SPECTRUM®

Security Policy Statement

r9.0

CA Product References

This document references SPECTRUM®.

Contents

Chapter 1: Overview

Overview

The SPECTRUM Security Policy Statement applies to the SPECTRUM product and is applicable as long as the product is used within the documented procedures defined in the product documentation.

The SPECTRUM Security Policy Statement details the encryption and hashing that is used by specific SPECTRUM components.

The SPECTRUM Security Policy Statement communicates the FIPS 140-2 statement for the SPECTRUM product. Specifically, it does the following:

- Clearly states what SPECTRUM modules are FIPS-compliant and which are FIPS-compatible
- Identifies FIPS certificate numbers for the encryption modules or hash algorithms used
- Communicates additional items that require extra physical security or protection
- Identifies the application boundaries surrounding the different application modules using encryption and or hashing
- Identifies what data is protected
- Communicates how keys are protected
- Explains how to enable FIPS mode on the software component

Definitions

The following terms are used in the SPECTRUM Security Policy Statement:

FIPS-compliant means that the component is capable of running FIPS-compliant encryption and hashing modules and offers the ability to run in FIPS mode.

FIPS-compatible means that the component uses FIPS-certified algorithms for encryption and hashing, but does not offer the ability to run in FIPS mode.

FIPS 140-2 Compatibility Matrix

The following table shows the extent to which SPECTRUM uses FIPS-compliant algorithms:

SPECTRUM Software Component	Module	Version	Certificate[1]	Algorithms[2]	Algorithm Cert#[3]	Mode[4]
SpectroSERVER User Password Storage	BSAFE Crypto-J	3.53	714	SHA-1	356	Compatible
OneClick User Password Storage	BSAFE Crypto-J	3.53	714	AES	271	Compatible
Integration Password Storage	BSAFE Crypto-J	3.53	714	AES	271	Compatible
eHealth Password Storage	BSAFE Crypto-J	3.53	714	AES	271	Compatible
SRG Password Storage*	BSAFE Crypto-J	3.53	714	AES	271	Compatible
EEM Single Sign-On (Proxy Password)	BSAFE Crypto-J	3.53	714	AES	271	Compatible
CA Service Desk Password Storage	BSAFE Crypto-J	3.53	714	AES	271	Compatible
MySQL Password Storage	BSAFE Crypto-J	3.53	714	AES	271	Compatible
SRAdmin Data Transmission	BSAFE Crypto-C ME	2.0	608	3DES	378	Compatible

[1] NIST certificate numbers can be found at http://csrc.nist.gov/groups/STM/cmvp/validation.html

[2] These are the only algorithms supported by the software. More information can be found at http://csrc.nist.gov/groups/STM/cavp/validation.html

[3] Algorithm certificate numbers can be verified by looking up the certificate number at NIST, opening the Security Policy, or reading the 'Level/Description' column associated with the Certificate number.

[4] 'No' means the software does not offer the ability to operate in FIPS mode. 'Yes' means the software is capable of operating in FIPS mode.

SPECTRUM Software Component	Module	Version	Certificate[1]	Algorithms[2]	Algorithm Cert#[3]	Mode[4]
SNMPv3 Privacy Data Transmission	CA OpenSSL	0.9.8		3DES, AES, SHA-1		Compatible
Secure Domain Manager**	BSAFE Crypto-C ME	2.0	608	3DES, SHA-1	378	Compliant
Secure Domain Manager	OpenSSL	0.9.8		3DES, SHA-1		Compatible
SDConnector Data Transmission	BSAFE Crypto-C ME	2.0	608	3DES	378	Compatible
Certgen	OpenSSL	0.9.8		3DES, SHA-1		Compatible

Notes:

* The SRG password storage encryption is optional (FIPSencrypt). You do not have to use AES. The default is DES when using the Crypt perl module.

