

CLAIMS

1. A computer program product for facilitating processing in a computing environment, the computer program product comprising:
 - a computer readable storage medium readable by one or more processing circuits and storing instructions for performing operations comprising:
 - receiving an authentication response message at an initiator channel on an initiator node from a responder channel on a responder node to establish a secure communication, the receiving at a local key manager (LKM) executing on the initiator node;
 - performing a state check based on a security association of the initiator node and the responder node;
 - performing a validation of the authentication response message;
 - extracting an identifier of a selected encryption algorithm from the authentication response message; and
 - requesting the initiator channel to communicate with the responder channel based at least in part on a successful state check, a successful validation, and the selected encryption algorithm.
2. The computer program product of claim 1, wherein communication between the responder channel and the initiator channel is via a storage area network (SAN).
3. The computer program product of claim 1, wherein the operations further comprise:
 - computing a responder signature based at least in part on one or more parameters extracted from a previously received initialization message; and
 - comparing the responder signature to a signature extracted from the authentication response message as a further validation.
4. The computer program product of claim 3, wherein the responder signature is computed based on an initiator nonce, a shared key, a responder identifier, and at least one key from a set of cryptographic keys.
5. The computer program product of claim 1, wherein the operations further comprise decrypting a payload of the authentication response message, and validation of the authentication response message comprises checking one or more message header parameters and an identifier of the payload based on decrypting the payload.
6. The computer program product of claim 1, wherein the state check further comprises verifying a security association state of the initiator node.

7. The computer program product of claim 1, wherein the state check further comprises verifying a last received message state and a last sent message state of the LKM.
8. The computer program product of claim 1, wherein the operations further comprise rejecting the authentication response message based on an unsuccessful validation result or based on determining that the authentication response message comprises a notify type message indicating an error condition at the responder node.
9. The computer program product of claim 1, wherein the LKM executes in a logical partition of a computer system.
10. The computer program product of claim 1, wherein the responder node is a host computer or a storage array.
11. The computer program product of claim 1, wherein the operations further comprise building an LKM Done message comprising one or more session keys, an initiator security parameter index (SPI), and a responder SPI to enable encrypted communication between the initiator channel and responder channel using the selected encryption algorithm.
12. The computer program product of claim 11, wherein the operations further comprise starting a rekey timer that triggers a rekey process with respect to an external key manager.
13. The computer program product of claim 12, wherein the operations further comprise setting a security association state to complete and sending the LKM Done message to the initiator channel after starting the rekey timer.
14. A computer-implemented method of facilitating processing within a computing environment, the computer-implemented method comprising:
 - receiving an authentication response message at an initiator channel on an initiator node from a responder channel on a responder node to establish a secure communication, the receiving at a local key manager (LKM) executing on the initiator node;
 - performing a state check based on a security association of the initiator node and the responder node;
 - performing a validation of the authentication response message;
 - extracting an identifier of a selected encryption algorithm from the authentication response message; and
 - requesting the initiator channel to communicate with the responder channel based at least in part on a successful state check, a successful validation, and the selected encryption algorithm.

15. The computer-implemented method of claim 14, further comprising:
 - computing a responder signature based at least in part on one or more parameters extracted from a previously received initialization message, wherein the responder signature is computed based on an initiator nonce, a shared key, a responder identifier, and at least one key from a set of cryptographic keys; and
 - comparing the responder signature to a signature extracted from the authentication response message as a further validation.
16. The computer-implemented method of claim 14, further comprising:
 - decrypting a payload of the authentication response message, wherein validation of the authentication response message comprises checking one or more message header parameters and an identifier of the payload based on decrypting the payload.
17. The computer-implemented method of claim 14, wherein the state check further comprises verifying a security association state of the initiator node, and the state check further comprises verifying a last received message state and a last sent message state of the LKM.
18. The computer-implemented method of claim 14, further comprising:
 - building an LKM Done message comprising one or more session keys, an initiator security parameter index (SPI), and a responder SPI to enable encrypted communication between the initiator channel and responder channel using the selected encryption algorithm; and
 - starting a rekey timer that triggers a rekey process with respect to an external key manager.
19. A computer system for facilitating processing within a computing environment, the computer system comprising:
 - an initiator node; and
 - a plurality of channels coupled to the initiator node, wherein the computer system is configured to perform operations comprising:
 - receiving an authentication response message at an initiator channel on the initiator node from a responder channel on a responder node to establish a secure communication, the receiving at a local key manager (LKM) executing on the initiator node;
 - performing a state check based on a security association of the initiator node and the responder node;
 - performing a validation of the authentication response message;
 - extracting an identifier of a selected encryption algorithm from the authentication response message; and
 - requesting the initiator channel to communicate with the responder channel based at least in part on a successful state check, a successful validation, and the selected encryption algorithm.

20. The computer system of claim 19, wherein the initiator node is a host computer and the LKM executes in a logical partition of the host computer, and the responder node is a storage array.