

CLAIMS

What is claimed is:

1. A key management system capable of storing cryptographic keys and attributes associated with the cryptographic keys, wherein the key management system is configured to:
 - transmit a key identifier that identifies a cryptographic key to a cryptographic coprocessor;
 - in response to transmitting the key identifier, receive a first set of attributes from the cryptographic coprocessor, wherein one or more attributes in the first set of attributes are associated with the cryptographic key and originating from a key attribute storage of the cryptographic coprocessor;
 - serialize the first set of attributes and a second set of attributes into a first sequence of attributes; store the first sequence of attributes within an attribute frame, wherein one or more attributes in the second set of attributes are associated with the cryptographic key, said one or more attributes in the second set of attributes originating from a key attribute storage of the key management system, and the second set of attributes being different from the first set of attributes;
 - transmit the first sequence of attributes from the attribute frame to the cryptographic coprocessor;
 - in response to transmitting the first sequence of attributes, receive from the cryptographic coprocessor a first message authentication code (MAC) calculated from the first sequence of attributes; and
 - verify the attribute frame by comparing the first MAC or a value derived from the first MAC to a reference value.
2. The key management system according to claim 1, the system being further configured to transmit the one or more attributes from the first sequence of attributes to the cryptographic coprocessor in consecutive calls in order to cause the cryptographic coprocessor to iteratively calculate the first MAC.

3. The key management system according to claim 1, the system further being configured to construct a placeholder MAC field in the attribute frame, and to store the first MAC iteratively calculated by and received from the cryptographic coprocessor in the constructed placeholder MAC field.

4. The key management system according to claim 1, the system further being configured to construct a placeholder cryptographic salt field in the attribute frame, to receive a cryptographic salt generated by the cryptographic coprocessor as an input for calculating the first MAC from the cryptographic coprocessor in response to transmitting the first sequence of attributes, and to store the cryptographic salt in the placeholder cryptographic salt field.

5. The key management system according to claim 1, the system further being configured to serialize the first set of attributes and the second set of attributes into the first sequence of attributes according to a normalization scheme, and to transmit the one or more attributes from the first sequence of attributes to the cryptographic coprocessor according to their order within the first sequence of attributes.

6. The key management system according to claim 5, the normalization scheme being dependent upon properties of the one or more attributes being serialized, the properties being selected from the group consisting of attribute values and attribute types.

7. The key management system according to claim 1, wherein verifying the attribute frame comprises:

- transmitting again the first sequence of attributes from the attribute frame to the cryptographic coprocessor;
- calculating a first cryptographic hash from the first MAC;
- in response to transmitting again the first sequence of attributes, receiving from the cryptographic coprocessor a second cryptographic hash as the reference value; and
- comparing the first cryptographic hash to the second cryptographic hash in order to verify the attribute frame.

8. The key management system according to claim 7, wherein verifying the attribute frame further comprises:
- transmitting again the key identifier to the cryptographic coprocessor;
 - in response to transmitting the key identifier, receiving a third set of attributes from the cryptographic coprocessor, wherein one or more attributes in the third set of attributes are associated with the cryptographic key and originating from the key attribute storage of the cryptographic coprocessor; and
 - validating that a subset of attributes from the first sequence of attributes conforms to the third set of attributes, and, if validation of the subset is not successful, stopping verification of the attribute frame.

9. A computer program product for operating a key management system, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by a processor to cause the processor to:

transmit a key identifier that identifies a cryptographic key to a cryptographic coprocessor;

in response to transmitting the key identifier, receive a first set of attributes from the cryptographic coprocessor, wherein one or more attributes in the first set of attributes are associated with the cryptographic key and originating from a key attribute storage of the cryptographic coprocessor;

serialize the first set of attributes and a second set of attributes into a first sequence of attributes; store the first sequence of attributes within an attribute frame, wherein one or more attributes in the second set of attributes are associated with the cryptographic key, said one or more attributes in the second set of attributes originating from a key attribute storage of the key management system, and the second set of attributes being different from the first set of attributes;

transmit the first sequence of attributes from the attribute frame to the cryptographic coprocessor;

in response to transmitting the first sequence of attributes, receive from the cryptographic coprocessor a first MAC calculated from the first sequence of attributes; and

verify the attribute frame by comparing the first MAC or a value derived from the first MAC to a reference value.

