These technical notes provide instructions for deploying Data at Rest Encryption with Enterprise Key Manager. Topics include:

- Executive summary ................................................................. 2
- Audience ...................................................................................... 3
- Terminology .................................................................................. 4
- Overview ........................................................................................ 6
- Configuring the D@RE environment ........................................ 8
- Service procedures .......................................................................... 10
- Conclusion ....................................................................................... 22
- References ...................................................................................... 23
- Appendix A: Configuring the DPM .............................................. 24
- Appendix B: Planning a PKI credentials strategy ................. 30
- Appendix C: PKI credentials on the service processor .......... 37
Executive summary

Securing sensitive data is one of the greatest challenges faced by many enterprises. Increasing regulatory and legislative demands and the constantly changing threat landscape have brought data security to the forefront of IT issues. Several of the most important data security threats are related to protection of the storage environment. Drive loss and theft are primary risk factors. EMC® Symmetrix® Data at Rest Encryption (D@RE) protects data confidentiality by adding back-end encryption to the entire array.

D@RE provides hardware-based, on-array, back-end encryption for Symmetrix arrays by using Fibre Channel I/O modules that incorporate XTS-AES 256-bit data-at-rest encryption. These modules encrypt and decrypt data as it is being written to or read from disk, thus protecting your information from unauthorized access even when disk drives are removed from the array.

D@RE supports either an internal embedded key manager, or RSA Data Protection Manager for external, enterprise-grade key management. For external key management, D@RE is qualified for interoperability with the RSA Key Manager (RKM) Appliance version 2.7 SP1, and the RSA Data Protection Manager (DPM) Appliance version 3.2 or lower.

**Note:** D@RE with the DPM is not supported in VM environments without an approved RPQ.

RKM is the legacy version of the RSA external key manager. DPM is the more recent release of the key manager with additional functionality. The terms RKM and DPM are interchangeable depending on your configuration. References to DPM in this document should be interpreted as RKM if you are using version 2.7 SP1. References to the RKM Server Administrator refer to the administrator of either version of the key manager.
Audience

The audience for this document includes:

- EMC staff and partners, including IT planners, storage architects, and administrators involved in evaluating, acquiring, managing, operating, or designing security for an EMC networked storage environment.
## Terminology

### Table 1  Symmetrix array terms

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disc Array Enclosure (DAE)</td>
<td>Storage module that contains drives, link control cards (LCCs), and power supplies and cooling components.</td>
</tr>
<tr>
<td>Enginuity</td>
<td>EMC Symmetrix arrays run the Enginuity™ operating environment.</td>
</tr>
<tr>
<td>Symmetrix Audit Log</td>
<td>An immutable (not changeable) audit log that tracks security events on a Symmetrix array. The audit log allows administrators to identify any breaches in the array and prove compliance with data protection policies.</td>
</tr>
<tr>
<td>Symmetrix Service Processor</td>
<td>A component that monitors the array environment, provides remote notification and remote support capabilities, and allows EMC personnel to access the array locally or remotely.</td>
</tr>
<tr>
<td>SymmWin Application</td>
<td>A graphics-based tool for configuring and monitoring a Symmetrix array.</td>
</tr>
<tr>
<td>I/O Module (SLIC)</td>
<td>Component that contains an AES-256 encryption controller and provides connectivity to DAEs. The Key Encryption Key is programmed into write-only, non-volatile memory in the I/O module, and it cannot be retrieved back from the hardware.</td>
</tr>
</tbody>
</table>

### Table 2  Encryption terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>XTS-AES Algorithm</td>
<td>An XEX-based Tweaked Codebook (TCB) mode with Cipher Text Stealing (CTS) disk encryption used for the encryption of sector-based storage devices.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Pairs of DPMs that include a primary appliance and a secondary appliance.</td>
</tr>
<tr>
<td>Data Encryption Key (DEK)</td>
<td>Used by Symmetrix key encryption algorithms to encrypt and decrypt data and apply confidentiality protection to information.</td>
</tr>
<tr>
<td>Key Encryption Key (KEK)</td>
<td>Keeps DEKs secure during storage and transmission. The approved technique to protect DEKs is to use KEKs along with the AES Key Wrap algorithm.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Load Balancer</td>
<td>Device that distributes network or application traffic across a number of servers.</td>
</tr>
<tr>
<td>RSA Key Manager Client</td>
<td>Resides on the service processor and communicates with the DPM to retrieve encryption keys and persistently cache them within the array.</td>
</tr>
<tr>
<td>RSA Data Protection Manager (DPM)</td>
<td>Provides encryption key management capabilities such as secure key generation, storage, distribution, and audit. Also referred to as the Key Manager Appliance.</td>
</tr>
</tbody>
</table>
D@RE now supports an external Enterprise Key Server, which provides the following benefits:

- Highly-available and resilient environment for long-term key storage external to the Symmetrix array.
- Support for a large numbers of keys and clients across geographic and organizational boundaries.
- Centralized key management and auditing for security compliance objectives.
- Separation of encryption key storage from encrypted data.
- Ability to temporarily decommission arrays for secure transport from one data center to another.

D@RE has been qualified for interoperability with the RSA Data Protection Manager (DPM), which is an all-in-one packaging of the RSA Key Manager Server that simplifies the installation and management of the system. The DPM delivers the Key Manager Server in a low-profile, rack-mountable form that can easily be shipped and installed as a complete platform. This includes the operating system, web server, application server, database, and RSA Access Manager. In addition, all of the third-party software components required to run the Key Manager Server are included.

The DPM does not include software that is not part of the Key Manager Server, such as the Key Manager Client (which is external) or a load balancer (which can be external).

Note: The DPM can be used with a FIPS 140-2 level 3 certified HSM. In addition, the Fibre Channel I/O modules used by D@RE are certified for FIPS 140-2 Level 1.
Figure 1 illustrates the D@RE architecture.

