

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, by a user device, an encrypted message from a back-end
3 server computer, the encrypted message being a message encrypted by the back-
4 end server computer with a master secret key or a key derived from the master
5 secret key;
6 signing, by the user device, using a secure element, the encrypted
7 message with a secure element private key to obtain a signed encrypted message;
8 cryptographically recovering, by the user device, using a whitebox, a
9 secure element public key from a certified key using a back-end server computer
10 public key, the certified key being certified by the back-end server computer and
11 based on at least the secure element public key, and wherein the whitebox also
12 stores the master secret key or the key derived from the master secret key;
13 cryptographically recovering, by the user device, using the whitebox,
14 the encrypted message from the signed encrypted message using the secure
15 element public key; and
16 decrypting, by the user device, using the whitebox, the encrypted
17 message using the master secret key or the key derived from the master secret key
18 in the whitebox to obtain the message.
- 1 2. The method of claim 1 further comprising:
2 installing, by the user device, an application comprising the whitebox
3 onto the user device, wherein the whitebox securely includes the master secret key
4 and the back-end server computer public key;
5 generating, by the user device, using the secure element on the user
6 device, the secure element public key and the secure element private key;
7 transmitting, by the user device, an enrollment message including the
8 secure element public key to the back-end server computer associated with the
9 application, wherein the back-end server computer signs the secure element public
10 key with a back-end server computer private key to form the certified key, encrypts
11 the message with the master secret key or the key derived from the master secret
12 key to obtain the encrypted message, and provides the encrypted message to the
13 user device; and

14 receiving, by the user device, the certified key from the back-end
15 server computer.

1 3. The method of claim 2 further comprising:
2 prior to transmitting the enrollment message, obtaining, by the user
3 device, using the secure element on the user device, a user identifier, and wherein
4 transmitting the enrollment message further comprises:
5 transmitting, by the user device, the enrollment message to the
6 back-end server computer, wherein the enrollment message includes the
7 secure element public key and the user identifier, wherein the back-end
8 server computer signs a combination of the secure element public key and the
9 user identifier with the back-end server computer private key to form the
10 certified key, encrypts the message with the master secret key or the key
11 derived from the master secret key to obtain the encrypted message, and
12 provides the encrypted message to the user device.

1 4. The method of claim 3, wherein the user identifier is an
2 enrollment user identifier, wherein the certified key is signed secure element
3 identification data, and wherein signing the encrypted message further comprises:
4 determining, by the user device, using the secure element, an
5 authentication message using the encrypted message and an authentication
6 user identifier; and
7 signing, by the user device, using the secure element, the
8 authentication message with the secure element private key to form a signed
9 authentication message,
10 wherein cryptographically recovering the secure element public key
11 from the certified key comprises:
12 cryptographically recovering, by the user device, using the
13 whitebox, the secure element identification data from the certified key;
14 obtaining, by the user device, using the whitebox, the secure
15 element public key and the enrollment user identifier; and
16 wherein cryptographically recovering the encrypted message from the
17 signed encrypted message comprises:

18 cryptographically recovering, by the user device, using the
19 whitebox, the authentication message from the signed authentication
20 message; and
21 obtaining, by the user device, using the whitebox, the encrypted
22 message and the authentication user identifier from the authentication
23 message; and
24 wherein decrypting the encrypted message comprises:
25 comparing, by the user device, using the whitebox, the
26 authentication user identifier to the enrollment user identifier;
27 if the authentication user identifier and the enrollment user
28 identifier match, generating, by the user device, using the whitebox, the key
29 derived from the master secret key and the authentication user identifier or
30 the enrollment user identifier; and
31 decrypting, by the user device, using the whitebox, the
32 encrypted message with the key derived from the master secret key.

1 5. The method of claim 4, wherein the message includes a limited
2 use key, wherein the limited use key is encrypted by the back-end server computer
3 using the key derived from the master secret key that is created by the back-end
4 server computer with the enrollment user identifier and the master secret key using a
5 key derivation function.

1 6. The method of claim 4, wherein the application is an interaction
2 application, a video streaming application, a data transfer application, a webpage
3 access application, or a social media application.

1 7. The method of claim 4 further comprising:
2 obtaining, by the user device, interaction data for an interaction
3 between a user of the user device and a resource provider of a resource provider
4 computer, wherein the limited use key is used to form a cryptogram that is used in
5 the interaction.

1 8. The method of claim 7 further comprising:
2 generating, by the user device, using the whitebox, the cryptogram for
3 the interaction based on the limited use key and the interaction data.

1 9. The method of claim 2, wherein prior to installing the application
2 comprising the whitebox onto the user device, the method further comprises:
3 generating, by the user device, a download request message that
4 requests to download the application;
5 providing, by the user device, the download request message to an
6 application store; and
7 receiving, by the user device, the application from the application store
8 in response to the download request message.

1 10. The method of claim 1, wherein the master secret key is a
2 symmetric key generated by the back-end server computer.