** You can configure a different algorithm for SDM and the SDM Connector. You do not have to use 3DES.

Chapter 2: Detailed SPECTRUM Component Descriptions

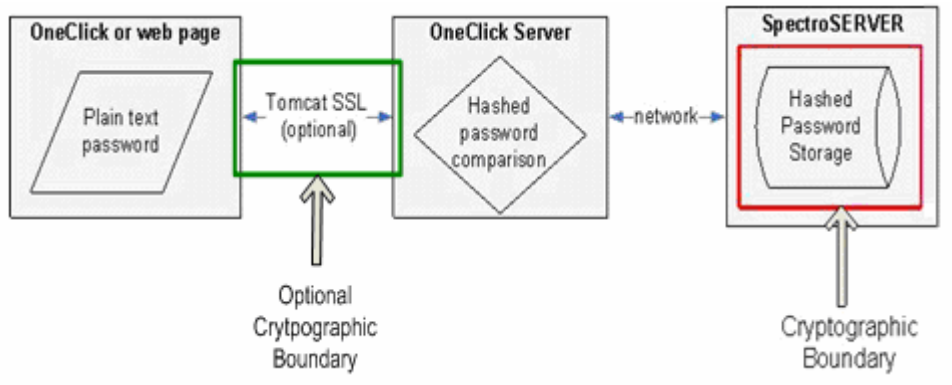
This chapter describes the encryption and hashing that is used by specific SPECTRUM components.

SpectroSERVER User Password Storage

SPECTRUM passwords are hashed with SHA-1 and are stored in the SpectroSERVER database for comparison when a user attempts to log in.

Note: Tomcat Secure Sockets Layer (SSL) should be enabled for protection over the wire.

The Cryptographic Boundary for SpectroSERVER user password storage is as follows:



The SPECTRUM password is protected.

Note: For more information about configuring and using SSL, see the *OneClick Administration Guide (5166)*.

Special Protection and Key Storage

The encryption key is internal to SPECTRUM.

Enable FIPS Mode

SHA-1 password hashing is enabled out of the box.

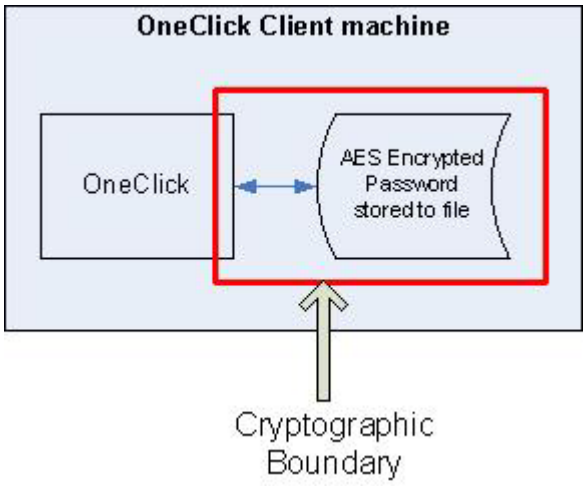
Changing Root Certificate

Not applicable at this time.

OneClick User Password Storage

OneClick passwords are stored to a file if the "Remember my password" option is selected in the SPECTRUM OneClick Login dialog.

The Cryptographic Boundary for OneClick password storage is as follows:



The OneClick username and password is encrypted with AES in the file.

Note: For more information about the OneClick login, see the *OneClick Console User Guide (5130)*.

Special Protection and Key Storage

The encryption key is internal to SPECTRUM.

Enable FIPS Mode

AES password and username encryption is enabled out of the box.

