CLAIMS

What is claimed is:

1. An apparatus to perform multifactor authentication persistence comprising:

~~a near-field communication (NFC) reader;~~

memory configured to store instructions;

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

~~authenticate a user via first factor authentication;~~

~~authenticate the user via second factor authentication different from the first factor~~ perform multifactor authentication, wherein ~~the second~~one factor of the multifactor authentication ~~comprises:~~includes establishing a short-range wireless communication with a contactless card ~~being tapped to the apparatus such that NFC communication is established~~, receiving ~~user authentication information~~data from the contactless card ~~via the NFC reader~~, sending the ~~user authentication information~~data to a system to ~~one or more remote computing devices~~authenticate, and receiving an indication ~~from the one or more remote computing devices~~ that the ~~user~~contactless card is ~~authenticated~~authentic;

determine ~~one or more device settings~~a snapshot of the apparatus ~~and one or more user behavioral biometrics~~ at a first time ~~of the second factor authentication~~;

~~cause a stability check on the apparatus to be performed: (i) at a second time after the first time or (ii) when a authentication event occurs after the first time;~~

~~in response to the apparatus being stable,~~ perform device fingerprinting on the apparatus at a second time;

compare the fingerprinting to the snapshot to determine whether the ~~apparatus is within~~fingerprinting meets a predetermined ~~drift threshold~~requirement;

~~in response to the apparatus being within the predetermined drift threshold,~~ allow the ~~second factor~~multifactor authentication to persist for a predetermined time period if the fingerprinting meets the predetermined requirement; and

~~in response to the apparatus not being within the predetermined drift threshold,~~ reauthenticate ~~the~~a user ~~via the second factor authentication.~~ if a fingerprint does not meet the predetermined requirement.

2. ~~The apparatus of claim 1, wherein the one or more device settings includes: (i) one or more applications installed on the apparatus, (ii) one or more wireless devices connected to the apparatus via wireless connection, (iii) a list of saved wireless devices connectable to the apparatus, (iv) a network that the apparatus is connected to, (v) a list of saved networks the apparatus is connectable to, (vi) version of an operating system on the apparatus, and/or~~

~~(vii) one or more setting preferences.~~ 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 ~~the determination~~another factor of the ~~one or more user behavioral biometrics~~multifactor authentication comprises ~~the one or more processors to:~~

~~receive, via one or more sensors or one or more interfaces, user behavioral data,~~an identifier and ~~determine based on the user behavioral data: (i) how the user physically holds the apparatus, (ii) how the user swipes or interacts with~~ a ~~display interface, (iii) how the user uses keyboard or gestural shortcuts, (iv) how the user types words, (v) a duration of time~~password for ~~the user to type words, (vi) how the user transitions between two or more icons, (vii) typing speed of user, and/or (viii) typing cadence of user.~~ 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 ~~stability check on the apparatus comprises~~ 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.

~~5. The apparatus of claim 1, wherein the one or more device settings of the apparatus and the one or more user behavioral biometrics associated with the apparatus are unique to the user at the first time of the second factor authentication,~~

~~wherein the device fingerprinting captures a current constellation of the one or more device settings of the apparatus and the one or more user behavioral biometrics associated with the apparatus at a third time of the device fingerprinting, and~~

~~wherein the predetermined drift threshold is a threshold deviation limit of the one or more device settings and the one or more user behavioral biometrics from the first time of the second factor authentication to the third time of the device fingerprinting.~~

~~6.~~ 7. The apparatus of any one of claims 1 to 6, wherein the ~~one or more processors are further caused to, in response to the apparatus not being stable, reauthenticate the user via both the first and second factor authentications~~fingerprinting comprises one or more device settings, one or more biometric inputs, or a combination thereof.

~~7. The apparatus of claim 1, wherein the one or more processors are further caused to: determine a risk level of a user action to be processed or performed; and process or perform the user action, and wherein the predetermined drift threshold is at least dependent on the risk level of the user action.~~

8. ~~A~~ 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:

~~authenticating, via one or more processors, a user based on first factor authentication; authenticating, via the one or more processors, the user based on second factor authentication different from the first factor authentication, wherein the second factor authentication comprises: a contactless card being tapped to an apparatus such that near field communication (NFC) is established, receiving user authentication information from the contactless card via an NFC reader, sending the user authentication information to one or more remote computing devices, and receiving indication from the one or more remote computing devices that the user is authenticated;~~

~~determining, via the one or more processors, one or more device settings of the apparatus and one or more user behavioral biometrics at a first time of the second factor authentication; causing, via the one or more processors, a stability check on the apparatus to be performed: (i) at a second time after the first time or (ii) when a authentication event occurs after the first time;~~

performing~~,~~ multifactor authentication, wherein one factor includes authenticating via ~~the one or more processors,~~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 ~~apparatus is within~~fingerprinting meets a predetermined ~~drift threshold in response to the apparatus being stable~~requirement;

allowing~~, via~~ the ~~one or more processors, the second factor~~multifactor authentication to persist for a predetermined time period ~~in response to the apparatus being within~~if the fingerprinting meets the predetermined requirement; and

reauthenticating a user if a fingerprint does not meet the predetermined ~~drift threshold; and~~requirement.

