

WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:
 - receiving, from a requesting device, a request to perform an operation, the request being received in a request message comprising an encrypted record and a first dynamic value, the encrypted record comprising a set of one or more entries corresponding to one or more previously performed operations associated with a user of the requesting device;
 - authorizing the request using the encrypted record, a first cryptographic key derived from a unique key associated with an authorizing entity, and a first dynamic value;
 - performing one or more operations based at least in part on the request being authorized;
 - generating a modified encrypted record comprising data associated with the one or more operations performed; and
 - transmitting, to the requesting device, at least the modified encrypted record and an indication that the operation was performed.
2. The computer-implemented method of claim 1, further comprising obtaining a second cryptographic key derived from the unique key associated with the authorizing entity.
3. The computer-implemented method of claim 2, wherein the second cryptographic key is obtained from the request message.
4. The computer-implemented method of claim 2, wherein authorizing the request further comprises:
 - generating a third cryptographic key from the first cryptographic key and the second cryptographic key; and
 - generating a decrypted record from the encrypted record utilizing the third cryptographic key, wherein authorizing the request is based at least in part on the decrypted record.
5. The computer-implemented method of claim 4, wherein authorizing the request further comprises:

aggregating a first set of entries of the decrypted record to generate a first value; and

aggregating a second set of entries of the decrypted record to generate a second value, wherein the request is authorized based at least in part on the first value and the second value.

6. The computer-implemented method of claim 5, wherein authorizing the request is based at least in part on determining that the first value is greater than or equal to a summation of the second value and an amount included in the request message.

7. The computer-implemented method of claim 1, wherein generating the modified encrypted record comprises:

generating a decrypted record from the encrypted record utilizing the first dynamic value;

modifying the decrypted record to include the data indicating the request was authorized;

generating a second dynamic value;

generating a new cryptographic key based at least in part on the second dynamic value and the unique key associated with the authorizing entity; and

encrypting the decrypted record as modified to generate the modified encrypted record, wherein encrypting the decrypted record utilizes the new cryptographic key generated based at least in part on the unique key and the second dynamic value, wherein the second dynamic is transmitted with the modified encrypted record.

8. The computer-implemented method of claim 7, wherein generating the new cryptographic key is further based at least in part on concatenating the first cryptographic key to the new cryptographic key prior to utilizing the new cryptographic key to encrypt the decrypted record.

9. A secure processing computer, comprising:

one or more processors; and

one or more memories storing executable instructions that, when executed by the one or more processors, cause the secure processing computer to perform the computer-implemented method of any of claims 1-8.

10. The secure processing computer of claim 9, wherein the one or more memories comprise a first secure memory space and a second secure memory space.

11. The secure processing computer of claim 10, wherein the first secure memory space stores code that, when executed by the one or more processors, causes the secure processing computer to derive and generate one or more cryptographic keys.

12. The secure processing computer of claim 10, wherein the second secure memory space stores code that, when executed by the one or more processors, causes the secure processing computer to decrypt the encrypted record to generate a decrypted record and perform authorization processing utilizing the decrypted record.

13. An authorizing entity computer, comprising:
one or more processors; and
one or more memories storing executable instructions that, when executed by the one or more processors, cause the authorizing entity computer to:
generate a unique key associated with an authorizing entity;
receive, from a user device, a first request to perform a first operation, the first request being received in a first request message comprising a first cryptographic key derived from the unique key;
perform the first operation based at least in part on the first request;
generate a record corresponding to a user associated with the first request, the record comprising a record entry indicating that the first operation was performed;
generate a second cryptographic key based at least in part on the unique key and a first dynamic value;
generate an encrypted record based at least in part on the record, the first cryptographic key, and the second cryptographic key; and
transmit, to the user device, the encrypted record, the first dynamic value, and an indication that the first operation was performed.

14. The authorizing entity computer of claim 13, wherein the executable instructions, when executed by the one or more processors, further cause the authorizing entity computer to:

receive, from the user device, a second request to perform a second operation, the second request being received in a second request message comprising the first cryptographic key, a subsequent dynamic value, and a subsequent encrypted record, the subsequent encrypted record comprising a set of record entries associated with the user, the set of record entries comprising the record entry;

generate a third cryptographic key based at least in part on the unique key associated with the authorizing entity and the subsequent dynamic key received in the second request message;

generate a decrypted record from the subsequent encrypted record utilizing the first cryptographic key and the third cryptographic key;

perform the second operation based at least in part on the second request; and

modify the decrypted record to include an additional record entry indicating the second operation was performed.

15. The authorizing entity computer of claim 14, wherein the subsequent dynamic value was generated by a secure processing computer, and wherein at least the subsequent dynamic value was utilized by the secure processing computer to generate the subsequent encrypted record.

16. The authorizing entity computer of claim 14, wherein the executable instructions, when executed by the one or more processors, further cause the authorizing entity computer to:

generate a fourth cryptographic key based at least in part on the unique key and a third dynamic value;

generate a newly encrypted record from the decrypted record as modified utilizing the first cryptographic key and the fourth cryptographic key; and

transmit, to the user device, the newly encrypted record, the third dynamic value, and a corresponding indication that the second request was authorized.

17. The authorizing entity computer of claim 16, wherein the first dynamic value and the third dynamic value are generated by the authorizing entity computer.

18. A user device, comprising:
one or more processors; and

one or more memories storing executable instructions that, when executed by the one or more processors, cause the user device to:

store, in the one or more memories, a first cryptographic key associated with an authorizing entity, the first cryptographic key being derived from a unique key associated with the authorizing entity, the unique key being unknown to the user device;

receive user input indicating a first operation is requested;

transmit, to an authorizing entity computer, a first request to perform the first operation, the first request being transmitted in a first request message comprising the first cryptographic key;

receive a first response to the first request, the first response being received in a response message comprising a first encrypted record, an indication that the first operation was performed, and a first dynamic value associated with the first encrypted record;

display data indicating that the first operation was performed; and

store the first encrypted record and the first dynamic value in the one or more memories of the user device.

19. The user device of claim 18, wherein the executable instructions, when executed by the one or more processors, further cause the user device to:

receive additional user input indicating a second operation is requested;

transmit, to an authorization manager component of a secure processing computer, a second request to perform the second operation, the second request being transmitted in a second request message comprising the first cryptographic key, the first encrypted record, and the first dynamic value;

receive a second response to the second request, the second response being received in a second response message comprising a second encrypted record, an additional indication that the second operation was performed, and a second dynamic value associated with the second encrypted record;

display additional data indicating that the second operation was performed; and

replace, in the one or more memories, the first encrypted record with the second encrypted record and the first dynamic value with the second dynamic value.

20. The user device of claim 19, wherein the authorizing entity computer is configured to encrypt the first encrypted record as part of performing the first operation, wherein the authorization manager component is configured to decrypt the first

encrypted record to perform the second operation, and wherein the first encrypted record is decrypted based at least in part on the unique key associated with the authorizing entity and the first dynamic value.