Changing Root Certificate

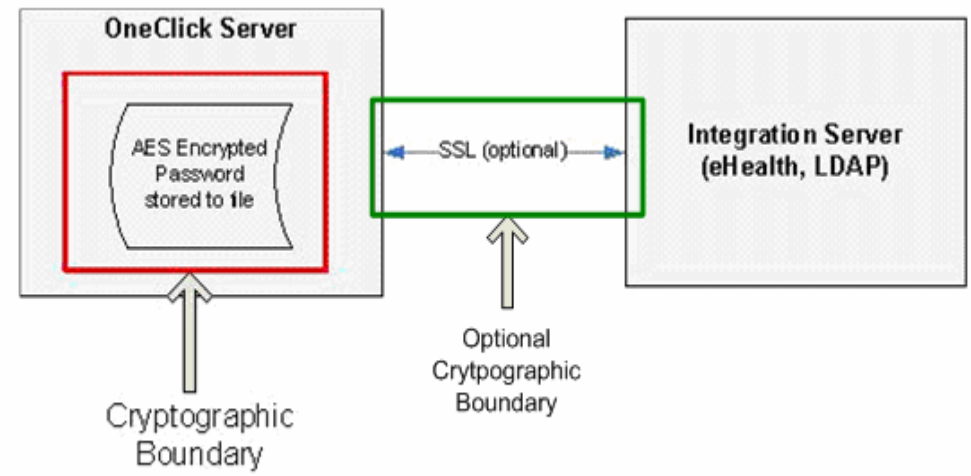
Not applicable at this time.

Integration Password Storage

Passwords for OneClick integrations are stored to a file and are encrypted using AES.

Note: For encryption over the network, SSL should be enabled for integrations between SPECTRUM and eHealth, and SPECTRUM and Lightweight Directory Access Protocol (LDAP).

The Cryptographic Boundary for integration password storage is as follows:



The password is encrypted with AES in the file.

Note: For more information about configuring and using eHealth, see the *eHealth SPECTRUM Integration Guide (5177)*. For more information about configuring and using LDAP, see the *OneClick Administration Guide (5166)*.

Special Protection and Key Storage

The encryption key is internal to SPECTRUM.

Enable FIPS Mode

AES password encryption is enabled out of the box.

Changing Root Certificate

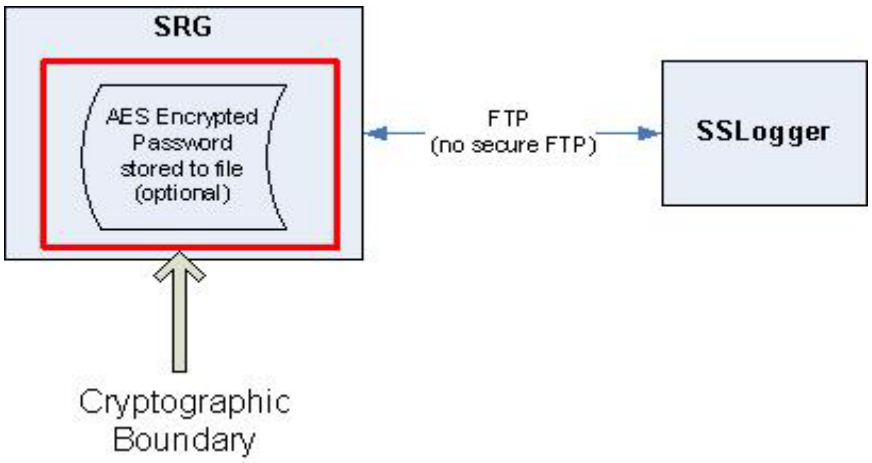
Not applicable at this time.

SRG Password Storage

You can AES-encrypt the FTP password in a file and use that password to connect to the SSLogger machine, using FTP.

Note: Secure FTP is not supported.

The Cryptographic Boundary for SRG password storage is as follows:



The password is encrypted with AES in the file.

Note: For more information about configuring and using Report Gateway, see the *Report Gateway User Guide (5141)*.

Special Protection and Key Storage

The encryption key is internal to SPECTRUM.

Enable FIPS Mode

The command line option to the SRG*.exe commands, FIPSencrypt, encrypts the password with FIPS-compliant methods, using AES.

Changing Root Certificate

Not applicable at this time.