~~10. reauthenticating, via the one or more processors, the user based on the second factor authentication in response to the apparatus not being within the predetermined drift threshold.~~

~~9. The method of claim 8, wherein the one or more device settings includes: (i) one or more applications installed on the apparatus, (ii) one or more wireless devices connected to the apparatus via wireless connection, (iii) a list of saved wireless devices connectable to the apparatus, (iv) a network that the apparatus is connected to, (v) a list of saved networks the apparatus is connectable to, (vi) version of an operating system on the apparatus, and/or (vii) one or more setting preferences.~~

~~10. The~~ 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 ~~8, wherein the determining of the one or more user behavioral biometrics further comprises:~~

~~receiving, via one or more sensors or one or more interfaces, user behavioral data, and~~

~~determining, via the one or more processors, based on the user behavioral data: (i) how the user physically holds the apparatus, (ii) how the user swipes or interacts with a display interface, (iii) how the user uses keyboard or gestural shortcuts, (iv) how the user types words, (v) a duration of time for the user to type words, (vi) how the user transitions between two or more icons, (vii) typing speed of user, and/or (viii) typing cadence of user.~~

~~11. The method of claim 8, wherein the~~9 to 12, comprising performing a stability check ~~on~~before the ~~apparatus comprises~~performance of the fingerprinting.

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

~~12.~~ 15. The computer-implemented method of any one of claims ~~8~~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 ~~the~~an apparatus ~~and the one or more user behavioral biometrics associated with the apparatus are unique to the user~~ at ~~the~~a first time ~~of the second factor authentication,~~;

~~wherein the~~perform device fingerprinting ~~captures a current constellation of the one or more device settings of the apparatus and the one or more user behavioral biometrics associated with~~on the apparatus at a ~~third~~second time ~~of the device fingerprinting, and~~;

~~wherein the predetermined drift threshold is a threshold deviation limit of the one or more device settings and the one or more user behavioral biometrics from the first time of the second factor authentication to the third time of the device~~ compare the fingerprinting~~.~~

~~13. The method of claim 8, further comprising reauthenticating, via the one or more processors, the user based on both the first and second factor authentications in response to the apparatus not being stable.~~

~~14. The method of claim 8, further comprising:~~

~~determining, via the one or more processors, a risk level of a user action to be processed or performed; and~~

~~processing or performing, via the one or more processors, the user action, and~~

~~wherein the predetermined drift threshold is at least dependent on the risk level of the user action.~~

~~15. At least one non-transitory computer readable storage medium storing computer readable program code executable by at least one processor to:~~

~~authenticate a user via first factor authentication;~~

~~authenticate the user via second factor authentication different from the first factor authentication, wherein the second factor authentication comprises: a contactless card being tapped to an apparatus such that near field communication (NFC) is established, receiving user authentication information from the contactless card via an NFC reader, sending the user authentication information to one or more remote computing devices, and receiving indication from the one or more remote computing devices that the user is authenticated;~~

~~determine one or more device settings of the apparatus and one or more user behavioral biometrics at a first time of the second factor authentication;~~

~~cause a stability check on the apparatus to be performed: (i) at a second time after the first time or (ii) when a authentication event occurs after the first time;~~

~~in response to the apparatus being stable, perform device fingerprinting on the apparatus~~ to the snapshot to determine whether the ~~apparatus is within~~fingerprinting meets a predetermined ~~drift threshold~~requirement;

~~in response to the apparatus being within the predetermined drift threshold,~~ allow the ~~second factor~~multifactor authentication to persist for a predetermined time period if the fingerprinting meets the predetermined requirement; and

~~in response to the apparatus not being within the predetermined drift threshold,~~ reauthenticate ~~the~~a user ~~via the second factor authentication.~~ if a fingerprint does not meet the predetermined requirement.

~~16. The at least one non-transitory computer readable storage medium of claim 15, wherein the one or more device settings includes: (i) one or more applications installed on the apparatus, (ii) one or more wireless devices connected to the apparatus via wireless connection, (iii) a list of saved wireless devices connectable to the apparatus, (iv) a network that the apparatus is connected to, (v) a list of saved networks the apparatus is connectable to, (vi) version of an operating system on the apparatus, and/or (vii) one or more setting preferences.~~

~~17. The at least one non-transitory computer-readable storage medium of claim 15, wherein the determination of the one or more user behavioral biometrics comprises the computer-readable program code to cause the one or more processors to:~~

~~receive, via one or more sensors or one or more interfaces, user behavioral data, and~~

~~determine based on the user behavioral data: (i) how the user physically holds the apparatus, (ii) how the user swipes or interacts with a display interface, (iii) how the user uses keyboard or gestural shorteuts, (iv) how the user types words, (v) a duration of time for the user to type words, (vi) how the user transitions between two or more icons, (vii) typing speed of user, and/or (viii) typing cadence of user.~~

~~18. The at least one non-transitory computer-readable storage medium of claim 15, wherein the stability check on the apparatus comprises a mobile network operator (MNO) verification.~~

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 at least one non-transitory~~The computer-readable storage medium of claim ~~15,~~ ~~wherein the one or more device settings of the apparatus and the one or more user behavioral biometrics associated with the apparatus are unique to the user at the first time of the second factor authentication,~~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.

~~wherein the device fingerprinting captures a current constellation of the one or more device settings of the apparatus and the one or more user behavioral biometrics associated with the apparatus at a third time of the device fingerprinting, and~~

~~wherein the predetermined drift threshold is a threshold deviation limit of the one or more device settings and the one or more user behavioral biometrics from the first time of the second factor authentication to the third time of the device fingerprinting.~~

20. ~~The at least one non-transitory~~The computer-readable storage medium of claim ~~15,~~ ~~wherein the computer-readable program code causes the one or more processors to, in response to the apparatus not being stable, reauthenticate the user via both the first and second factor authentications.~~ 19, wherein the stability check is a mobile network operator (MNO) verification.