1 11. A user device comprising:
2 a processor; and
3 a computer-readable medium coupled to the processor, the computer-
4 readable medium comprising code executable by the processor for implementing a
5 method comprising:
6 receiving an encrypted message from a back-end server
7 computer, the encrypted message being a message encrypted by the back-
8 end server computer with a master secret key or a key derived from the
9 master secret key;
10 signing, using a secure element, the encrypted message with a
11 secure element private key to obtain a signed encrypted message;
12 cryptographically recovering, using a whitebox, a secure
13 element public key from a certified key using a back-end server computer
14 public key, the certified key being certified by the back-end server computer;
15 cryptographically recovering, using the whitebox, the encrypted
16 message from the signed encrypted message using the secure element public
17 key; and
18 decrypting, using the whitebox, the encrypted message using
19 the master secret key or the key derived from the master secret key to obtain
20 the message.

1 12. The user device of claim 11, wherein the method further
2 comprises:
3 installing an application comprising the whitebox onto the user device,
4 wherein the whitebox securely includes the master secret key and the back-end
5 server computer public key;
6 generating using the secure element on the user device, the secure
7 element public key and the secure element private key;
8 transmitting an enrollment message including the secure element
9 public key to the back-end server computer associated with the application, wherein
10 the back-end server computer signs the secure element public key with a back-end
11 server computer private key to form the certified key, encrypts the message with the
12 master secret key or the key derived from the master secret key to obtain the
13 encrypted message, and provides the encrypted message to the user device; and
14 receiving the certified key from the back-end server computer.

1 13. The user device of claim 12, wherein the method further
2 comprises:
3 prior to transmitting the enrollment message, obtaining, by the user
4 device, using the secure element on the user device, a user identifier, and wherein
5 transmitting the enrollment message further comprises:
6 transmitting, by the user device, the enrollment message to the back-
7 end server computer, wherein the enrollment message includes the secure element
8 public key and the user identifier, wherein the back-end server computer signs a
9 combination of the secure element public key and the user identifier with the back-
10 end server computer private key to form the certified key, encrypts the message with
11 the master secret key or the key derived from the master secret key to obtain the
12 encrypted message, and provides the encrypted message to the user device
13 .

1 14. The user device of claim 13,
2 wherein the user identifier is an enrollment user identifier, wherein the
3 certified key is signed secure element identification data, and wherein signing the
4 encrypted message further comprises:

5 determining, by the user device, using the secure element, an
6 authentication message using the encrypted message and an authentication
7 user identifier; and
8 signing, by the user device, using the secure element, the
9 authentication message with the secure element private key to form a signed
10 authentication message,
11 wherein cryptographically recovering the secure element public key
12 from the certified key comprises:
13 cryptographically recovering, by the user device, using the
14 whitebox, the secure element identification data from the certified key;
15 obtaining, by the user device, using the whitebox, the secure
16 element public key and the enrollment user identifier; and
17 wherein e) cryptographically recovering the encrypted message from
18 the signed encrypted message comprises:
19 cryptographically recovering, by the user device, using the
20 whitebox, the authentication message from the signed authentication
21 message; and
22 obtaining, by the user device, using the whitebox, the encrypted
23 message and the authentication user identifier from the authentication
24 message; and
25 wherein decrypting the encrypted message comprises:
26 comparing, by the user device, using the whitebox, the
27 authentication user identifier to the enrollment user identifier;
28 if the authentication user identifier and the enrollment user
29 identifier match, generating, by the user device, using the whitebox, the key
30 derived from the master secret key and the authentication user identifier or
31 the enrollment user identifier; and
32 decrypting, by the user device, using the whitebox, the encrypted
33 message with the key derived from the master secret key.

1 15. The user device of claim 12, wherein the back-end server
2 computer signs the secure element public key with the back-end server computer
3 private key using a message recoverable signature process.

1 16. The user device of claim 11, wherein the user device is a mobile
2 phone.

1 17. The user device of claim 11, wherein the secure element is on
2 the user device and is in communication with the processor.

1 18. The user device of claim 11, wherein the whitebox is on the
2 computer readable medium, and wherein the message is encrypted with the master
3 secret key.

1 19. A method comprising:
2 obtaining, by a back-end server computer, a message comprising
3 content to provide to an application installed on a user device;
4 encrypting, by the back-end server computer, the message with a
5 master secret key or a key derived from the master secret key to obtain an encrypted
6 message; and
7 providing, by the back-end server computer, the encrypted message to
8 the user device, wherein the user device, using a secure element, signs the
9 encrypted message with a secure element private key to obtain a signed encrypted
10 message, cryptographically recovers, using a whitebox in the application, a secure
11 element public key from a certified key using a back-end server computer public key,
12 cryptographically recovers, using the whitebox, the encrypted message from the
13 signed encrypted message using the secure element public key, and decrypts, using
14 the whitebox, the encrypted message using the master secret key or the key derived
15 from the master secret key to obtain the message.

1 20. The method of claim 19 further comprising:
2 prior to obtaining the message, generating, by the back-end server
3 computer the back-end server computer public key and a back-end server computer
4 private key;
5 generating, by the back-end server computer, the master secret key;
6 obtaining, by the back-end server computer, an uncompiled application
7 to compile;

8 compiling, by the back-end server computer, the uncompiled
9 application, the master secret key, and the back-end server computer public key into
10 the application;
11 providing, by the back-end server computer, the application to an
12 application store;
13 receiving, by the back-end server computer, an enrollment message
14 including the secure element public key from the user device that has installed the
15 application compiled by the back-end server computer;
16 signing, by the back-end server computer, the secure element public
17 key with the back-end server computer private key to form the certified key; and
18 providing, by the back-end server computer, the certified key to the
19 user device.