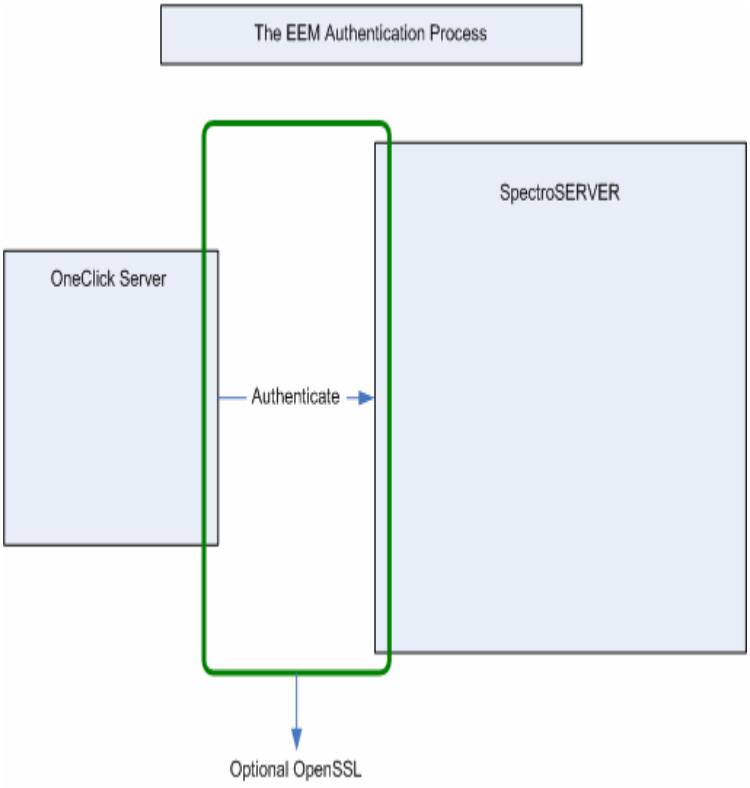
Embedded Entitlements Manager (EEM) Single Sign-On (Proxy Password)

Single Sign-On functions are used mainly for logging in, but can also be used to access cross-platform resources, such as eHealth reports.

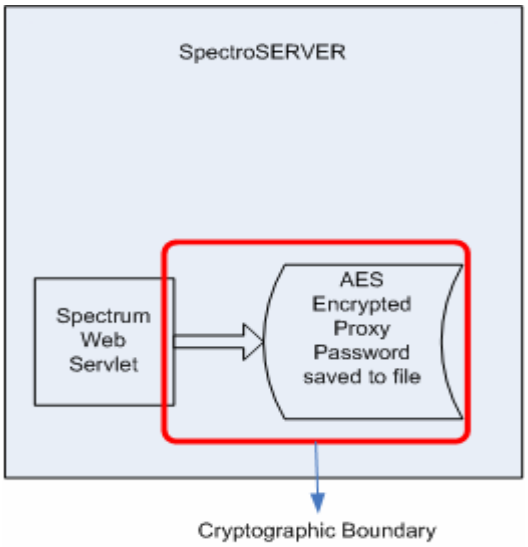
Note: If the token expires and a resource requires authentication, the authentication process repeats.

The following figures illustrate the Cryptographic Boundary for Embedded Entitlements Manager (EEM) single sign-on (proxy password).

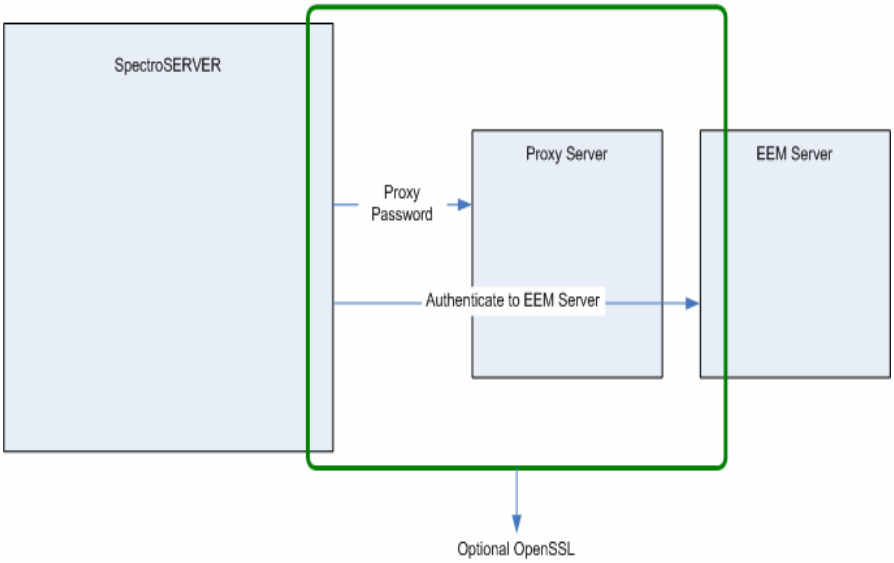
The following figure illustrates how the OneClick Server communicates with the SpectroSERVER to authenticate which OneClick Server transmissions can be encrypted with OpenSSL:



