

CLAIMS

1 1. A method comprising performing, by a computer associated with an
2 encrypting entity:
3 generating a key for a message;
4 generating N key parts of the key, N being an integer of at least two;
5 for each of the N key parts:
6 encrypting the key part using a trusted key of a corresponding controlling
7 authority;
8 generating the message including at least:
9 a first portion including at least M of the encrypted key parts and
10 identifiers of a plurality of controlling authorities; and
11 a second portion encrypted using the key; and
12 sending the message, wherein at least M of the N key parts are combinable to
13 generate the key such that the generated key is operable to decrypt the second portion of the
14 message, M being an integer equal to or less than N.

1 2. The method of claim 1, wherein the key is a symmetric key generated
2 using a private key of the encrypting entity and a public key associated with a target device.

1 3. The method of claim 1, wherein the key is a randomly generated key that
2 is not known to a target device.

1 4. The method of claim 1, wherein encrypting the key part comprises:
2 generating a symmetric key using a public key of the corresponding controlling
3 authority and a private key of the encrypting entity; and
4 encrypting the key part using the symmetric key.

1 5. The method of claim 1, wherein sending the message comprises sending
2 the message to a target device, wherein the target device is a claimant device associated with a
3 claimant that requests to decrypt the message.

1 6. The method of claim 1, wherein the message includes policy information,
2 wherein the policy information comprises:
3 information indicating entities authorized or not authorized to decrypt encrypted
4 key parts, and
5 information indicating credential types, claims, and validation methods that are
6 acceptable for authentication or authorization of the entities.

1 7. The method of claim 1, wherein each of the identifiers of the plurality of
2 controlling authorities includes a URL routed to the corresponding controlling authority.

1 8. The method of claim 7, wherein the message is sent to computers
2 associated with the controlling authorities corresponding to the at least M of the N key parts
3 based on the identifiers of the plurality of controlling authorities.

1 9. A method comprising performing, by a target device:
2 receiving a message including at least:
3 a first portion including at least M encrypted key parts of a key generated
4 for the message and identifiers of a plurality of controlling authorities, wherein each encrypted
5 key part is encrypted using a trusted key of a corresponding controlling authority, and wherein a
6 computer associated with an encrypting entity generates N key parts of the key, N being an
7 integer of at least two and M being an integer equal to or less than N; and
8 a second portion encrypted using the key;
9 routing the message to one or more computers with a request to decrypt the
10 message;
11 receiving a plurality of re-encrypted key parts encrypted specifically for the target
12 device, each re-encrypted key part encrypted by a corresponding controlling authority from the
13 plurality of controlling authorities;
14 decrypting at least M of the plurality of re-encrypted key parts to obtain at least M
15 key parts;
16 generating the key by combining the at least M key parts; and
17 decrypting the second portion of the message using the generated key.

1 10. The method of claim 9, wherein decrypting the at least M of the
2 plurality of re-encrypted key parts comprises:
3 for each of the at least M of the plurality of re-encrypted key parts:
4 generating a symmetric key using a private key associated with the target
5 device and a public key of the corresponding controlling authority; and
6 decrypting the re-encrypted key part using the symmetric key.

1 11. The method of claim 9, wherein each of the identifiers of the plurality of
2 controlling authorities includes a URL routed to the corresponding controlling authority.

1 12. The method of claim 11, wherein routing the message comprises sending
2 the message to a plurality of computers associated with the plurality of controlling authorities
3 based on the identifiers.

1 13. The method of claim 9, wherein routing the message comprises sending
2 the message to a computer associated with a controlling authority from the plurality of
3 controlling authorities with a request to send the message to a plurality of computers associated
4 with the plurality of controlling authorities.

1 14. The method of claim 9, wherein routing the message comprises sending
2 the message to an intermediary computer with a request to send the message to a plurality of
3 computers associated with the plurality of controlling authorities.

1 15. The method of claim 14, wherein the message includes a URL routed to
2 the intermediary computer.

1 16. A method comprising performing, by a computer associated with a
2 controlling authority:
3 receiving a message including at least:
4 a first portion including at least M encrypted key parts of a key generated
5 for the message and identifiers of a plurality of controlling authorities, wherein each encrypted
6 key part is encrypted using a trusted key of a corresponding controlling authority, and wherein a

7 computer associated with an encrypting entity generates N key parts of the key, N being an
8 integer of at least two and M being an integer equal to or less than N; and
9 a second portion encrypted using the key;
10 decrypting an encrypted key part in the message to obtain a key part;
11 re-encrypting the key part to generate a re-encrypted key part encrypted
12 specifically for a target device; and
13 sending the re-encrypted key part, wherein at least M of the key parts of the key
14 are combinable to generate the key such that the generated key is operable to decrypt the second
15 portion of the message.

1 17. The method of claim 16, wherein decrypting the encrypted key part
2 comprises:
3 obtaining a private key of the corresponding controlling authority; and
4 decrypting the encrypted key part using the private key.

1 18. The method of claim 16, wherein decrypting the encrypted key part
2 comprises:
3 generating a symmetric key using a public key of the encrypting entity and a
4 private key of the controlling authority; and
5 decrypting the encrypted key part using the symmetric key.

1 19. The method of claim 16, wherein re-encrypting the key part comprises:
2 generating a symmetric key using a private key of the controlling authority and a
3 public key associated with the target device; and
4 re-encrypting the key part using the symmetric key.

1 20. The method of claim 16, wherein receiving the message comprises
2 receiving the message from the target device, and wherein sending the re-encrypted key part
3 comprises sending the re-encrypted key part to the target device.

1 21. The method of claim 16, wherein receiving the message comprises
2 receiving the message from an intermediary computer, and wherein sending the re-encrypted key
3 part comprises sending the re-encrypted key part to the intermediary computer.

1 22. The method of claim 16, wherein the computer is a first computer and the
2 controlling authority is a first controlling authority, and wherein receiving the message
3 comprises receiving the message from a second computer associated with a second controlling
4 authority and sending the re-encrypted key part comprise sending the re-encrypted key part to the
5 second computer associated with second controlling authority.

1 23. The method of claim 16, wherein the method further comprises:
2 sending the message to a plurality of computers associated with the plurality of
3 controlling authorities;
4 receiving at least M-1 re-encrypted key parts encrypted specifically for the target
5 device from the plurality of computers associated with the plurality of controlling authorities;
6 and
7 sending the re-encrypted key part and the received at least M-1 re-encrypted key
8 parts to the target device.

1 24. The method of claim 16, wherein the target device is a claimant device
2 associated with a claimant that requests to decrypt the message.

1 25. A computer product comprising a computer readable medium storing a
2 plurality of instructions for controlling a computer system to perform the method of any one of
3 claims 1-24.

1 26. A system comprising:
2 the computer product of claim 25; and
3 one or more processors for executing instructions stored on the computer readable
4 medium.

1 27. A system comprising one or more processors for performing the method
2 of any one of claims 1-24.