10. The computer program product of claim 9, the program instructions being further configured to transmit the one or more attributes from the first sequence of attributes to the cryptographic coprocessor in consecutive calls in order to cause the cryptographic coprocessor to iteratively calculate the first MAC.

11. The computer program product of claim 9, the program instructions further being configured to construct a placeholder MAC field in the attribute frame, and to store the first

MAC iteratively calculated by and received from the cryptographic coprocessor in the constructed placeholder MAC field.

12. The computer program product of claim 9, the program instructions further being configured to construct a placeholder cryptographic salt field in the attribute frame, to receive a cryptographic salt generated by the cryptographic coprocessor as an input for calculating the first MAC from the cryptographic coprocessor in response to transmitting the first sequence of attributes, and to store the cryptographic salt in the placeholder cryptographic salt field.

13. A method for operating a key management system, the method comprising:
- transmitting a key identifier that identifies a cryptographic key to a cryptographic coprocessor;
 - in response to transmitting the key identifier, receiving a first set of attributes from the cryptographic coprocessor, wherein one or more attributes in the first set of attributes are associated with the cryptographic key and originating from a key attribute storage of the cryptographic coprocessor;
 - serializing the first set of attributes and a second set of attributes into a first sequence of attributes;
 - storing the first sequence of attributes within an attribute frame, wherein one or more attributes from the second set of attributes are associated with the cryptographic key, said one or more attributes in the second set of attributes originating from a key attribute storage of the key management system, and the second set of attributes being different from the first set of attributes;
 - transmitting the first sequence of attributes from the attribute frame to the cryptographic coprocessor;
 - in response to transmitting the first sequence of attributes, receiving from the cryptographic coprocessor a first MAC calculated from the first sequence of attributes; and
 - verifying the attribute frame by comparing the first MAC or a value derived from the first MAC to a reference value.
14. The method of according to claim 13, the method being further configured to transmit the one or more attributes from the first sequence of attributes to the cryptographic coprocessor in consecutive calls in order to cause the cryptographic coprocessor to iteratively calculate the first MAC.
15. The method of according to claim 13, the method further being configured to construct a placeholder MAC field in the attribute frame, and to store the first MAC iteratively calculated by and received from the cryptographic coprocessor in the constructed placeholder MAC field.

16. The method of according to claim 13, the method further being configured to construct a placeholder cryptographic salt field in the attribute frame, to receive a cryptographic salt generated by the cryptographic coprocessor as an input for calculating the first MAC from the cryptographic coprocessor in response to transmitting the first sequence of attributes, and to store the cryptographic salt in the placeholder cryptographic salt field.

17. The method of according to claim 13, the method further being configured to serialize the first set of attributes and the second set of attributes into the first sequence of attributes according to a normalization scheme, and to transmit the one or more attributes from the first sequence of attributes to the cryptographic coprocessor according to their order within the sequence of attributes.

18. The method of according to claim 17, the normalization scheme being dependent upon properties of the one or more attributes being serialized, the properties being selected from the group consisting of attribute values and attribute types.

19. The method of according to claim 13, wherein verifying the attribute frame comprises:
transmitting again the first sequence of attributes from the attribute frame to the cryptographic coprocessor;
calculating a first cryptographic hash from the first MAC;
in response to transmitting again the first sequence of attributes, receiving from the cryptographic coprocessor a second cryptographic hash as the reference value; and
comparing the first cryptographic hash to the second cryptographic hash in order to verify the attribute frame.

20. The method of according to claim 19, wherein verifying the attribute frame further comprises:
transmitting again the key identifier to the cryptographic coprocessor;
in response to transmitting the key identifier, receiving a third set of attributes from the

cryptographic coprocessor, wherein one or more attributes in the third set of attributes are associated with the cryptographic key and originating from the key attribute storage of the cryptographic coprocessor; and

validating that a subset of attributes from the first sequence of attributes conforms to the third set of attributes, and, if validation of the subset is not successful, stopping verification of the attribute frame.