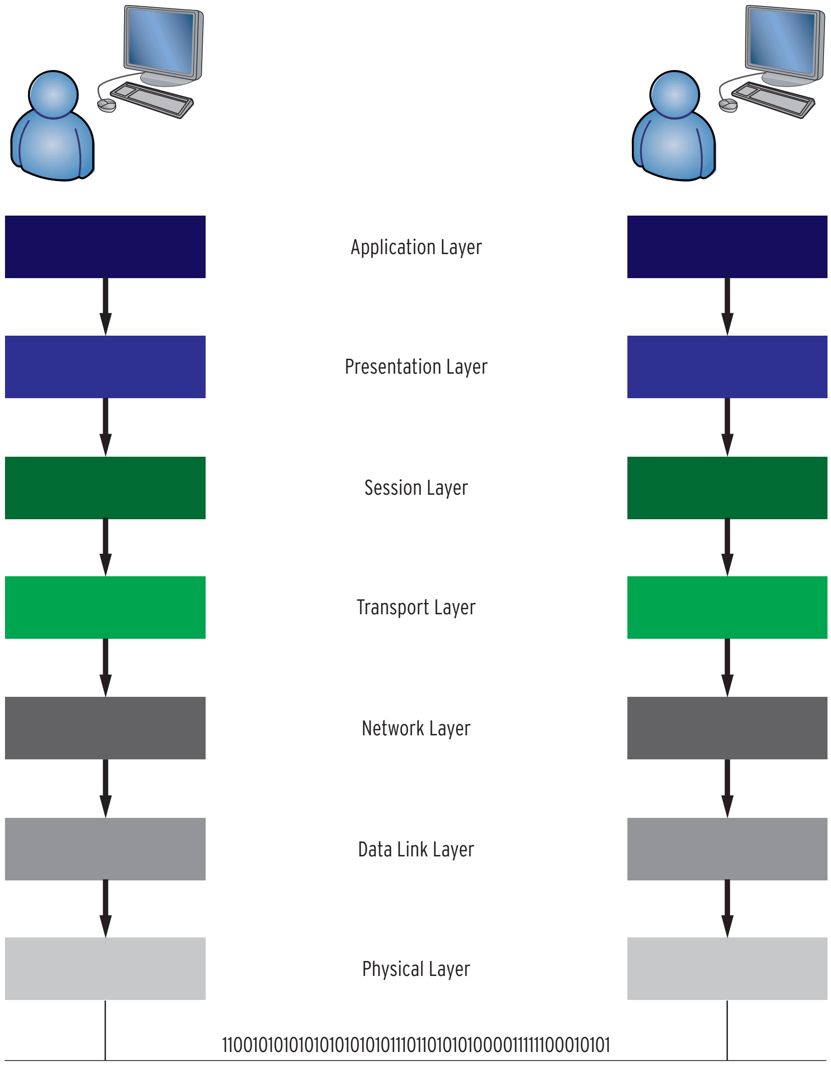


Figure F.1 OSI Model

Physical Layer (Layer 1)

The primary responsibility of the Physical Layer is transmitting data across a communications medium from one device to another. This layer defines the electrical and mechanical interfaces such as the hardware network interface cards use in interfacing with the physical medium that carries the bit stream. A Physical Layer device simply transmits or receives data and lacks any knowledge of the data that it transmits. Copper and fiber Ethernet are both examples of physical media in common use. Network hubs and repeaters are devices common to this layer.

Data Link Layer (Layer 2)

The Data Link Layer is responsible for providing reliable transit of data across physical mediums by controlling frame synchronization, flow control, error detection, and providing physical addressing. Directly connected devices (*Figure F.2*) communicate at this layer without the need for a Layer 3 device, such as a router.

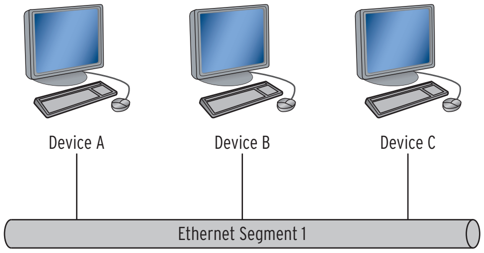


Figure F.2 Ethernet Segment

The Data Link Layer is subdivided into the Logical Link Control (LLC) and the Media Access Control (MAC) sub-layers. The LLC sub-layer manages communication among devices and handles the frame synchronization, flow control, and error checking introduced previously. The MAC sub-layer manages physical addressing at the Data Link layer. MAC addresses are physical addresses that are embedded into the hardware and determine how devices should identify each other uniquely on the same network segment. The OSI model represents MAC addresses, also known as hardware addresses, in the form of *01-23-45-67-89-ab*.