![D@RE Architecture Diagram]

**Figure 1 D@RE Architecture**

For a detailed description of the architecture and features of the Data Protection Manager, refer to the *RSA Data Protection Manager Planning Guide*.
Configuring the D@RE environment

Configuring the D@RE environment requires collaboration between the RKM Server Administrator and the Symmetrix Customer Engineer. Table 3 provides a high-level overview of the configuration process and identifies the administrator responsible for performing each step.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Owner</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set up the D@RE environment on the DPM.</td>
<td>RKM Server Administrator</td>
<td>1. Obtain the PKI Credentials for the DPM and the Symmetrix Key Manager Client. For best practices, see “Appendix B: Planning a PKI credentials strategy” on page 30.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Define the following key manager objects:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Identity group</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Identity (for manual enrollment)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Key classes (KEK and DEK)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Crypto policies (KEK and DEK)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For detailed instructions and best practices, see “Appendix A: Configuring the DPM” on page 24.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Define the client enrollment type (Auto Enrollment or Manual Enrollment).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For Auto Enrollment, define the profile name and the activation code, and then bulk upload credentials.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For Manual Enrollment, provide the credential files and the client credential password to the Symmetrix Customer Engineer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For detailed instructions and best practices, see “Appendix A: Configuring the DPM” on page 24.</td>
</tr>
</tbody>
</table>
### Table 3  Configuring the D@RE environment

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Owner</th>
<th>Details</th>
</tr>
</thead>
</table>
| 2    | Obtain the D@RE DPM configuration information for each Symmetrix system from the RKM Server Administrator | Symmetrix Customer Engineer | Obtain the following information from the RKM Server Administrator:  
- Enrollment type (Auto Enrollment or Manual Enrollment)  
- DPM IP/host name (If you are using a load balancer, enter the virtual IP. Add details about how to determine the correct IP in a cluster group environment.)  
- DPM Port number (Port 443 is the default. This is the standard port for secure SSL connections. Changing the port requires authorization by EMC using the EMC Request for Product Qualifier process.)  
- DEK and KEK key class names  
- For Auto Enrollment: profile name and activation code.  
- For Manual Enrollment: credential files and client credential password.  
- Identity  
- Client application name  
For detailed instructions and best practices, see “Appendix A: Configuring the DPM” on page 24. |
| 3 (New Installation) | Install a new Symmetrix array with the DPM | Symmetrix Customer Engineer | 1. Run the Symmwin Configure and Install New Symmetrix script.  
2. Select Enterprise Key Server as the server type.  
3. Provide the DPM information when prompted.  
For detailed instructions, see “Configure and Install New Symmetrix” on page 10. |
| 3 (Migration) | Migrate from the embedded server to the enterprise key server | Symmetrix Customer Engineer | 1. Run the Symmwin Migrate from embedded to enterprise key server script.  
2. Provide the DPM information when prompted.  
For detailed instructions, see “Migrate from the embedded server to the enterprise key server” on page 13. |
Service procedures

The following sections describe the service procedures that are related to D@RE with the DPM.

Configure and Install New Symmetrix

This section describes the key management events that occur during the installation of a new Symmetrix array with the DPM.

Prerequisites

◆ The D@RE environment must be configured on the DPM. Table 3, “Configuring the D@RE environment,” on page 8 provides additional details.

◆ You must have obtained the D@RE DPM configuration information from the RKM Server Administrator.

◆ For manual enrollment, the certificates and client credential files must be available on external USB storage or the service processor.

◆ For use with the RSA Key Manager Appliance version 2.7 SP1, the Symmetrix array must be running Enginuity version 5875.198.148 or higher.

◆ For use with the RSA Data Protection Manager version 3.2 or lower, the Symmetrix array must be running Enginuity version 5875 Q1 2012 SR or higher.

◆ All engines must have encryption capable Back End I/O Modules (PN 303-176-100B).

◆ D@RE must be enabled in the Symmetrix array configuration settings before you start the installation procedure.

Note: The installation script will fail if any of the prerequisites are not satisfied.

The DPM and the Key Manager Client communicate over a Secure Socket Layer (SSL) connection. SSL uses public key cryptography to establish a secure, mutually authenticated communication channel between the DPM and the Key Manager Client.

If you want to generate the SSL key pairs and certificate files on the service processor, see “Appendix C: PKI credentials on the service processor” on page 37.
Enabling D@RE

To enable D@RE,

1. In SymmWin, open Configuration > IMPL Initialization > Common Settings > DARE System.

2. Set the DARE flag to YES.

3. Verify that D@RE is enabled by using SymmWin to view the impl.bin file.

   Figure 2 shows the impl.bin file for a system with D@RE enabled.

   ![Figure 2 Using the impl.bin file to verify that D@RE is enabled](image)
4. Once D@RE has been enabled and you have verified that all of the prerequisites are met, install the Symmetrix array by running the following script from SymmWin:

   **Procedures > Procedure Wizard > System Initialization Tools > Configure and Install New Symmetrix**

The following key management events occur during the installation:

1. The installation script prompts you to select either Enterprise Key Server or Embedded Key Server. Select Enterprise Key Server.
   
   **Note:** Once a Symmetrix array has been configured to use the external Enterprise Key Server, switching back to the Embedded Key Server is not supported.

2. The script requests the following information, as previously provided by the RKM Server Administrator:
   - Enrollment type (Auto Enrollment or Manual Enrollment)
   - DPM IP address or host name
   - DPM port number (default is 443)
   - Identity
   - Client application name

3. For Auto Enrollment, provide the following information:
   - Profile name and activation code

4. For Manual Enrollment, provide the following information:
   - Path to the client credential file/identity certificate file
   **Note:** This is a P12 certificate with a .pfx or .p12 file extension.
   - Client credential password or PKCS#12 password
   - Path to the root certificate/server CA certificate file
   **Note:** This file has a .cer or .pem file extension.

