WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

obtaining, by a device, a unique derivation key;

obtaining, by the device, a dynamic value;

generating, by the device, an encrypted value by encrypting an identifier and the dynamic value using the unique derivation key;

generating, by the device, an obfuscated identifier based at least in part on a portion of the identifier and a portion of the encrypted value; and

providing, by the device, a message comprising at least the obfuscated identifier and the encrypted value to an access device, causing the access device to generate an authorization request message comprising a first data field comprising the obfuscated identifier and a second data field comprising the encrypted value for transmission to a central server computer for further authorization processing.

2. The computer-implemented method of claim 1, further comprising:

generating a modified counter value in response to providing the message comprising at least the obfuscated identifier and the encrypted value; and

storing the modified counter value.

3. The computer-implemented method of claim 2, further comprising:

generating, by the device, a subsequent encrypted identifier utilizing the identifier, the modified counter value, and the unique derivation key;

storing, by the device, the subsequent encrypted identifier;

generating, by the device, a subsequent obfuscated identifier based at least in part on a portion of the identifier and a portion of the subsequent encrypted identifier; and

providing, by the device, a subsequent message comprising at least the subsequent obfuscated identifier and the subsequent encrypted identifier.

4. The computer-implemented method of claim 1, wherein the portion of the encrypted value comprises a right-most seven digits of the encrypted value.

5. The computer-implemented method of claim 1, wherein the dynamic value and the identifier are concatenated prior to generating the encrypted value.

6. The computer-implemented method of claim 1, wherein the dynamic value comprises at least one of: a counter, a date, a time, or a transaction value.

7. The computer-implemented method of claim 1, wherein providing the message causes a central server computer to perform operations comprising:

determining that the encrypted value is present in the message;

deriving the unique derivation key utilizing a master derivation key and a portion of the obfuscated identifier;

generating a decrypted value from the encrypted value of the message utilizing the unique derivation key;

modifying the message to include the decrypted value; and

transmitting the modified message to an authorization computer for authorization.

8. The computer-implemented method of claim 1, further comprising calculating a Luhn checksum value based at least in part on obfuscated identifier, wherein the message further comprises the Luhn checksum value.

9. The computer-implemented method of claim 1, wherein the message is provided in response to a transaction initiated with the device.

10. The computer-implemented method of claim 1, wherein the unique derivation key obtained is derived during a personalization process associated with the device.

11. A computing device, comprising:

one or more processors; and

one or more memories storing computer-executable instructions, wherein executing the computer-executable instructions by the one or more processors, causes the computing device to:

obtain a unique derivation key;

obtain a dynamic value;

generate an encrypted value by encrypting an identifier and the dynamic value using the unique derivation key;

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

provide a message comprising at least the obfuscated identifier and the encrypted value to an access device, causing the access device to generate an authorization request message comprising a first data field comprising the obfuscated

identifier and a second data field comprising the encrypted value for transmission to a central server computer for further authorization processing.

12. The computing device of claim 11, wherein the computing device is further configured to:

generate a modified counter value in response to providing the message comprising at least the obfuscated identifier and the encrypted value; and

store the modified counter value.

13. The computing device of claim 12, wherein the computing device is further configured to:

generate a subsequent encrypted identifier utilizing the identifier, the modified counter value, and the unique derivation key;

store the subsequent encrypted identifier;

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

provide a subsequent message comprising at least the subsequent obfuscated identifier and the subsequent encrypted identifier.

14. The computing device of claim 11, wherein the portion of the encrypted value comprises a right-most seven digits of the encrypted value.

15. The computing device of claim 11, wherein the dynamic value and the identifier are concatenated prior to generating the encrypted value.

16. The computing device of claim 11, wherein the dynamic value comprises at least one of: a counter, a date, a time, or a transaction value.

17. The computing device of claim 11, wherein providing the message causes a central server computer to perform operations comprising:

determining that the encrypted value is present in the message;

deriving the unique derivation key utilizing a master derivation key and a portion of the obfuscated identifier;

generating a decrypted value from the encrypted value of the message utilizing the unique derivation key;

modifying the message to include the decrypted value; and

transmitting the modified message to an authorization computer for authorization.

18. The computing device of claim 11, wherein the computing device is further configured to calculate a Luhn checksum value based at least in part on obfuscated identifier, wherein the message further comprises the Luhn checksum value.

19. The computing device of claim 11, wherein the message is provided in response to a transaction initiated with the computing device.

20. The computing device of claim 11, wherein the unique derivation key obtained is derived during a personalization process associated with the computing device.