WHAT IS CLAIMED IS:

1. A method comprising:

obtaining, by a mobile device, a second biometric sample of a user;

generating a second biometric template from the second biometric sample;

generating a first secret cryptographic key and a public value by passing the second biometric template to a first function of a fuzzy extractor;

transmitting the public value to an access device;

receiving, from the access device, a plurality of encrypted first biometric templates, each of the plurality of encrypted first biometric templates being encrypted with a respective secret cryptographic key;

attempting to decrypt a first one of the plurality of encrypted first biometric templates with the first secret cryptographic key;

responsive to failure to decrypt the first one of the plurality of encrypted first biometric templates, attempting to decrypt a next one of the plurality of encrypted biometric templates;

responsive to decrypting the next one of the plurality of encrypted first biometric templates thereby indicating that the next one of the plurality of encrypted biometric templates is encrypted with a secret cryptographic key generated by passing the public value and a first biometric template which is generated by the access device from a first biometric sample on the access device to a second function of the fuzzy extractor, determining whether the first biometric template matches the second biometric template; and

responsive to determining that the first biometric template matches the second biometric template, sending a confirmation of the match to the access device.

2. The method of claim 1,

wherein generating the first biometric template from the first biometric sample comprises generating a first small biometric template and a first large biometric template;

wherein generating the second biometric template from the second biometric sample comprises generating a second small biometric template and a second large biometric template;

wherein generating the public value comprises passing the second small biometric template to the first function of the fuzzy extractor;

wherein the secret cryptographic key is generated by passing the first small biometric template and the public value of the mobile device to the second function of the fuzzy extractor;

wherein the access device encrypts the first biometric template with the secret cryptographic key by encrypting the first large biometric template with the secret cryptographic key; and

wherein the match is between the first large biometric template and the second large biometric template.

3. The method of claim 2, wherein the first small biometric template is one of:

an obfuscated copy of the first large biometric template; and

an incomplete copy of the first large biometric template.

4. The method of claim 2, wherein the first large biometric template and the first small biometric template are generated from the first biometric sample by:

extracting one or more distinct characteristics from the first biometric sample; and

generating digital reference of the one or more distinct characteristics.

5. The method of claim 1, wherein the access device is a point of sale terminal.

6. The method of claim 1, wherein the mobile device is a mobile phone.

7. The method of claim 2, wherein a similarity between the first small biometric template and the small biometric template of the mobile device exceeds a threshold matching score.

8. The method of claim 2, further comprising:
receiving a transmitting station identifier at the mobile device from a transmitting station.

9. The method of claim 2 wherein obtaining the second biometric sample of the user comprises one of:
taking a photographic image of the user's face;
taking a fingerprint of the user;
taking a voice sample of the user;
taking a DNA sample of the user;
taking a retinal scan of the user; and
taking a hair sample of the user.

10. The method of claim 1, wherein the first biometric template is encrypted along with a resource provider identifier and a nonce.

11. The method of claim 1, wherein the public value is a public key.

12. The method of claim 1, wherein the confirmation comprises a payment message that comprises an amount, a resource provider identifier and a primary account number.

13. The method of claim 12, wherein the payment message is signed by the first secret cryptographic key.

14. The method of claim 12, wherein the access device broadcasts the encrypted first biometric template to a plurality of mobile devices in the vicinity of the access device.

15. A mobile device comprising:
a processor; and
a computer readable medium coupled to the processor, the computer readable medium comprising code executable by the processor for implementing a method according to any of claims 1-14.