5. The script displays all of the entered configuration information and requests a final confirmation.

6. The script attempts to connect the Key Manager Client to the DPM. If the script cannot make the connection, it displays an error message that indicates a possible problem with connectivity.
7. After a secure connection is established between the Key Manager Client and the DPM, the script performs the following operations to verify that the DPM is correctly configured:
   a. Creates a test DEK and KEK and examines their properties to verify that the key classes are configured correctly on the DPM.

   Note: See “Crypto policies” on page 27 for the correct settings.

   b. Verifies that the server is not in a read-only mode.
   c. Wraps the test DEK with the test KEK to confirm functionality.
   
   If any of the settings are incorrect, the script displays an error message that describes the discrepancy and provides the correct setting. After the RKM Server Administrator has applied the correct settings on the DPM, you can resume the script.

8. The script asks the DPM to generate a KEK for the array.

9. The script asks the DPM to generate a DEK for each drive.

10. The script initializes the Symmetrix array with the wrapped DEKs, and performs the rest of the generic initial configuration steps such as cable verification and VTOC.

11. The script backs up the Key Manager Client configuration details to the array for use during a service processor replacement.

12. The script populates the Symmetrix Audit Log entries.

Migrate from the embedded server to the enterprise key server

This section describes the key management events that occur during the non-disruptive migration of a Symmetrix array from using the Embedded Key Server to using the DPM. During the process, the Key Manager Client is reconfigured to connect to the DPM. The keys are then migrated to the DPM and securely deleted from the local keystore.

The DPM and the Key Manager Client communicate over a Secure Socket Layer (SSL) connection. SSL uses public key cryptography to establish a secure, mutually authenticated communication channel between the DPM and the Key Manager Client.
If you want to generate the SSL key pairs and certificate files on the service processor, see “Appendix C: PKI credentials on the service processor” on page 37.

**Note:** Once a Symmetrix array has been configured to use the external Enterprise Key Server, switching back to the Embedded Key Server is not supported.

To migrate to the enterprise key server, run the following script from SymmWin:

**Procedures > Procedure Wizard > System Initialization Tools > DARE > Migrate from embedded to enterprise key server**

**Prerequisites**
- The D@RE environment must be configured on the DPM. Table 3, “Configuring the D@RE environment,” on page 8 provides additional details.
- You must have obtained the D@RE DPM configuration information from the RKM Server Administrator.
- For manual enrollment, the certificate and client credential files must be available on the service processor.

**Key management events**
1. The script verifies that D@RE is enabled and running in the embedded mode.
2. The script requests the following information, as previously provided by the RKM Server Administrator:
   - Enrollment type (Auto Enrollment or Manual Enrollment)
   - DPM IP address or host name
   - DPM port number (default is 443)
   - Identity
   - Client application name
3. The script requests the following information, as previously provided by the RKM Server Administrator:
   - Profile name
   - Activation code
4. For Manual Enrollment, provide the following information:
   - Path to the client credential file/identity certificate file

**Note:** This is a P12 certificate with a .pfx or .p12 file extension.
Service procedures

- Client credential password or PKCS#12 password
- Path to the root certificate/server CA certificate file
  
  **Note:** This file has a .cer or .pem file extension.

5. The script displays all of the entered configuration information and requests a final confirmation.

6. The script attempts to connect the Key Manager Client to the DPM. If the script cannot make the connection, it displays an error message that indicates a possible problem with connectivity.

7. After a secure connection is established between the Key Manager Client and the DPM, the script performs the following operations to verify that the DPM is correctly configured:
   a. Creates a test DEK and KEK and examines their properties to verify that the key classes are configured correctly on the DPM.

   **Note:** See “Crypto policies” on page 27 for the correct settings.

   b. Verifies that the server is not in a read-only mode.

   c. Wraps the test DEK with the test KEK to confirm functionality.

If any of the settings are incorrect, the script displays an error message that describes the discrepancy and provides the correct setting. After the RKM Server Administrator has applied the correct settings on the DPM, you can resume the script.

8. The script migrates the KEK and DEKs to the DPM.

9. The script backs up the Key Manager Client configuration details to the array for use during a service processor replacement.

10. The script securely deletes the local keystore.

11. The script populates the Symmetrix Audit Log entries.

**Note:** If the migration fails, you must run a script to delete all of the keys and metadata. Contact product support for the script. Ensure that the key classes are deleted on all of the nodes before restarting.

---

**Service Processor replacement**

To replace the service processor:
Service procedures

1. Follow the instructions in the Symmetrix Hardware Document Viewer under Start > (Your VMAX Series)> Procedure > Maintenance > Other > Replace server.

2. When the Service Processor replacement is complete, the previously backed up client configuration is restored from the array to the new service processor, the configuration files are extracted, and the credentials are restored.

3. SymmWin verifies that the keys are intact and the Symmetrix array can still communicate with the DPM.

Array decommission

This section describes permanent and temporary array decommissions. A permanent decommission provides the ability for instant and irreversible data shredding. All of the encryption keys are permanently destroyed on the DPM, and all of the persistent cached copies of the keys on the array are zeroized. As a result, all of the data on the array becomes cryptographically erased.

A temporary decommission provides the ability to securely relocate a Symmetrix array within the data center or across data centers without the risk of key loss or key compromise. All of the persistent copies of the keys on the array are zeroized, but the keys are left intact on the DPM. Upon re-installation at the new location and re-enrollment with the DPM, the array re-acquires the keys from a DPM in the same cluster group. It can be the same DPM that was used before the move or a different one.

To facilitate relocation of the Symmetrix array across data centers and geographical boundaries, all of the DPMs protecting keys for the array must be part of the same cluster group. It is not possible to share keys between DPMs that are not part of the same cluster group.

**Note:** You will need data erasure-level Symmetrix Secure Credentials to perform decommission operations.

Permanent array decommission

To permanently decommission a Symmetrix array, run the following script from SymmWin:

- **Procedures > Procedure Wizard > System Initialization Tools > DARE > Permanent Array Decommission**

Key management events

1. The service processor destroys the KEK on the DPM.
2. For every drive configured in the array, the service processor destroys the DEK on the DPM.

