

CLAIMS

1. A computing system, comprising:
a processor; and
a memory coupled to the processor, storing instructions that when executed by the processor, cause the computing system to perform the following operations:
 - receiving a request for protected data from a potentially untrusted requestor associated with a nested TrEE and an attestation statement of a secure kernel, wherein the nested TrEE comprises a trustlet running on top of the secure kernel, wherein the trustlet is associated with a trustlet ID that is based at least in part on at least one of the following: information on which the trustlet is to operate, a user of the trustlet, or a service type associated with at least one of the request or a configuration of the system;
 - encrypting a transfer encryption key with a second encryption key that is included in the attestation statement;
 - retrieving the protected data;
 - encrypting the protected data with the transfer encryption key and an authentication tag, wherein the authentication tag binds the requestor with the trustlet ID; and
 - providing the encrypted transfer encryption key, the encrypted protected data, and encrypted authentication tag to the requestor.
2. The computing system of claim 1, wherein the trustlet ID comprises a trustlet type and a session ID.
3. The computing system of claim 2, wherein the second encryption key comprises a secure kernel encryption key.
4. The computing system of claim 3, wherein a private secure kernel encryption key corresponding to the secure kernel encryption key is required to decrypt the encrypted protected data.
5. The computing system of claim 1, wherein the instructions comprise additional instructions that when executed by the processor, cause the computing system to perform the following operations:
 - comparing the trustlet ID to a list of authorized trustlet IDs; and
 - encrypting the protected data with the transfer encryption key and an authentication tag only if the trustlet ID is associated with the list of authorized trustlet IDs.

6. The computing system of claim 1, wherein the protected data comprises a wrapping key.

67. A method for delivering protected data to a nested trusted execution environment (TrEE) comprising a trustlet running on top of secure kernel, wherein both the trustlet and the secure kernel are associated with a potentially untrusted requestor, the method comprising:

receiving, by at least one processor of a processor-based system, a request for protected data from the potentially untrusted requestor associated with the nested TrEE, and an attestation statement of the secure kernel, and an indication that a second encryption key that is included in the attestation statement is an encryption key of the secure kernel, wherein the trustlet is associated with a trustlet ID; that includes at least one of (a) a service type that is based on at least one of the request or a configuration of the system or (b) an identifier related to at least one of information on which the trustlet is to operate or a user of the trustlet;

encrypting a transfer encryption key with ~~the~~ a second encryption key that is included in the attestation statement;

retrieving, by at least one processor of the processor-based system, the protected data;

encrypting the protected data with the transfer encryption key and an authentication tag, wherein the authentication tag binds the requestor with the trustlet ID; and

providing the encrypted transfer encryption key, the encrypted protected data, and encrypted authentication tag to the requestor.

78. The method of claim 67, wherein the trustlet ID comprises a trustlet type and a session ID.

89. The method of claim 78, wherein providing the encrypted transfer encryption key, the encrypted protected data, and encrypted authentication tag to the requestor comprises:

causing the potentially untrusted requestor to send the encrypted transfer encryption key and the encrypted protected data to the secure kernel, which enables the secure kernel to decrypt the transfer key with a private second encryption key corresponding to the second encryption key and to decrypt the protected data with the decrypted transfer key.

910. The method of claim 89, wherein providing the encrypted transfer

encryption key, the encrypted protected data, and encrypted authentication tag to the requestor comprises:

causing the secure kernel to send the encrypted transfer encryption key and the encrypted protected data to the trustlet, which causes the trustlet to forward the encrypted transfer encryption key and the encrypted protected data to the secure kernel.

~~10~~11. The method of claim ~~8~~9, wherein providing the encrypted transfer encryption key, the encrypted protected data, and encrypted authentication tag to the requestor comprises:

enabling the secure kernel to confirm that the encrypted protected data is for the trustlet based on the trustlet type and the session ID and to send the decrypted protected data to the trustlet based on the trustlet type and the session ID.

~~11~~12. The method of claim ~~6~~7, wherein the protected data comprises a wrapping key.

~~12~~13. The method of claim ~~6~~7, further comprising:

comparing, by at least one processor of the processor-based system, the trustlet ID to a list of authorized trustlet IDs; and

encrypting, by at least one processor of the processor-based system, the protected data with the transfer encryption key and an authentication tag only if the trustlet ID is associated with the list of authorized trustlet IDs.

14. The method of claim 7, wherein the authentication tag binds the requestor with at least one of a trustlet type or a session ID included in the trustlet ID.

~~13~~15. A computer readable storage medium comprising instructions for delivering protected data to a nested trusted execution environment (TrEE) comprising a trustlet running on top of secure kernel, the medium comprising instructions that, when executed on a computer system, cause the computer system to at least:

receive a request for protected data from a potentially untrusted requestor associated with the nested TrEE and an attestation statement of the secure kernel, wherein the trustlet is associated with a trustlet ID;

determine a service type of trustlet to target based on the request or based on a configuration of the system, wherein the trustlet that runs on top of the secure kernel is of the type:

encrypt a transfer encryption key with a second encryption key that is included in the attestation statement;

retrieve the protected data;

encrypt the protected data with the transfer encryption key and an authentication tag, wherein the authentication tag binds the requestor with the trustlet ID; and

provide the encrypted transfer encryption key, the encrypted protected data, and encrypted authentication tag to the requestor.

~~14~~16. The computer readable storage medium of claim ~~13~~15, wherein the trustlet ID comprises a trustlet type and a session ID.

~~15~~17. The computer readable storage medium of claim ~~14~~16, wherein the second encryption key comprises a secure kernel encryption key.

~~16~~18. The computer readable storage medium of claim ~~15~~17, wherein a private secure kernel encryption key corresponding to the secure kernel encryption key is required to decrypt the encrypted protected data.

~~17~~19. The computer readable storage medium of claim ~~13~~15, wherein the protected data comprises a wrapping key.

~~18~~20. The computer readable storage medium of claim ~~13~~15, wherein the instructions further comprise instructions that when executed on the ~~computer~~ computing system, cause the computing system to at least:

compare the trustlet ID to a list of authorized trustlet IDs; and

encrypt the protected data with the transfer encryption key and an authentication tag only if the trustlet ID is associated with the list of authorized trustlet IDs.

~~19. The method of claim 6, wherein the authentication tag binds the requestor with at least one of a trustlet type or a session ID included in the trustlet ID.~~

~~20. The method of claim 6, wherein the trustlet ID includes at least one of (a) a service type that is based on at least one of the request or a configuration of the system or (b) an identifier relating to at least one of information on which the trustlet is to operate or a user of the trustlet.~~