At this layer, devices organize data they receive into frames, called headers, that encapsulate the data with descriptive information. *Figure F.3* depicts an example of an Ethernet frame.

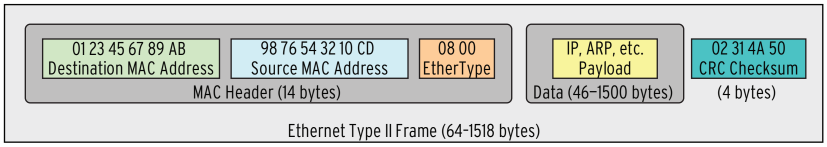


Figure F.3 Ethernet Frame

The Ethernet frame in *Figure F.3* includes the following components:

- MAC Header: Includes the source and destination MAC addresses that determine which devices are communicating on the network. Also included is the EtherType, which defines the type of Ethernet framing used.
- Data: The data field includes the payload type as well as the actual data transmitted.
- CRC Checksum: The CRC checksum provides error checking to verify that the data are received exactly as sent.

Network Layer (Layer 3)

The Network Layer is responsible for transmitting data from one device to another device that is on a separate network segment. The separate network segment could be within close proximity, such as within the same building, or in a completely different country, as seen with the Internet.

Addressing, routing, fragmentation, error handling, and congestion control are all functions of the Network Layer.

Layer 3 addressing is different from Layer 2 addressing, in that Layer 3 addresses are logical. Logical addresses are hardware independent, unlike MAC addresses that are assigned to specific hardware. The Network Layer manages mappings between these logical addresses and physical addresses. Address Resolution Protocol (ARP) performs this mapping in IP networks.

The most common Layer 3 addressing scheme is Internet Protocol (IP) addressing. IP addresses are 32-bit addresses, commonly denoted in dotted-decimal notation, that identify devices across different network segments.

Table F.1 shows an example IP address of 192.168.254.1 in dotted-decimal notation, with the equivalent 32-bit binary notation. Each 8-bit octet value is equivalent to the decimal value in the dotted-decimal notation. For example, the first binary octet of 11000000 is equivalent to 192 in the first octet of the dotted-decimal notation.

Table F.1 Sample IP Address

Dotted-Decimal Notation	192.168.254.1
32-Bit Binary Notation	11000000. 10101000. 11111110. 00000001

Routing is necessary to define the traffic's path between two networks. In *Figure F.4*, there are two IP networks, 192.168.254.0/24 and 10.10.10.0/24, with a router between the two networks. The router provides the ability for Device A, Device B, and Device C to communicate with Device D, Device E, and Device F. Without this router, these devices would not be able to communicate with each other. Device A, Device B, and Device C can all communicate among each other without the need for a router, as described in *Data Link Layer (Layer 2)*. The same is true for communication among Device D, Device E, and Device F.

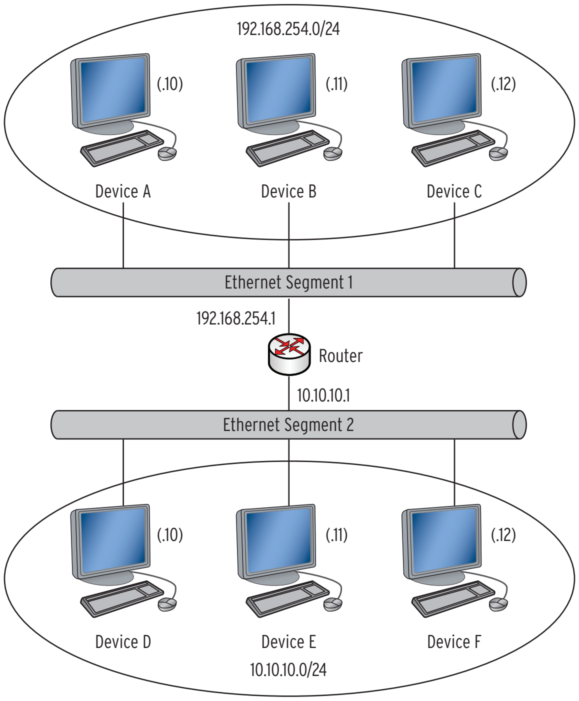


Figure F.4 Layer 3 IP Network

Transport Layer (Layer 4)