3. The system is taken offline.

4. All KEKs and DEKs are zeroized within the array.

5. A certificate file that details the decommission status is produced on the service processor for audit purposes.

Temporary decommission

To temporarily decommission a Symmetrix array, run the following script from SymmWin:

```
Procedures > Procedure Wizard > System Initialization Tools > DARE > Temporary Array Decommission
```

Prerequisites for recommissioning the array

- You must have obtained the D@RE DPM configuration information from the RKM Server Administrator.

- For manual enrollment, the certificates and client credential files must be available on the service processor.

Key management events

1. The system is taken offline.

2. All KEKs and DEKs are zeroized within the array.

3. The system is powered off.

4. A certificate file that details the decommission status is produced on the service processor for audit purposes.

5. The array is moved to a new location and powered on.

   Note: The array will fail to IML during the power on due to missing keys.

6. Run the following script from SymmWin:

   ```
   Procedures > Procedure Wizard > System Initialization Tools > DARE > Recommission Temporary Decommissioned Array
   ```

7. The script requests the following input:
Service procedures

- Enrollment type (Manual Enrollment / Automatic Enrollment)
- Identity
- Client application name

8. If you are using automatic enrollment, the script requests the following information:
   - Auto registration profile
   - Activation code

9. If you are using manual enrollment, the script requests the following information:
   - Client credential file/identity certificate file.
   - Client credential password or PKCS#12 password.
   - Root certificate/server CA certificate file.

10. The script attempts to connect the Key Manager Client to the DPM. If the script cannot make the connection, it displays an error message that indicates a possible problem with connectivity.

11. The service processor retrieves the KEK from the DPM.

12. The service processor retrieves the DEK for each drive in the system.

13. The service processor populates the array with the retrieved KEK and DEKs.

14. The system performs a full IML and the vault image is restored from the drives.

15. The system becomes operational.

16. The script backs up the new client configuration in the array.

17. The script populates the Symmetrix Audit Log entries.

Modify RKM Server Configuration Information

This script is used to change the DPM or load balancer that the Key Manager Client is configured to work with. The script allows you to update the Host Name/IP address and port information. In a multi-cluster environment, it can be used to switch the DPM that the Key Manager Client is actively communicating with. This operation is not for re-enrolling an existing client. It only updates the IP connectivity while preserving the credentials.
Service procedures

Prerequisites
◆ DPM IP or host name
◆ DPM port
To modify the RKM server configuration information, run the following script from SymmWin:

Procedures > Procedure Wizard > CE/RTS/PSE Services > DARE > Modify RKM Server Configuration Information

Key management events

The following key management events occur when you modify the RKM server configuration information:

1. The script requests the DPM IP and port.
2. The script updates the configuration file, backs up the client configuration to the array, and verifies connectivity using the new connection.
3. The script populates the Symmetrix Audit Log entries.

Re-enroll RKM client with server

This script allows the Key Manager Client to re-enroll with the DPM with new credentials. Re-enrolling is required in the event that the credentials expire or the credential files are corrupted.

Prerequisites
◆ For manual enrollment, the certificates and client credential files must be available on the service processor.
◆ Obtain the following information from the RKM Server Administrator:
For automatic enrollment:
• Profile name
• Activation code
• Client application name
For manual enrollment:
• Client credential file/identity certificate file
• Client credential password
• Root certificate
• Identity
To re-enroll the Key Manager Client to the DPM, run the following script from SymmWin:

**Procedures > Procedure Wizard > CE/RTS/PSE Services > DARE > Re-enroll RKM Client with Server**

### Key management events

The following key management events occur during re-enrollment of the Key Manager Client with the DPM:

1. The script requests the following input:
   - Enrollment type (Manual Enrollment / Automatic Enrollment)
   - Identity
   - Client application name

2. If you are using automatic enrollment, the script requests the following information:
   - Auto registration profile
   - Activation code

3. If you are using manual enrollment, the script requests the following information:
   - Client credential file/identity certificate file.
   - Client credential password or PKCS#12 password.
   - Root certificate/server CA certificate file.

4. The script attempts to connect the Key Manager Client to the DPM. If the script cannot make the connection, it displays an error message that indicates a possible problem with connectivity.

5. The script updates the configuration file and backs up the client configuration to the array.

6. The script populates the Symmetrix Audit Log entries.

---

**Periodic DARE Integrity Test**

The Periodic DARE Integrity Test ensures that the Symmetrix array is functioning properly. The script performs the following actions:

- Verifies network connectivity to the DPM.
- Verifies key integrity between the Symmetrix array and the DPM.
Service procedures

- Checks to see if credentials are going to expire soon.
The system dials home if there is a problem with DPM connectivity, key integrity, or credentials.

If there is an issue with connectivity to the DPM:

1. Verify the DPM configuration information on the DARE tab of the Symmetrix Site Configuration window.
   Figure 3 shows an example of the Symmetrix Site Configuration window.

2. Verify network connectivity.
3. Verify that the DPM is up and running. You may need to involve the DPM administrator.
4. Involve Symmetrix or RSA support personnel.

If there is an issue with key integrity (which includes expired keys and key compromise), involve Symmetrix or RSA support personnel.

If the credentials are going to expire soon, follow the procedure outlined in “Re-enroll RKM client with server” on page 19 to re-enroll the Key Manager Client with the DPM.
D@RE is an easy-to-use, minimal-management solution for data-at-rest encryption. D@RE keeps information safe from drive theft or loss by providing back-end encryption for the entire array. By utilizing the DPM, D@RE is able to automatically manage encryption key operations.
Table 4 on page 23 describes the documents that contain additional information about the RSA Key Manager and D@RE.

