

WHAT IS CLAIMED IS:

1. A computer-implemented method for communicating sensitive data, comprising:
 - receiving, by a user device from an access device, a first message comprising a terminal type indicator, the user device storing 1) a first identifier corresponding to a static account identifier and 2) a second identifier corresponding to a primary account identifier;
 - generating an encrypted identifier based on a portion of the second identifier;
 - in response to the terminal type indicator indicating a first terminal type:
 - transmitting, from the user device to the access device, a request message comprising the first identifier and the encrypted identifier; and
 - in response to the terminal type indicator indicating a second terminal type:
 - generating, by the user device, an obfuscated identifier based at least in part on a first portion of the second identifier and a second portion of the encrypted identifier; and
 - transmitting, from the user device to the access device, the request message comprising the obfuscated identifier and the encrypted identifier.
2. The computer-implemented method of claim 1, further comprising:
 - obtaining, by the user device, a stored counter value, wherein the encrypted identifier is generated further utilizing the stored counter value;
 - generating a modified counter value in response to transmitting the request message; and
 - storing the modified counter value at the user device.
3. The computer-implemented method of claim 2, wherein generating the encrypted identifier further comprises encrypting the second identifier and the modified counter value with a unique derivation key stored at the user device.
4. The computer-implemented method of claim 1, wherein the second portion of the encrypted identifier comprises a right-most seven digits of the encrypted identifier.

5. The computer-implemented method of claim 1, wherein the first portion of the second identifier comprises a left-most eight digits of the second identifier.

6. The computer-implemented method of claim 1, wherein the portion of the second identifier comprises an identification number associated with an acquirer.

7. The computer-implemented method of claim 1, wherein transmitting the request message comprising the first identifier and the encrypted identifier to the access device, causes the access device to:

compare the first identifier to a plurality of stored identifiers;

reject the request message when the first identifier is included in the plurality of stored identifiers, wherein rejecting the request message causes the user device to be denied access to a resource managed by the access device; and

approve the request message when the first identifier is not included in the plurality of stored identifiers, wherein approving the request message causes the user device to be granted access to the resource managed by the access device.

8. The computer-implemented method of claim 1, wherein transmitting the request message comprising the first identifier and the encrypted identifier to the access device, causes the access device to:

generate an authorization request message comprising the first identifier and the encrypted identifier; and

transmit the authorization request message to an authorizing entity computer.

9. The computer-implemented method of claim 8, wherein the authorizing entity computer is configured to:

receive the authorization request message comprising the first identifier and the encrypted identifier;

identify a stored identifier associated with the first identifier;

generate a decrypted identifier from the encrypted identifier;

compare the stored identifier to the decrypted identifier; and

process the authorization request message based at least in part on comparing the stored identifier to the decrypted identifier.

10. The computer-implemented method of claim 1, wherein transmitting the request message comprising the obfuscated identifier and the encrypted identifier to the access device, causes the access device to:

generate an authorization request message comprising the obfuscated identifier and the encrypted identifier; and

transmit the authorization request message to an authorizing entity computer, wherein transmitting the authorization request message comprising the obfuscated identifier and the encrypted identifier causes the authorizing entity computer to derive a derivation key based at least in part on a corresponding portion of the obfuscated identifier, generate a decrypted identifier from the encrypted identifier utilizing the derivation key, and process the authorization request message utilizing the decrypted identifier.

11. A user device, comprising:

one or more processors; and

one or more memories storing computer-executable instructions for communicating sensitive data, wherein executing the computer-executable instructions by the one or more processors, causes the user device to:

receive, from an access device, a first message comprising a terminal type indicator, the user device storing 1) a first identifier corresponding to a static account identifier and 2) a second identifier corresponding to a primary account identifier;

generate an encrypted identifier based on a portion of the second identifier;

in response to the terminal type indicator indicating a first terminal type:

transmit, to the access device, a request message comprising the first identifier and the encrypted identifier; and

in response to the terminal type indicator indicating a second terminal type:

generate an obfuscated identifier based at least in part on a first portion of the second identifier and a second portion of the encrypted identifier; and

transmit, to the access device, the request message comprising the obfuscated identifier and the encrypted identifier.

12. The user device of claim 11, wherein executing the computer-executable instructions by the one or more processors, further causes the user device to:
obtain a stored counter value, wherein the encrypted identifier is generated further utilizing the stored counter value;
generate a modified counter value in response to transmitting the request message; and
store the modified counter value at the user device.

13. The user device of claim 12, wherein generating the encrypted identifier further comprises encrypting the second identifier and the modified counter value with a unique derivation key stored at the user device.

14. The user device of claim 11, wherein the second portion of the encrypted identifier comprises a right-most seven digits of the encrypted identifier.

15. The user device of claim 11, wherein the first portion of the second identifier comprises a left-most eight digits of the second identifier.

16. The user device of claim 11, wherein the portion of the second identifier comprises an identification number associated with an acquirer.

17. The user device of claim 11, wherein transmitting the request message comprising the first identifier and the encrypted identifier to the access device, causes the access device to:

compare the first identifier to a plurality of stored identifiers;
reject the request message when the first identifier is included in the plurality of stored identifiers, wherein rejecting the request message causes the user device to be denied access to a resource managed by the access device; and
approve the request message when the first identifier is not included in the plurality of stored identifiers, wherein approving the request message causes the user device to be granted access to the resource managed by the access device.

18. The user device of claim 11, wherein transmitting the request message comprising the first identifier and the encrypted identifier to the access device, causes the access device to:

generate an authorization request message comprising the first identifier and the encrypted identifier; and
transmit the authorization request message to an authorizing entity computer.

19. The user device of claim 18, wherein the authorizing entity computer is configured to:

receive the authorization request message comprising the first identifier and the encrypted identifier;
identify a stored identifier associated with the first identifier;
generate a decrypted identifier from the encrypted identifier;
compare the stored identifier to the decrypted identifier; and
process the authorization request message based at least in part on comparing the stored identifier to the decrypted identifier.

20. The user device of claim 11, wherein transmitting the request message comprising the obfuscated identifier and the encrypted identifier to the access device, causes the access device to:

generate an authorization request message comprising the obfuscated identifier and the encrypted identifier; and
transmit the authorization request message to an authorizing entity computer, wherein transmitting the authorization request message comprising the obfuscated identifier and the encrypted identifier causes the authorizing entity computer to derive a derivation key based at least in part on a corresponding portion of the obfuscated identifier, generate a decrypted identifier from the encrypted identifier utilizing the derivation key, and process the authorization request message utilizing the decrypted identifier.