When data arrive at a network device that the Network Layer determines is the final destination, the Network Layer formats the data and passes the information to the Transport Layer. This layer is responsible for end-to-end control and ensures successful data transfer. The main Transport Layer functions are flow control and error recovery.

Flow control manages the amount of data transmitted between communicating devices so that the sending device does not send more data than the receiving device can process.

Each Transport Layer protocol handles error recovery differently, but it typically involves requesting data retransmission in the event that a device detects an error.

Transmission Control Protocol (TCP) is the Transport Layer protocol the TCP/IP suite uses to provide reliable, end-to-end communication. The suite also includes User Datagram Protocol (UDP) as a connectionless protocol, meaning that data transmission occurs with no guarantee of successful delivery.

Connection-Oriented Versus Connectionless

Connection-oriented protocols, such as TCP, establish a connection between the sending device and the receiving device prior to data transmission. These protocols make connection between two devices through a three-way handshake (*Figure F.5*). The three steps in the handshake are as follows:

1. The sending device sends a synchronization (SYN) packet to the receiving device.
2. The receiving device sends back a synchronization/acknowledgment (SYN/ACK) packet to the sending device.
3. The sending device completes the three-way handshake by sending an acknowledgment (ACK) to the receiving device.

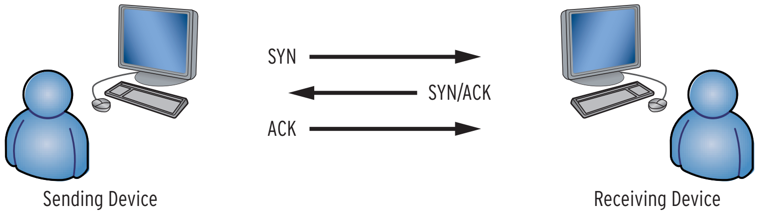


Figure F.5 TCP Three-Way Handshake

At completion of the three-way handshake, a connection is established and the two devices can begin transmitting and receiving data. The connection is maintained between the two devices throughout the session, providing a reliable connection and verification of data transmission.

In a connectionless protocol, such as UDP, there is no established connection prior to data transmission. There is also no retained connection at any point during data transmission. The protocol is connectionless, so routing information must accompany each data packet to provide information on how the data should traverse the network. Connectionless protocols provide no means for data transmission verification and are often referred to as unreliable protocols for this reason.

Session Layer (Layer 5)

The Session Layer handles session establishment, management, and termination between two end-user software application processes. This is the first layer that switches focus from the actual networking details and deals primarily with sessions consisting of service requests and responses that occur between applications installed on communicating devices.

Presentation Layer (Layer 6)

The Presentation Layer provides for standard data presentation so that applications can exchange data in a meaningful manner across a network. The sending device converts data into a standard format for transmission on the network. The receiving device converts the data sent in this standard format to a format recognizable by the receiving device’s application. This processing occurs transparently to ensure that the receiving device can read the data from the sending device.

Application Layer (Layer 7)

The Application Layer is the layer closest to the end user of a system. Software applications provide a means for end users to interface with a device to transmit and receive data. The Application Layer provides the interface between the end user and software applications that a system uses to process data over the network. Application Layer protocols define rules for communicating with network applications in a standardized format.

Appendix G

Classless Inter-Domain Routing (CIDR)

CIDR was developed as a method to help alleviate the exhaustion of IPv4 addresses available on the Internet and also to reduce and simplify global routing tables across Internet routers.