### Table 4

**Documentation related to D@RE**

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA Data Protection Manager Appliance Release Notes</td>
<td>Provides the latest information on the RSA Data Protection Manager Appliance.</td>
<td>Available from the RSA Data Protection Manager Appliance online help</td>
</tr>
<tr>
<td>RSA Data Protection Manager Appliance Getting Started Guide</td>
<td>Provides layout information and setup instructions for the RSA Data Protection Manager Appliance.</td>
<td></td>
</tr>
<tr>
<td>RSA Data Protection Manager Appliance Migration Guide</td>
<td>Intended for administrators who are planning and implementing a migration of their RSA Data Protection Manager Appliance from version 2.7 SP1 to version 3.2 or lower.</td>
<td></td>
</tr>
<tr>
<td>RSA Data Protection Manager Appliance Planning Guide</td>
<td>Provides a general understanding of RSA Data Protection Manager Appliance, its high-level architecture, features, and deployment information and suggestions.</td>
<td></td>
</tr>
<tr>
<td>EMC Solutions Enabler Symmetrix Array Management CLI Product Guide.</td>
<td>The Monitoring Symmetrix Data at Rest Encryption section provides details about administering and monitoring D@RE.</td>
<td>Available on the Solutions Enabler product CD.</td>
</tr>
<tr>
<td>EMC Symmetrix Data at Rest Encryption Detailed Review</td>
<td>Describes the features and operations of Data at Rest Encryption with the embedded key server.</td>
<td>Available on EMC Online Support.</td>
</tr>
</tbody>
</table>
Appendix A: Configuring the DPM

Issues that you need to consider when configuring a DPM to support D@RE include:

◆ Deciding whether to use an existing DPM, discussed on page 24.
◆ Deciding whether to use manual or automatic enrollment, discussed on page 24.
◆ Planning identity groups and identities, discussed on page 24.

This section focuses on those aspects of configuring a DPM that are specific to supporting D@RE. Refer to RSA documentation for general information on configuring a DPM.

Deciding whether to use an existing DPM

If your enterprise has already deployed a DPM, you can use that appliance to support D@RE. The DPM must be Key Manager Appliance version 2.7 SP1 or DPM version 3.2 or lower.

Contact RSA professional services to help determine if there is adequate capacity and performance available on an existing DPM deployment for the Symmetrix clients involved.

Deciding whether to use manual or automatic enrollment

D@RE supports both auto enrollment and manual enrollment.

The DPM and the Key Manager Client communicate over an SSL connection. SSL uses public key cryptography to establish a secure, mutually authenticated communication channel between the DPM and the Key Manager Client.

With auto enrollment, the RKM Server Administrator creates the profile name and the activation code and provides this information to the Symmetrix Customer Engineer before the installation. The client credential and certificate files are preloaded on the DPM, and the appliance downloads a pair of these files to the client during the enrollment process.
With manual enrollment, the RKM Server Administrator assigns a unique identity to the client and provides the CA root profile, credential file, and password to the Symmetrix Customer Engineer. D@RE supports both single CA-signed and chained CA-signed certificates.

**Note:** Only certificates and credentials signed using the RSA algorithm are supported. ECC or DSA algorithm-signed credentials will not work with the D@RE environment.

For both manual and auto enrollment, the identity name must be unique per array and the application name must be unique for each client enrollment (even for the same array). With manual enrollment, the identity name and the application name are added to the DPM by the RKM Server Administrator ahead of time, while with auto enrollment the unique choices for these names are provided to the Symmetrix Customer Engineer instead.

### Planning identity groups and identities

As part of the planning process for deploying a DPM, you need to plan identity groups and identities to support D@RE.

An *identity group* is the mechanism that the DPM uses to map an enterprise’s security processes and requirements to a set of key domains where a specific key class is valid. An identity group consists of a key class and a set of identities that have access rights to that key class. Identity groups allows the enterprise to isolate systems with different operational and security requirements. For example, an enterprise may be divided into regional data centers, each of which is defined by a separate identity group. Or an enterprise may consist of separate service providers, each of which requires its own identity group.

An identity is entity (for example, D@RE) that needs to use a key class to protect sensitive data. An identity binds an application to a public key certificate. An identity can be a member of multiple identity groups.

If multiple Symmetrix arrays are connected to a DPM, cluster, or cluster group, each array must have a unique identity. However, each array may be placed in either the same identity group or in different identity groups. All of the identities in the same identity group can
access and operate with the same set of keys, but since each array has an independent set of keys, it is not necessary to group multiple arrays into the same identity group.

It is best practice to confine each Symmetrix identity to its own identity group for security and management purposes. The name of the identity group can be assigned by the RKM Server Administrator, but EMC recommends that the name include the Symmetrix array serial number.

---

**Defining key manager objects**

The following key manager objects must be pre-defined on the Key Manager Administration console:

- Identity Group
- Identity (for manual enrollment)
- Crypto Policies
- Key Classes
- Profile Name
- Activation Code (for auto enrollment)
- Enrollment Type (auto or manual)

In addition to defining the objects described above, the RKM Server Administrator must provide the following information to the Symmetrix Customer Engineer:

- Client Application Name
- Credentials (for auto enrollment)

**Note:** Refer to the *RSA Key Manager Server Administration Guide* for detailed instructions on defining RKM key manager objects.

The tables in the following sections list the attributes for the key manager objects that must be defined on the Key Manager Administration console. The tables only list the attributes that require information specific to D@RE.
Identity group

Enter the D@RE specific attributes listed in Table 5.

Table 5 Identity groups

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User-defined value.</td>
</tr>
<tr>
<td></td>
<td><strong>EMC recommendation:</strong></td>
</tr>
<tr>
<td></td>
<td>EMC_Symm_&lt;Symmetrix serial number&gt;</td>
</tr>
</tbody>
</table>

Identity

For manual enrollment, enter the D@RE specific attributes listed in Table 6.