The following figure illustrates how the SpectroSERVER uses a configuration file to determine the authenticator. In this instance, the authenticator is configured to be Single Sign On through an EEM server, behind a proxy server. The password for the proxy server is AES-encrypted and is stored on the SpectroSERVER in a file.



The following figure illustrates how the proxy password is transmitted to the proxy server, which then allows the SpectroSERVER to communicate to the EEM server for authentication. These transmissions can also be encrypted with OpenSSL:



The proxy password is encrypted with AES in the file. The transmission of the data between servers can protected by SSL, but is not required.

Note: For more information about the EEM login and configuration information, see the *SPECTRUM/Embedded Entitlements Manager Integration Guide (5190)*. For more information about configuring the SSL, see the *OneClick Administration Guide (5166)*.

Special Protection and Key Storage

There is no special protection for the file; however, the key is internal to SPECTRUM.

Enable FIPS Mode

AES password encryption is enabled out of the box. It cannot be turned off. SSL is optional, and can be turned off.

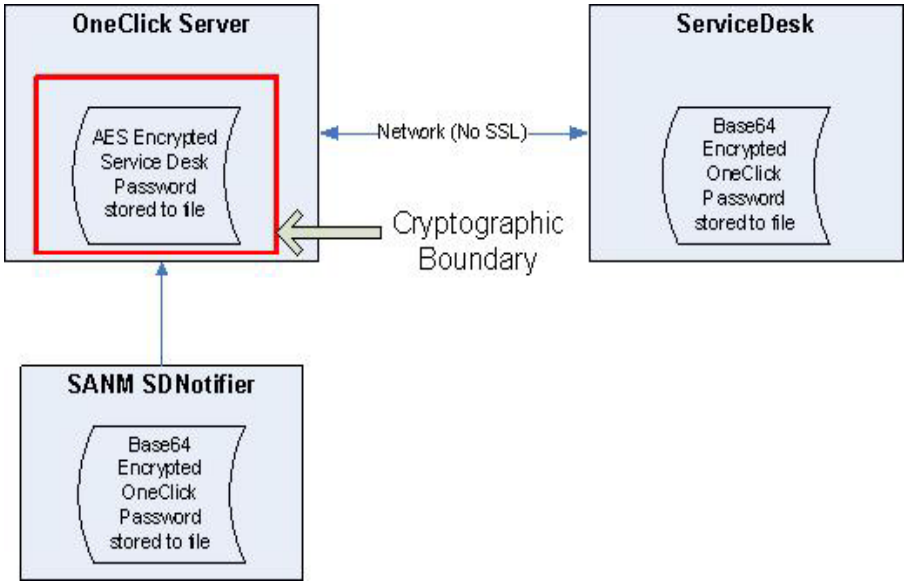
Changing Root Certificate

Not applicable at this time.

CA Service Desk Password Storage

The Service Desk password is stored to a file with AES encryption. The OneClick password is stored to a file with Base64 encryption.

The Cryptographic Boundary for CA Service Desk password storage is as follows:



Note: For more information about integrating with CA Service Desk, see the *SPECTRUM and CA Service Desk Integration Guide (5178)*.