CIDR is an addressing scheme that allows for better use of IP addresses that traditionally fell into the old Class A, B, and C address schemes. In the traditional address scheme, Class A, B, and C addresses were categorized with 8, 16, and 24 bits, respectively, for the subnet mask. The smallest block of IP addresses in this addressing scheme is 254. This led to unused and wasted addresses in scenarios where someone needed 10 IP addresses but had to purchase the entire Class C block of 254 usable addresses. In situations where someone needed more than 254 addresses, they either had to purchase another Class C block or jump to a Class B or Class A network. The jump from Class C (254 usable addresses) to Class B (65,534 usable addresses) to Class A (16,777,214 usable addresses) provided no middle ground for IP addressing.

The solution was to allow network bits other than 8, 16, and 24, which resulted in providing that middle ground in the addressing scheme. For example, someone who needed only 10 IP addresses could be given a block of 14 usable IP addresses through the use of 28 network bits instead of 24 in the subnet mask.

CIDR allows blocks of contiguous addresses to be combined through route aggregation to create a larger classless set of IP addresses. It is then possible to summarize these aggregated routes into routing tables, resulting in fewer route advertisements.

In the following example, we would need to advertise a route for each classful network.

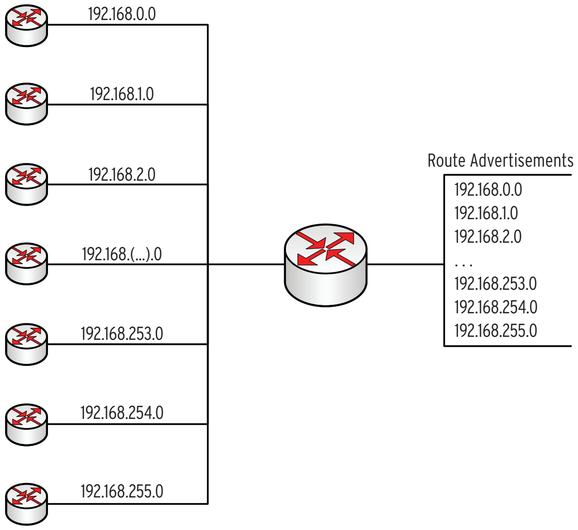


Figure G.1 Classful Route Advertisements

By using CIDR notation, we can use route aggregation to combine multiple routes, as seen below. High-level route entries can represent many lower-level routes in the global routing table, simplifying routing and management of route tables.

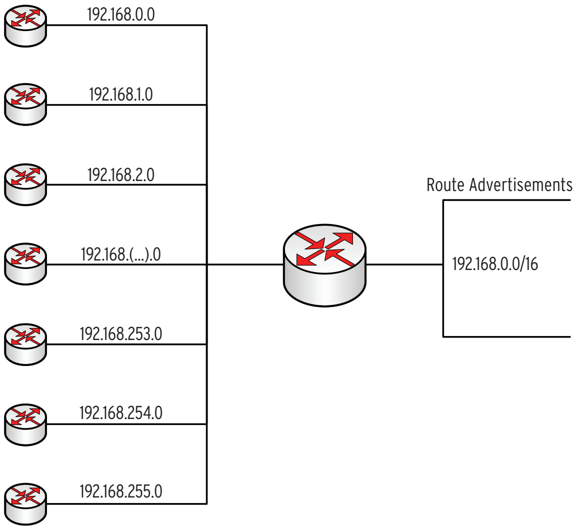


Figure G.2 CIDR Route Advertisements

CIDR has carried over to use in private network RFC 1918 addresses, through the use of CIDR notation when defining the subnet mask and in simplifying internal routing tables. CIDR notation uses the format where the network ID and associated subnet mask are listed as xxx.xxx.xxx.xxx/n. The value *n* is the number of leftmost bits set to a value of "1" in the mask. A traditional classful depiction of a network ID and subnet mask would be as follows:

- Network ID: 192.168.1.0
- Subnet Mask: 255.255.255.0 (dotted decimal notation)

To take the above example and convert it to CIDR notation, you would need to count the number of leftmost bits set to a value of "1" in the binary notation of the subnet mask. The binary notation of the subnet mask of 255.255.255.0 would be 11111111 11111111 11111111 00000000. There are 24 bits set to a value of "1", so *n* would equal 24. The CIDR notation would be 192.168.1.0/24. The table below provides additional information about CIDR and the equivalent dotted decimal notation.