**Note:** The identity must be unique for every Symmetrix client configured on the server.

Table 6 Identity

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User-defined value.</td>
</tr>
<tr>
<td></td>
<td><strong>EMC recommendation:</strong></td>
</tr>
<tr>
<td></td>
<td>EMC_Symm_&lt;Symmetrix serial number&gt;</td>
</tr>
</tbody>
</table>

Crypto policies

For the KEK crypto policy, enter the D@RE specific attributes listed in Table 7.

**Note:** Defined crypto policies can be shared between Symmetrix clients configured on the server

Table 7 KEK Crypto Policy

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>User-defined name of this crypto policy.</td>
</tr>
<tr>
<td></td>
<td><strong>EMC Recommendation:</strong></td>
</tr>
<tr>
<td></td>
<td>EMC_Symm_KEK</td>
</tr>
<tr>
<td>Cipher</td>
<td>Algorithm</td>
</tr>
<tr>
<td></td>
<td>Required value of <strong>AES</strong></td>
</tr>
<tr>
<td>Key size</td>
<td>Required value of <strong>256</strong></td>
</tr>
<tr>
<td>Mode</td>
<td>Required value of <strong>ECB</strong></td>
</tr>
<tr>
<td>Duration</td>
<td>Duration</td>
</tr>
<tr>
<td></td>
<td>Required value of <strong>Infinite</strong></td>
</tr>
</tbody>
</table>
For the DEK crypto policy, enter the D@RE specific attributes listed in Table 8.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>User-defined name of this crypto policy.</td>
</tr>
<tr>
<td></td>
<td><strong>EMC Recommendation:</strong></td>
</tr>
<tr>
<td></td>
<td>EMC_Symm_DEK</td>
</tr>
<tr>
<td>Cipher</td>
<td>Algorithm</td>
</tr>
<tr>
<td></td>
<td>Required value of AES</td>
</tr>
<tr>
<td>Key size</td>
<td>Required value of 512</td>
</tr>
<tr>
<td>Mode</td>
<td>Required value of XTS</td>
</tr>
<tr>
<td>Duration</td>
<td>Duration</td>
</tr>
<tr>
<td></td>
<td>Required value of Infinite</td>
</tr>
</tbody>
</table>

**Key classes**

For the KEK key class, enter the D@RE specific attributes listed in Table 9.

**Note:** Key class names must be unique for every Symmetrix client configured on the server.

**Note:** The option that allows you to choose between using the current key or using a new key each time does not have any impact on D@RE.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>User-defined value.</td>
</tr>
<tr>
<td></td>
<td><strong>EMC recommendation:</strong></td>
</tr>
<tr>
<td></td>
<td>EMC_Symm KEK_&lt;Symmetrix serial number&gt;</td>
</tr>
<tr>
<td>Identity Group</td>
<td>Select the user-defined name of the identity group that contains the Symmetrix array.</td>
</tr>
<tr>
<td>Cipher</td>
<td>Algorithm</td>
</tr>
<tr>
<td></td>
<td>Select the previously defined KEK crypto policy.</td>
</tr>
<tr>
<td>Key size</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td></td>
</tr>
<tr>
<td>Duration</td>
<td></td>
</tr>
</tbody>
</table>
For the DEK key class, enter the D@RE specific attributes listed in Table 10.

Note: The option that allows you to choose between using the current key or using a new key each time does not have any impact on D@RE.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Name</td>
<td>User-defined value.</td>
</tr>
<tr>
<td></td>
<td><strong>EMC recommendation:</strong></td>
</tr>
<tr>
<td></td>
<td>EMC_Symm_DEK_&lt;Symmetrix serial number&gt;</td>
</tr>
<tr>
<td>Identity Group</td>
<td>Select the user-defined name of the identity group that contains the Symmetrix array.</td>
</tr>
<tr>
<td>Cipher Algorithm</td>
<td>Select the previously defined KEK crypto policy.</td>
</tr>
<tr>
<td>Key size</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td></td>
</tr>
<tr>
<td>Duration</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B: Planning a PKI credentials strategy

A DPM and a Key Manager Client each require PKI credentials to enable a secure, mutually authenticated communication.

Refer to the section entitled "Public Key Infrastructure Requirements" in the RSA Key Manager Server Administrator’s Guide for additional information about PKI credential requirements.

Issues that you need to consider when planning a PKI credentials strategy for D@RE include:

- Understanding PKI credentials requirements, discussed on page 30.
- Choosing a PKI platform, discussed on page 32.
- Planning to obtain PKI credentials, discussed on page 35.

Understanding PKI credentials requirements

The Key Manager Client component on the service processor communicates with the DPM to obtain cryptographic keys used to encrypt disk devices. The DPM and the Key Manager Client communicate over an SSL connection. SSL uses public key cryptography to establish a secure, mutually authenticated communication channel between the DPM and the Key Manager Client.

Public key cryptography uses a matched pair of mathematically related keys — known as a public/private key pair — to encrypt and decrypt data and to generate and verify digital signatures. A mathematical algorithm and a value (called a "key") encrypt data into an unreadable form. A second key used with the mathematical algorithm is used to decrypt the data.

Each key in a public key/private key pair performs a one-way transformation on the data and performs the inverse function of its matching key. If the public key is used to encrypt data, the private key is used to decrypt that data. Likewise, if the private key is used to encrypt data, the public key is used to decrypt that data.

The sender uses the intended recipient’s public key to scramble data. Once encrypted, the data can only be decoded with the recipient’s private key. Inversely, the sender can also scramble data using its private key. This provides the basis for a digital signature. If a recipient
decrypts data with another entity’s public key, the other entity must have used its private key to encrypt that data in the first place. Since only the owner can utilize its private key, the encrypted data becomes a kind of electronic signature.

Both the DPM and the Key Manager Client have their own public key/private key pair. The private key is kept secret. The public key is embedded in a digital certificate known as a public key certificate. The public key certificate ensures that the public key contained in it belongs to the entity to which the certificate was issued.