Special Protection and Key Storage

The encryption key is internal to SPECTRUM.

Enable FIPS Mode

AES and Base64 password encryption is enabled out of the box.

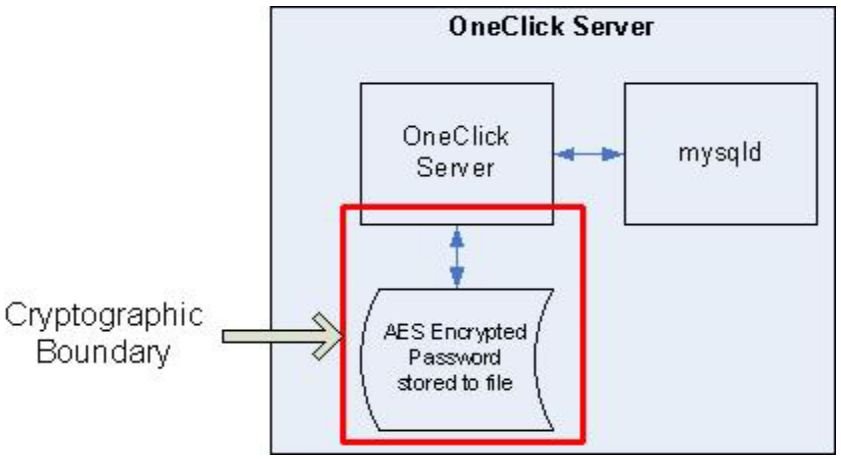
Changing Root Certificate

Not applicable at this time.

MySQL Password Storage

The mysql password is stored to a file with AES encryption.

The Cryptographic Boundary for MySQL password storage is as follows:



Note: For more information about configuring and using MySQL, see the *OneClick Administration Guide (5166)*.

Special Protection and Key Storage

The encryption key is internal to SPECTRUM.

Enable FIPS Mode

AES password encryption is enabled out of the box.

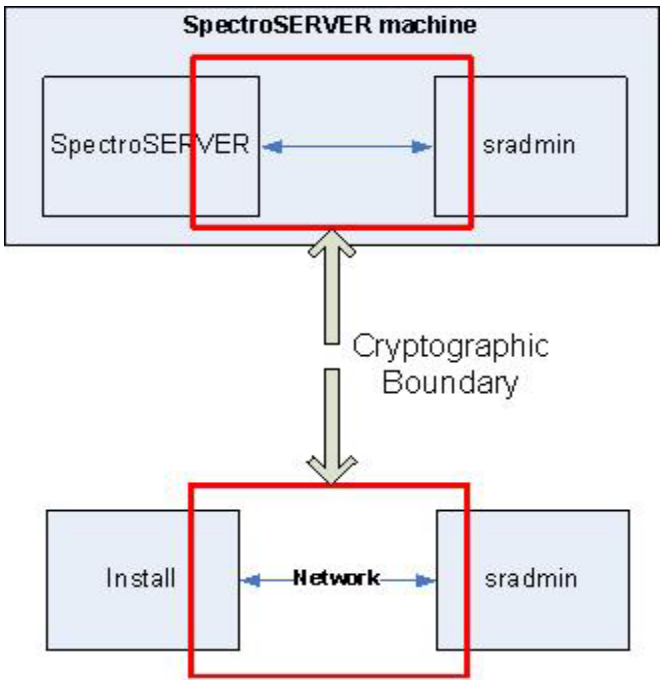
Changing Root Certificate

Not applicable at this time.

SRAdmin Data Transmission

The username and password for SPECTRUM Remote Administration (SRAdmin) is encrypted using 3DES.

The Cryptographic Boundary for SRAdmin data transmission is as follows:



The sradmin username and password are encrypted with 3DES and are sent over the network.

Note: For more information about configuring and using SRAdmin, see the *Installation Guide (5136)*.

Special Protection and Key Storage

The encryption key is internal to SPECTRUM and is also based off the time of the system.

Enable FIPS Mode

3DES username and password encryption is enabled out of the box.