Table G.1 CIDR to Dotted Decimal Mapping (Sheet 1 of 2)

Subnet Mask (CIDR)	Subnet Mask (Dotted Decimal)	# of bits for Network ID	# of bits for Host ID	# of Hosts per Network
/1	128.0.0.0	1	31	2,147,483,646
/2	192.0.0.0	2	30	1,073,741,822
/3	224.0.0.0	3	29	536,870,910
/4	240.0.0.0	4	28	268,435,454
/5	248.0.0.0	5	27	134,217,726
/6	252.0.0.0	6	26	67,108,862
/7	254.0.0.0	7	25	33,554,430
/8	255.0.0.0	8	24	16,777,214
/9	255.128.0.0	9	23	8,388,606

Table G.1 CIDR to Dotted Decimal Mapping (Sheet 2 of 2)

Subnet Mask (CIDR)	Subnet Mask (Dotted Decimal)	# of bits for Network ID	# of bits for Host ID	# of Hosts per Network
/10	255.192.0.0	10	22	4,194,302
/11	255.224.0.0	11	21	2,097,150
/12	255.240.0.0	12	20	1,048,574
/13	255.248.0.0	13	19	524,286
/14	255.252.0.0	14	18	262,142
/15	255.254.0.0	15	17	131,070
/16	255.255.0.0	16	16	65,534
/17	255.255.128.0	17	15	32,766
/18	255.255.192.0	18	14	16,382
/19	255.255.224.0	19	13	8,190
/20	255.255.240.0	20	12	4,094
/21	255.255.248.0	21	11	2,046
/22	255.255.252.0	22	10	1,022
/23	255.255.254.0	23	9	510
/24	255.255.255.0	24	8	254
/25	255.255.255.128	25	7	126
/26	255.255.255.192	26	6	62
/27	255.255.255.224	27	5	30
/28	255.255.255.240	28	4	14
/29	255.255.255.248	29	3	6
/30	255.255.255.252	30	2	2

This page intentionally left blank

Appendix H
X.509

Introduction

In cryptography, X.509 is an International Telecommunication Union standard for public key infrastructure (PKI). X.509 specifies formats for public key certificates and validation paths for authentication. The SEL-3025 uses X.509 certificates in the web server for secure device management, and for IPsec authentication.

Public Key Cryptography

Public key cryptography is distinguished by the use of asymmetric keys instead of the more traditional symmetric keys. Asymmetric keys are mathematically related so that whatever one key encrypts, the other key must be used to decrypt. There is no way to derive one key from knowledge of its paired key. These key pairs are known as public and private keys. The private key must be kept secret, while the public key can be distributed freely. This allows for many methods of protecting and authorizing messages that are not possible with symmetric key cryptography.

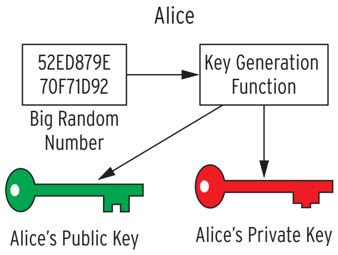


Figure H.1 Asymmetric Keys

Symmetric key cryptography, which has been used in various forms for thousands of years, uses a single key that both encrypts and decrypts the message. This key must be shared between the sender and receiver in advance. If the key cannot be shared securely, the confidentiality of any transmission encrypted with that key cannot be known.

In public key cryptography, the encryption key is not the same as the decryption key. If a message is encrypted with the publicly known key, only the private key can be used to decrypt it. This private key is known only to the owner of the key pair. Only the sender and the intended receiver will know the message, ensuring confidentiality.

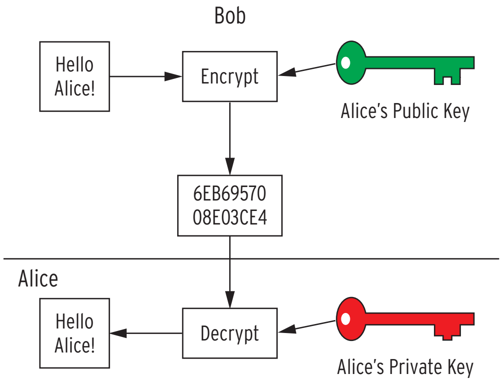


Figure H.2 Confidentiality With Asymmetric Keys

Public key cryptography is much more computation intensive than symmetric key cryptography. This makes it infeasible to send large amounts of data, or secure a series of transmissions, using this technology. Public key cryptography offers confidentiality and the corresponding ability to exchange symmetric keys securely and confidentially. This is known as hybrid cryptography and is one way that IPsec uses public key cryptography.

