

WHAT IS CLAIMED IS:

1. A method for authenticated communications between devices, the method comprising:
 - establishing communications for data streaming between a first device and a second device;
 - establishing a shared key;
 - exchanging the shared key between the first device and the second device;
 - encrypting a dataset by the first device using the shared key;
 - decrypting the dataset by the second device using the shared key;
 - evaluating key regeneration criteria to determine whether the shared key should be regenerated;
 - in response to determining that the shared key should be regenerated, generating a new shared key, and
 - encrypting a next dataset by the first device using the new shared key.
2. The method of claim 1, wherein the establishing a shared key comprises:
 - providing encryption algorithm parameters and a seed for an encryption algorithm.
3. The method of claim 1, wherein the exchanging the shared key comprises integrating a plurality of key exchange methodologies.
4. The method of claim 3, further comprising:
 - dynamically varying at least one of the key exchange methodology and frequency of key exchange.
5. The method of claim 4, wherein at least one of the key exchange methodology and frequency of key exchange is dynamically varied based on performance requirements of the first device or the second device and a security threat level.
6. The method of claim 1, wherein key regeneration criteria are evaluated to determine whether the shared key should be regenerated.

7. The method of claim 6, wherein the key regeneration criteria identify possible encryption algorithms and specific parameters for the encryption algorithms.

8. The method of claim 6, further comprising monitoring conditions that indicate when the shared key should be regenerated until key regeneration criteria are met.

9. The method of claim 1, wherein the generating the new shared key comprises: providing new encryption algorithm parameters for the shared key.

10. The method of claim 1, further comprising:
providing high security by utilizing secure keys and maximizing a rate of key rotation for a dataset.

11. A system for authenticated communications between devices, the system comprising:
a communications interface; and
a processor configured to:
establish communications for data streaming between a first device and a second device;
establish a shared key;
exchange the shared key between the first device and the second device;
encrypt a dataset by the first device using the shared key, wherein the second device decrypts the dataset using the shared key;
evaluate key regeneration criteria to determine whether the shared key should be regenerated;
in response to determining that the shared key should be regenerated,
generate a new shared key, and
encrypt a next dataset by the first device using the new shared key.

12. The system of claim 11, wherein the processor is further configured to establish a shared key by providing encryption algorithm parameters and a seed for an encryption algorithm.

13. The system of claim 11, wherein the processor is further configured to wherein the processor is further configured to integrate a plurality of key exchange methodologies for the shared key exchange.

14. The system of claim 13, wherein the processor is further configured to: dynamically vary at least one of the key exchange methodology and frequency of key exchange.

15. The system of claim 14, wherein at least one of the key exchange methodology and frequency of key exchange is dynamically varied based on performance requirements of the first device or the second device and a security threat level.

16. The system of claim 11, wherein the processor is further configured to: evaluate key regeneration criteria to determine whether the shared key should be regenerated.

17. The system of claim 16, wherein the key regeneration criteria identify possible encryption algorithms and specific parameters for the encryption algorithms.

18. The system of claim 16, the processor is further configured to: monitor conditions that indicate when the shared key should be regenerated until key regeneration criteria are met.

19. The system of claim 11, wherein the processor is further configured to: provide new encryption algorithm parameters to generate the shared key.

20. The system of claim 11, further comprising:
the processor is further configured to:
provide high security by utilizing secure keys and maximizing a rate of key rotation for a dataset.