The public key certificate has itself been “digitally signed” by a Certification Authority. The Certification Authority is responsible for verifying the identity of the owner of a public key certificate. For example, the Certification Authority can be a network security director, an IT help desk, or an external provider such as VeriSign. The Certification Authority signs the public key certificate using its private key, which is used to verify the public key certificate.

By exchanging public key certificates, a DPM and the Key Manager Client can learn each other’s public key. When establishing the SSL connection, each entity authenticates itself to the other using public key certificates. The public key certificate, signed by a Certification Authority, ensures that the certificate holder is really who he claims to be. Once the DPM and the Key Manager Client know each other’s public key, they can use them to encrypt data and send it to one another, or to verify digital signatures.
Appendix B: Planning a PKI credentials strategy

#### Required PKI credentials

Table 11 on page 32 summarizes PKI credentials requirements for D@RE

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
<th>DPM</th>
<th>Key Manager Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public key certificate</td>
<td>Digital certificate that packages a public key, information about the algorithms used to generate the key pair, owner or subject data, the digital signature of a Certification Authority (CA) that has verified the subject data, and a date range during which the certificate can be considered valid. The public key certificate must be in Privacy Enhanced Mail (PEM) format. An example of a public key certificate is RKM_server.pem.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Private key file</td>
<td>File that contains the private key. The private key file does not include any server information. It contains encryption information and a fingerprint. The private key file must be in PEM format. An example of a private key file is RKM_server.pem.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Trusted root certificate</td>
<td>Digital certificate that has been digitally signed by the CA that signed the public key certificate. The trusted root certificate must be in CER, CRT, or PEM file format. An example of a trusted root certificate is client_root.pem.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Choosing a PKI platform

**Note:** EMC recommends that you consult with your RSA representative to determine the PKI platform best suited to your environment.

A public key infrastructure (PKI) supports the implementation and operation of a certificate-based public key cryptographic system. The main function of a PKI is to distribute credentials accurately and reliably to users and applications that need them. The DPM does not provide a facility for generating or requesting PKI credentials. You
must have some method of generating or obtaining certificates, either by using self-signed certificates, implementing an internal PKI, or contracting with an external PKI provider.

Planning considerations for choosing a PKI platform include:

- If your enterprise has an existing PKI platform, deciding whether to use that platform or to implement a new PKI platform.
- If you are implementing a new PKI platform, choosing an appropriate solution from:
  - Self-signed certificates
  - Internal PKI platform
  - External PKI provider

**Deciding whether to use an existing PKI platform**

If your enterprise already has a PKI platform in place, you will probably want to use that PKI to support D@RE. Questions to answer before committing to an existing PKI include:

- Can the existing PKI satisfy all the requirements for a D@RE deployment.
- Do you have sufficient control over this system? Is it operated by another group that may hinder functional flexibility or request turnaround time?

**Implementing a new PKI platform**

**Note:** Enterprises without an existing PKI platform should strongly consider implementing RSA Key Services to support D@RE. The benefits for RSA digital certificate life cycle management and automating a recovery solution result in decreased overall effort and expense. Consult your RSA representative for more information.

The options for implementing a PKI platform include:

- Using OpenSSL to generate self-signed certificates.
- Deploying standalone PKI software for an internal PKI.
- Outsourcing PKI services to an external PKI provider.

Choosing a PKI is often based on the metrics of cost, flexibility, control, and speed of deployment. Examine the advantages and disadvantages of each approach and determine which PKI solution is best suited to your enterprise.
Self-signed certificates
A self-signed certificate does not have an external CA attesting to its authenticity. Rather, you (or a trusted agent at your site) attest to its authenticity. While self-signed digital certificates should not be relied upon externally by third parties, they can be appropriate for internal applications.

OpenSSL is an open source toolkit that can be used to generate self-signed certificates.

Self-signed certificates have the following advantages:

- Self-signed certificates provide a low-cost approach to establish a functional PKI infrastructure.
- Certificates can be generated with essentially no turnaround time.

Self-signed certificates have the following disadvantages:

- Steep learning curve.
- The enterprise must provide its own support.
- The long validity period of self-signed digital certificates makes it more likely that they can be compromised.
- More effort is involved to revoke self-signed certificates, because you must revoke certificates on each individual computer instead of at a central CA.

Inhouse PKI platform
In an inhouse PKI deployment, an enterprise purchases PKI software and creates a standalone PKI service used to generate public key certificates. In the inhouse PKI model, the enterprise assumes responsibility for provisioning, deploying, and maintaining the PKI. Dedicated staff are responsible for defining policies for creating and distributing certificates throughout the enterprise.

Examples of inhouse PKI solutions include:

- RSA Certificate Manager
- Microsoft Certification Authority

The advantages of an inhouse PKI include complete ownership of the PKI platform, which provides greater control and flexibility, since security policies can be tailored to unique business needs.

The primary disadvantage of an inhouse PKI is that the enterprise is responsible for defining security policies and for implementing and managing all components of the PKI.
External PKI provider

In the external PKI provider model, an enterprise contracts PKI services from a third-party CA. The CA builds and maintains the PKI and provides certificate processing services. CA-generated certificates should be chosen if the appropriate PKI services are already implemented at your enterprise.

Examples of external PKI providers include:

- Verisign
- Thawte
- GlobalSign
- Equifax

The primary advantage of External PKI providers is that they remove the burden of planning, building, and maintaining a PKI platform from the enterprise, allowing it to concentrate on its core business.

External PKI providers have the following disadvantages:

- The enterprise must select an external CA and implement its services before implementing D@RE.
- The shorter validity period of CA-issued certificates might require more frequent rekeying of the certificates.

