WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a security device in a transaction, a biometric sample from a user;

transmitting, by the security device, the biometric sample of the user or a biometric template thereof to a service provider computer, wherein the service provider computer matches the biometric sample or the biometric template to a user account;

upon matching the biometric sample or the biometric template to the user account, receiving, by the security device, access credential data comprising a payment token and supplemental information associated with the user account, wherein the payment token is a substitute for a real credential associated with the user account;

outputting, by a display on the security device, an indication that the match is present and at least a portion of the supplemental information, wherein the supplemental information is user-related information which is supplemental to payment account data;

generating, by the security device, an interaction cryptogram; and

after a resource provider reviews and verifies the displayed supplemental information, transmitting, by the security device, the access credential data and the interaction cryptogram to an access device in communication with the security device, such that the access device is caused to generate an authorization request message and transmit the authorization request message to an authorization provider for authorization for the transaction.

2. The method of claim 1, wherein the supplemental information relates to an age of the user.

3. The method of claim 1, wherein the supplemental information relates to a level of access for the user.

4. The method of claim 1, wherein the access credential data further comprises a cryptographic key.

5. The method of claim 4, wherein the cryptographic key is a limited use key.

6. The method of claim 1, wherein the access device, upon receiving authorization, is caused to provide instructions to an access gate, the instructions causing the access gate to grant the user access to a secure area.

7. The method of claim 1, wherein at least a portion of the supplemental information associated with the user account is used to determine whether the transaction is to be authorized.

8. The method of claim 1, further comprising deleting, from the security device, the access credential data within a predetermined period of time after transmitting the access credential data to the access device.

9. The method of claim 1, wherein the security device is in wireless communication with the access device.

10. A security device comprising:

a processor, a display coupled to the processor, and

a memory including instructions that, when executed with the processor, cause the security device to, at least:

receive, in a transaction, a biometric sample from a user;

transmit the biometric sample of the user or a biometric template thereof to a service provider computer, wherein the service provider computer matches the biometric sample to a user account;

upon matching the biometric sample or the biometric template to the user account, receive access credential data comprising a payment token and supplemental information associated with the user account, wherein the payment token is a substitute for a real credential associated with the user account;

output on the display an indication that the match is present and at least a portion of the supplemental information, wherein the supplemental

information is user-related information which is supplemental to payment account data;

generate an interaction cryptogram; and

after a resource provider reviews and verifies the displayed supplemental information, transmit the access credential data and the interaction cryptogram to an access device in communication with the security device, such that the access device is caused to generate an authorization request message and transmit the authorization request message to an authorization provider for authorization for the transaction.

11. The security device of claim 10, wherein the instructions further cause the security device to receive transaction data from the access device, and wherein the interaction cryptogram is generated in response to receiving the transaction data.

12. The security device of claim 11, wherein the interaction cryptogram is formed based on encrypting a portion of the transaction data received from the access device using a cryptographic key.

13. The security device of claim 12, wherein the portion of the transaction data received from the access device comprises at least one of a transaction amount, terminal identifier, or unpredictable number.

14. The security device of claim 11, wherein the transaction data received from the access device comprises one or more conditions of completing a transaction.

15. The security device of claim 14, wherein the instructions further cause the security device to determine, based on the supplemental information associated with the user account, whether the one or more conditions of completing the transaction are met.

16. The security device of claim 15, wherein upon determining the one or more conditions of completing the transaction are not met, the transaction is declined.

17. The security device of claim 10, wherein the biometric sample received from the user comprises facial data, fingerprint data, or voice data.