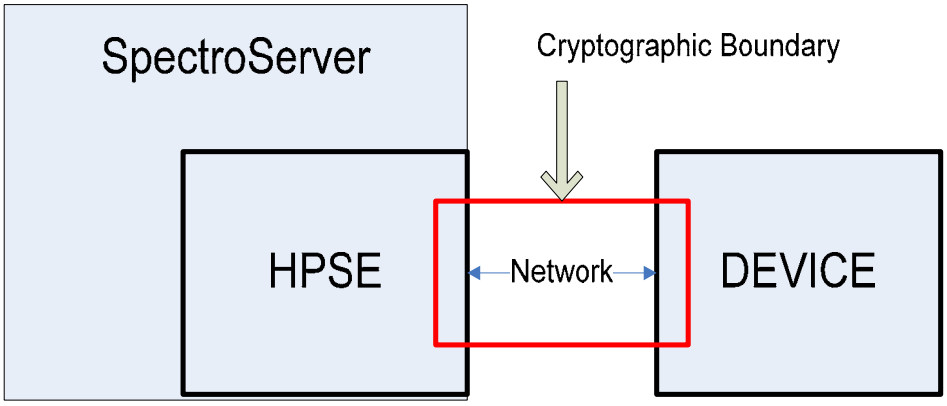
Changing Root Certificate

Not applicable at this time.

SNMPv3 Privacy Data Transmission

To query devices using SNMPv3 with authentication and privacy, SPECTRUM can be configured so that the SNMPv3 messages are encrypted using 3DES or AES. SPECTRUM can also be configured to use SHA-1 for authentication when querying devices using SNMPv3 with only authentication or authentication with privacy.

The Cryptographic Boundary for SNMPv3 privacy data transmission is as follows:



The SNMPv3 messages are encrypted using either 3DES or AES and are sent over the network.

Note: For more information about configuring and using SNMPv3, see the *Modeling Your IT Infrastructure Administrator Guide (5167).*

Special Protection and Key Storage

The encryption key is internal to SPECTRUM.

Enable FIPS Mode

SNMPv3 does not support FIPS mode, but SNMPv3 supports FIPS-compliant algorithms.

To change the default privacy encryption algorithm for all device models to 3DES or AES, the snmpv3_default_priv_protocol parameter in the *<$SPECROOT>*\SS\.vnmrc file must be set to 3DES or AES.

For example:

```
snmpv3_default_priv_protocol=3des
```

or

```
snmpv3_default_priv_protocol=aes
```

Alternatively, to override the default privacy encryption algorithm for a particular device model, the encryption algorithm should be appended to the community string for that device model.

For example:

```
#v3/<authPW>:3DES^<privPW>/<user>
```

To change the default authentication algorithm for all device models to SHA-1, the snmpv3_default_auth_protocol parameter in the <*SPECROOT*>\SS\.vnmrc file must be set to SHA.

For example:

```
snmpv3_default_auth_protocol=sha
```

Alternatively, to override the default authentication algorithm for a particular device model that uses authentication only, the authentication algorithm should be appended to the community string in the following format:

For example:

```
#v3/SHA^<authPW>/<user>
```

To override the default authentication algorithm for a particular device model that uses authentication with privacy, the authentication algorithm should be appended to the community string in the following format:

```
#v3/SHA^<authPW>:<privPW>/<user>
```

Note: For more information, see the *Modeling Your IT Infrastructure Administrator Guide (5167)*.