Planning to obtain PKI credentials

Table 12 on page 36 describes the general process for obtaining PKI credentials. The specific steps differ slightly based on the PKI platform used. These instructions assume that you are generating the PKI credentials on the DPM. To generate PKI credentials on the Symmetrix service processor, see “Appendix C: PKI credentials on the service processor” on page 37.
### Table 12: Obtaining PKI credentials

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generate public key/private key pair.</td>
<td>Applicant uses a client tool (for example, OpenSSL) on the DPM to generate a public key/private key pair.</td>
</tr>
<tr>
<td>2</td>
<td>Generate CSR.</td>
<td>Applicant creates a certificate signing request (CSR). The CSR contains information identifying the applicant and the public key chosen by the applicant.</td>
</tr>
<tr>
<td>3</td>
<td>Send CSR to CA.</td>
<td>Applicant sends the CSR to a CA to apply for a public key certificate. In an internal PKI deployment, the CA is part of the same enterprise. In an external PKI deployment, the CA is an outsourced provider.</td>
</tr>
<tr>
<td>4</td>
<td>Generate public key certificate.</td>
<td>The trusted root or CA creates a public key certificate with the appropriate information (public keys, expiration date, and other data) and signs it using their private key. The trusted root or CA then delivers the public key certificate and a trusted root certificate to the applicant.</td>
</tr>
<tr>
<td>5</td>
<td>Load public key certificate and trusted root certificate.</td>
<td>The applicant loads the public key certificate and trusted root certificate on the DPM.</td>
</tr>
</tbody>
</table>
Appendix C: PKI credentials on the service processor

This appendix provides instructions for generating PKI credentials on the Symmetrix service processor. This process can be used for the installation of a Symmetrix array with the enterprise key server or for migrating from the embedded key server to the enterprise key server.

Table 13 provides an overview of the participants and their responsibilities during this process.

<table>
<thead>
<tr>
<th>Participant</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetrix Customer Engineer</td>
<td>• Create the Certificate Signing Request (client.csr)</td>
</tr>
<tr>
<td></td>
<td>• Create the PKCS#12 client credential file (client.p12)</td>
</tr>
<tr>
<td></td>
<td>• Run the key migration script on the service processor</td>
</tr>
<tr>
<td>Certificate Signer</td>
<td>• Certification Authority to sign the SSL certificate</td>
</tr>
<tr>
<td>Customer Representative</td>
<td>• Submit the client.csr file to the Certificate Signer</td>
</tr>
<tr>
<td></td>
<td>• Obtain the signed certificate (client.pem)</td>
</tr>
<tr>
<td></td>
<td>• Obtain the client root CA certificate (client_root_CA.pem)</td>
</tr>
<tr>
<td>RKM Server Administrator</td>
<td>• Handle certificates on the RKM side</td>
</tr>
<tr>
<td></td>
<td>• Provide the Symmetrix Customer Engineer with the server root CA certificate</td>
</tr>
<tr>
<td></td>
<td>(server_rootCA.pem)</td>
</tr>
<tr>
<td></td>
<td>• Upload the client.pem file onto the RKM administrative console to associate</td>
</tr>
<tr>
<td></td>
<td>the certification with the corresponding identity</td>
</tr>
</tbody>
</table>

To generate PKI credentials on the service processor:

1. Symmetrix Customer Engineer: Install OpenSSL on the service processor:
   a. Download openssl-0.9.8h-1-setup.exe from the following location:
      http://gnuwin32.sourceforge.net/packages/openssl.htm
   b. Complete the installation by using all of the default values.
2. Open the command prompt and enter the following command:
   cd C:\Program Files\GnuWin32\bin
3. To generate an RSA 2048-bit key and save it in a new client.key file, enter:
Appendix C: PKI credentials on the service processor

openssl genrsa -des3 -out client.key 2048

4. When prompted, provide a password that is at least 8 characters long.

5. Obtain the following details from the Customer Representative. This information will be used to complete the Certificate Signing Request (CSR).
   - Country Name (2 letter code)
   - State or Province Name (full name)
   - Locality Name
   - Organization Name
   - Organizational Unit Name
   - Common Name (VMAX host name)
   - Email Address

   Note: Do not enter the “challenge password” attribute.

6. To generate a CSR for the new key created in step 3, enter:

   openssl req -new -key client.key -out client.csr -config "C:\Program Files\GnuWin32\share\openssl.cnf"

7. When prompted, enter the password that you specified in step 4

8. Provide the resulting CSR file to the Certificate Signer (via the Customer Representative).

9. **Certificate Signer**: Process the CSR and (via the Customer Representative) return the signed certificate (client.pem) to the Symmetrix Customer Engineer and the RKM Server Administrator. Via the Customer Representative, return the client root CA certificate (client_rootCA.pem) to the RKM Server Administrator.

   Note: The signed certificate must be in PEM format. The client root CA certificate can be in PEM, CER, or CRT format.

10. **RKM Server Administrator**: Check the files and confirm that client_rootCA.pem is the certificate of the root Certification Authority that signed client.pem.
11. **RKM Server Administrator**: Ensure that the RKM server’s webserver trusts `client_rootCA.pem` for client certificate authentication.

12. **Symmetrix Customer Engineer**: To add the client certificate (`client.pem`) to the PKCS12 credential file (`client.p12`), enter:

   ```
   openssl pkcs12 -export -in client.pem -inkey client.key -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -out client.p12
   ```

   a. On the first password prompt, provide the private key password specified in step 4.

   b. On the second password prompt (and a third one for verification), provide a new password (at least 8 characters long) to encrypt the new PKCS#12. This password can be the same as the one used in step 4.

13. **RKM Server Administrator**: Provide the Symmetrix Customer Engineer with the server root CA certificate (`server_rootCA.pem`).

14. **Symmetrix Customer Engineer**: Run the key migration script to export the keys to the external key manager. See “Migrate from the embedded server to the enterprise key server” on page 13 for additional details.

   Note: When prompted to choose the enrollment type, you must select Manual Enrollment.

15. Once the migration is complete, uninstall `openssl-0.9.8h-1` from the service processor and delete the `C:\Program Files\GnuWin32\bin` folder and files.