You can also use public key cryptography for authentication. Do this by using a private key, rather than the public key, as the encryption key. The public key you use to decrypt the message will identify the sender. This is known as an electronic signature.

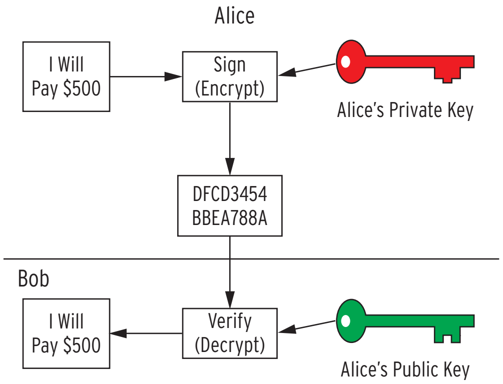


Figure H.3 Authentication With Asymmetric Keys

X.509 Certificates

Digital certificates, also known as public key certificates, provide a formal method for tracking pairs of asymmetric keys and their owners. You can use these electronic documents, through the use of digital signatures, to bind public keys to their owners. You would use digital certificates primarily in three different ways involving public key infrastructure, web of trust, and simple public key infrastructure. The certificate issuer distinguishes these three methods.

Digital Signatures

A digital signature is a more formal method of authentication than an electronic signature. They can be compared to the wax seals that were placed on envelopes before email was available. To create a digital signature, you would first compute a hash of the certificate and then encrypt that hash with the issuer's private key. You would then attach this signature to the certificate. To verify the authenticity of the certificate, the system first separates certificate and signature. The system computes a hash of the certificate and then uses the issuer's public key to decrypt the signature. We compare these two results and, if they match, we know the certificate is authentic.

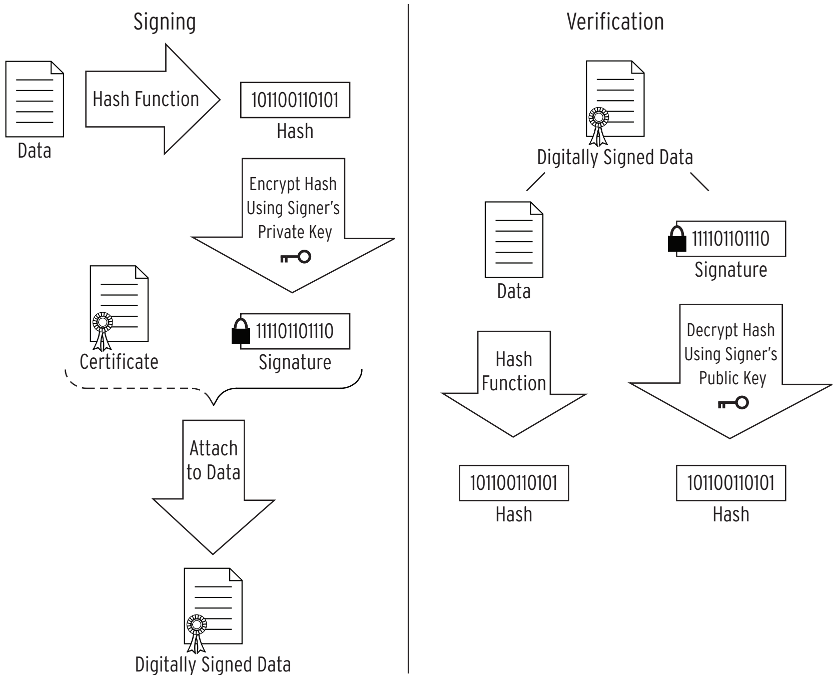


Figure H.4 Digital Signatures

Public Key Infrastructure

One of three common uses for digital certificates is in a public key infrastructure (PKI). PKI is a formal, hierarchical system where a digital certificate contains the signature of a more trusted certificate. At the top of the PKI hierarchy is the most trusted certificate, the root certificate. This certificate is self-signed, highly protected, and should only be used to sign CA certificates. If the root certificate is compromised, we must assume all certificates below it to be compromised as well.

