CLAIMS

What is claimed is:

1. An apparatus to perform multifactor authentication persistence comprising:

memory configured to store instructions;

one or more processors configured to execute the stored instructions that, when executed, cause the one or more processors to:

perform multifactor authentication, wherein one factor of the multifactor authentication includes establishing a short-range wireless communication with a contactless card, receiving data from the contactless card, sending the data to a system to authenticate, and receiving an indication that the contactless card is authentic;

determine a snapshot of the apparatus at a first time;

perform device fingerprinting on the apparatus at a second time;

compare the fingerprinting to the snapshot to determine whether the fingerprinting meets a predetermined requirement;

allow the multifactor authentication to persist for a predetermined time period if the fingerprinting meets the predetermined requirement; and

reauthenticate a user if a fingerprint does not meet the predetermined requirement.

2. The apparatus of claim 1, wherein the data is comprised in a message generated by the contactless card applying a first session key to a shared secret to generate encrypted data and applying a second session key to the encrypted data and a random number to generate the message.

3. The apparatus of claim 1 or claim 2, wherein another factor of the multifactor authentication comprises an identifier and a password for an application, a biometric input, a passcode, or a personal identification number (PIN).

4. The apparatus of any one of claims 1 to 3, wherein the snapshot comprises one or more device settings, one or more biometric inputs, or a combination thereof.

5. The apparatus of any one of claims 1 to 4, wherein the instructions are further configured to cause the one or more processors to perform a stability check prior to the performance of the fingerprinting.

6. The apparatus of claim 5, wherein the stability check is a mobile network operator (MNO) verification.

7. The apparatus of any one of claims 1 to 6, wherein the fingerprinting comprises one or more device settings, one or more biometric inputs, or a combination thereof.

8. The apparatus of any one of claims 1 to 7, wherein the predetermined requirement is an allowed amount change between the snapshot and the fingerprint.

9. A computer-implemented method comprising:

performing multifactor authentication, wherein one factor includes authenticating via data received from a contactless card;

determining a snapshot of an apparatus at a first time;

performing device fingerprinting on the apparatus at a second time;

comparing the fingerprinting to the snapshot to determine whether the fingerprinting meets a predetermined requirement;

allowing the multifactor authentication to persist for a predetermined time period if the fingerprinting meets the predetermined requirement; and

reauthenticating a user if a fingerprint does not meet the predetermined requirement.

10. The computer-implemented method of claim 9, wherein the data is comprised in a message generated by the contactless card applying a first session key to a shared secret to generate a message access code (MAC) cryptogram and applying a second session key to the MAC cryptogram and a random number to generate the message.

11. The computer-implemented method of claim 9 or claim 10, wherein another factor of the multifactor authentication comprises an identifier and a password for an application, a biometric input, a passcode, or a personal identification number (PIN).

12. The computer-implemented method of any one of claims 9 to 11, wherein the snapshot comprises one or more device settings, one or more biometric inputs, or a combination thereof.

13. The computer-implemented method of any one of claims 9 to 12, comprising performing a stability check before the performance of the fingerprinting.

14. The computer-implemented method of claim 13, wherein the stability check is a mobile network operator (MNO) verification.

15. The computer-implemented method of any one of claims 9 to 14, wherein the fingerprinting comprises one or more device settings, one or more biometric inputs, or a combination thereof.

16. The computer-implemented method of any one of claims 9 to 15, wherein the predetermined requirement is an allowed amount change between the snapshot and the fingerprint.

17. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a computer, cause the computer to:

perform multifactor authentication, wherein one factor includes:

receive data from a contactless card,

send the data to a system to authenticate, and

receive an indication that the contactless card is authentic;

determine a snapshot of an apparatus at a first time;

perform device fingerprinting on the apparatus at a second time;

compare the fingerprinting to the snapshot to determine whether the fingerprinting meets a predetermined requirement;

allow the multifactor authentication to persist for a predetermined time period if the fingerprinting meets the predetermined requirement; and

reauthenticate a user if a fingerprint does not meet the predetermined requirement.

18. The computer-readable storage medium of claim 17, wherein the data is comprised in a message generated by the contactless card apply a first session key to a shared secret to generate a message access code (MAC) cryptogram and applying a second session key to the MAC cryptogram and a random number to generate the message.

19. The computer-readable storage medium of claim 17 or claim 18, wherein the instructions are further configured to cause the computer to perform a stability check before the performance of the fingerprinting.

20. The computer-readable storage medium of claim 19, wherein the stability check is a mobile network operator (MNO) verification.