WHAT IS CLAIMED IS:

1. A method comprising:

storing, by a user device, a message data template comprising data fields for a counter value, a cryptogram, and a credential, the message data template being used to form a multi-record message;

initiating, by the user device, an interaction with an access device;

incrementing, by the user device, a counter on the user device to produce the counter value;

generating, by the user device, the cryptogram, wherein the cryptogram comprises a dynamic cryptogram, and wherein said generating comprises encrypting the counter value using a cryptographic key and a cryptogram generating algorithm to form the dynamic cryptogram;

incorporating, by the user device, i) the counter value, ii) the dynamic cryptogram and iii) the credential into the data fields of the message data template to form a multi-record message; and

transmitting, by the user device, the multi-record message to the access device.

2. The method of claim 1, wherein the multi-record message is an NDEF message.

3. The method of claim 2, wherein the multi-record message comprises a plurality of records, and the plurality of records include a first record for the credential, a second record for the cryptogram, and a third record for the counter.

4. The method of claim 1, wherein the credential is a token or a PAN.

5. The method of claim 1, wherein the access device is a phone.

6. The method of claim 1, wherein the interaction includes a request for access to a resource or to a secure location.

7. The method of claim 1, wherein the message data template is generated by an authorization computer.

8. The method of claim 1, wherein the message data template is generated by a third-party associated with an authorization computer.

9. The method of claim 8, wherein the authorization computer is an issuer computer.

10. The method of claim 1, wherein the multi-record message is a base64 string.

11. A user device comprising:

a processor, and a computer readable medium comprising code executable by the processor for performing a method comprising:

storing a message data template comprising data fields for a counter value, a cryptogram, and a credential, the message data template being used to form a multi-record message;

initiating an interaction with an access device;

incrementing a counter on the user device to produce the counter value;

generating the cryptogram, wherein the cryptogram comprises a dynamic cryptogram, and wherein said generating comprises encrypting the counter value using a cryptographic key and a cryptogram generating algorithm to form the dynamic cryptogram;

incorporating the counter value, the dynamic cryptogram and the credential into the data fields of the message data template to form a multi-record message; and

transmitting the multi-record message to the access device.

12. The user device of claim 11, wherein the message data template is stored on a NFC tag element.

13. The user device of claim 12, wherein the NFC tag element is a NFC Type 4 Tag.

14. The user device of claim 11, wherein the user device is a phone.

15. The user device of claim 11, wherein the user device is an access card.

16. The user device of claim 11, wherein the cryptogram is generated using a secret cryptographic key and cryptogram generating algorithm.

17. The user device of claim 16, wherein the cryptogram generating algorithm is 3DES or AES.

18. The user device of claim 16, wherein the secret cryptographic key is provided to the user device by an authorization computer.

19. The user device of claim 11, wherein the credential may be retrieved from a secure element of the user device.

20. A method comprising:

initiating, by an access device, communication with a user device;

receiving, by the access device, a multi-record message from the user device, wherein the multi-record message comprises at least a counter value, a cryptogram and a credential, wherein the cryptogram comprises a dynamic cryptogram, and wherein the dynamic cryptogram is generated by encrypting the counter value using a cryptographic key and a cryptogram generating algorithm to form the dynamic cryptogram;

extracting, by the access device, i) the counter value, ii) the dynamic cryptogram, and iii) the credential from the multi-record message;

generating, by the access device, an authorization request message, wherein the authorization request message comprises at least the extracted counter value, cryptogram, and credential;

transmitting, by the access device, the authorization request message to an authorization computer; and

receiving, by the access device, an authorization response message from the authorization computer.