A certificate authority (CA) is an entity that issues, or signs, other certificates. To obtain a certificate, an entity will generate a key pair, and send the public key and credentials to a CA. The CA will verify the authenticity of the credentials and issue the certificate containing those credentials, the public key, and the CA's digital signature. A CA is responsible for saying "yes" these people are whom they claim to be. CAs are authenticated by other CAs or by the root certificate.

Be aware that an attacker can subvert this process. This happens when an attacker requests a certificate and provides valid credentials for the victim. The CA, thinking everything is good, issues a certificate in the victim's name to the attacker. Take care in communicating with the CA to ensure that this will not happen.

Web of Trust

Another of the three common uses of digital certificates is in the web of trust. This is a less formal method of authentication than PKI provides, but is still in common use. The largest use of the web of trust model is in Pretty Good Privacy (PGP) used for email security. This model is very similar to PKI in that a trusted third party is verifying the authenticity of a certificate. The difference is that this trusted third party is not a CA, but rather a person who endorses the authenticity of another person. Signing the public key of the person requiring endorsement (or trust) with the endorser's (trusted entity) own private key establishes a web of trust. *Figure H.1* below illustrates a simple example of a web of trust. If Alice trusts Bob, and Bob trusts Charlie, then Alice implicitly trusts Charlie.

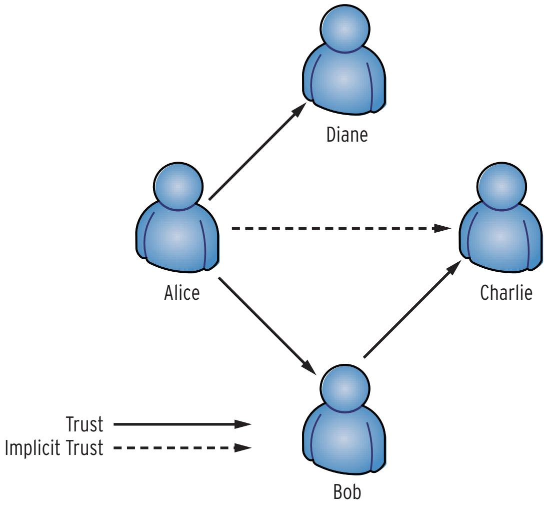


Figure H.5 Web of Trust

Simple Public Key Infrastructure

The third common use of digital certificates is in the simple public key infrastructure (SPKI). This model evolved from the need to limit the complexity inherent in PKI and the web of trust. There is no trusted third party in SPKI, because the owner and issuer of the certificate are the same entity. For SPKI to be secure, certificates must be pre-shared among all entities who communicate on that system. This ensures that all knowledge for security decisions resides locally.

Online Certificate Status Protocol (OCSP)

In consideration of the case where an authentic certificate has been stolen, there are methods to revoke certificates. One method is the certificate revocation list (CRL). The CRL method has a few problems that allow a revoked certificate to still be used. This arises from the lag associated with producing CRLs. Also, a certificate will be accepted by default, even if revoked, if the CRL is not accessible.

The online certificate status protocol (OCSP) was created to fix some of these problems. OCSP requires less bandwidth than CRLs and enables near real-time status checks to verify a certificate's status. OCSP also allows a certificate to be denied by default if the OCSP server is not accessible.

OCSP is a request/response protocol that provides real-time revocation status information for X.509 certificates. When an OCSP-enabled certificate is presented to an application, such as a web browser, the browser uses OCSP to check the certificate and ensure it is valid before proceeding with the session. OCSP uses the following response indicators to help determine certificate revocation status:

- Good: Indicates that the certificate is valid and has not been revoked
- Revoked: Indicates that the certificate has been revoked
- Unknown: Indicates that the responder does not know about the certificate being requested

The system performs a real-time revocation check for each certificate so that if a certificate is compromised or for some other reason requires revocation, it will no longer appear as valid.

Sample X.509 Certificate

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                  OU=Certification Services Division,
                  CN=Thawte Server CA/Email=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After: Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
```

```
Signature Algorithm: md5WithRSAEncryption
    07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
    a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
    3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
    4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
    8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
    e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
    b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
    70:47
```

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com