Changing Root Certificate

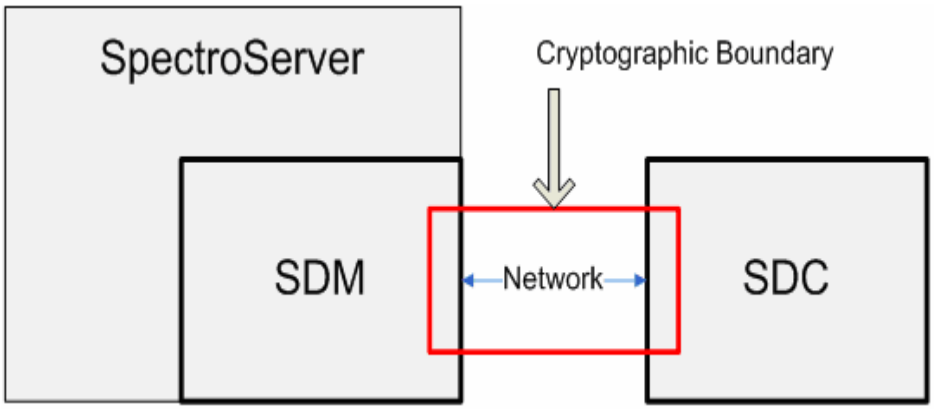
Not applicable at this time.

Secure Domain Manager

Bi-directional communication takes place between the Secure Domain Manager (SDM) and the Secure Domain Connector (SDC).

Note: When not running in FIPS mode, SPECTRUM, using SDM and SDC, runs in a FIPS-compatible state. See the FIPS 140-2 Compatibility Matrix for optional encryption algorithms.

The Cryptographic Boundary for the Secure Domain Manager is as follows:



SNMP or ICMP requests and replies, as well as SNMP traps communication are protected. No other communication takes place.

Note: For more information about configuring and using the Secure Domain Manager, see the *Secure Domain Manager User Guide (5171)*.

Special Protection and Key Storage

The SDM private key is located at <*$SPECROOT*>/SDM/CERTS/SDMCAKey.pem. The private key requires administrator read and write privileges only.

Enable FIPS Mode

Locate the sdm.config file and add the –withfips option.

Note: Any time this option is changed, the entire system needs to be restarted.

Changing Root Certificate

Run the following command to create a new network security certificate for the SDManager:

```
CertGen.exe –t cert –c <Country Code>
```

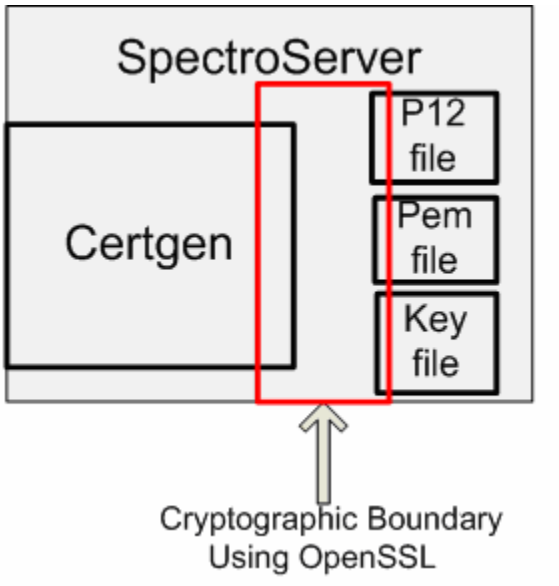
For added security, use the -p option to generate the certificate with a password as follows:

```
CertGen.exe –t cert –p <password> -c <Country Code>
```

Certgen

Certgen uses openSSL 0.9.8 to create certificate authorities, key files, and security certificates used to encrypt communications between SDM and SDC. The algorithm used to create the certificate is 3DES.

The Cryptographic Boundary for Certgen is as follows:



The p12 certificate is used primarily to protect the data being transferred between the Secure Domain Manager and the Secure Domain Connectors.

Note: For more information about configuring and using the CertGen, see the *Secure Domain Manager User Guide (5171)*.

Special Protection and Key Storage

All certificate authority, private keys, and certificates are located at <*$SPECROOT*>/SDM/CERTS. All files require administrator read and write privileges.

Enable FIPS Mode

No FIPS mode required.

Changing Root Certificate

Run the following command to create a new network security certificate for the SDManager:

```
CertGen.exe –t cert –c <Country Code>
```

For added security, use the -p option to generate the certificate with a password as follows:

```
CertGen.exe –t cert –p <password> -c <Country Code>
```