

(19) 中华人民共和国国家知识产权局



(12) 发明专利

(10) 授权公告号 CN 102257505 B

(45) 授权公告日 2015. 12. 16

(21) 申请号 200980151384. 4

代理人 宋献涛

(22) 申请日 2009. 12. 22

(51) Int. Cl.

(30) 优先权数据

G06F 21/31(2013. 01)

61/140, 969 2008. 12. 28 US

G06F 21/45(2013. 01)

12/641, 305 2009. 12. 17 US

(85) PCT国际申请进入国家阶段日

(56) 对比文件

2011. 06. 21

CN 101099385 A, 2008. 01. 02,

(86) PCT国际申请的申请数据

CN 1875564 A, 2006. 12. 06,

PCT/US2009/069126 2009. 12. 22

US 5943423 A, 1999. 08. 24,

(87) PCT国际申请的公布数据

US 7010690 B1, 2006. 03. 07,

WO2010/075343 EN 2010. 07. 01

审查员 李文浩

(73) 专利权人 高通股份有限公司

地址 美国加利福尼亚州

(72) 发明人 马修·W·霍尔菲尔德

劳伦斯·G·伦德布拉德

(74) 专利代理机构 北京律盟知识产权代理有限

权利要求书7页 说明书26页 附图12页

责任公司 11287

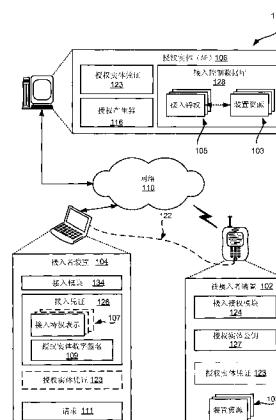
(54) 发明名称

用于提供经授权装置接入的设备和方法

(57) 摘要

本发明描述用于向接入者装置提供用以与被接入者装置上的装置资源交互的接入凭证的方法、设备和系统。与所述被接入者装置具有信任关系的授权实体或链接的次级授权实体产生所述接入凭证。所述接入凭证包含修改检测指示符、至少一个接入特权和接入者公钥。所述至少一个接入特权对应于所述被接入者装置上的至少一个装置资源。所述授权实体将所述接入凭证转发到所述接入者装置，所述接入者装置将所述接入凭证呈现给所述被接入者装置供鉴别。一旦通过鉴别，所述被接入者装置便准予对一个或一个以上装置资源的接入，且控制请求以确保其在所述至少一个接入特权的范围内。

CN 102257505



CN

1. 一种获得对另一装置上的受限制资源的经授权接入的方法, 其包括 :

在接入者装置处从外部授权实体接收接入凭证, 所述外部授权实体与被接入者装置具有直接或间接信任关系, 其中所述接入凭证包含至少一个接入特权表示、接入者公钥和由所述外部授权实体创建的修改检测指示符 ;

向所述被接入者装置传达所述接入凭证、身份证据以及对与所述被接入者装置上的至少一个装置资源的交互的请求 ; 以及

在所述接入者装置处接收在所述被接入者装置处执行的接入鉴别过程的结果, 其中所述接入鉴别过程基于由所述外部授权实体创建的所述修改检测指示符而验证所述接入凭证的真实性, 基于所述接入者公钥而验证所提供的所述身份证据, 且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权, 且其中所述接入鉴别过程的所述结果包括所述接入者装置被准予或拒绝对所述被接入者装置上的所述至少一个装置资源的接入。

2. 根据权利要求 1 所述的方法, 其中接收所述接入凭证进一步包括接收由具有次级凭证的次级授权实体授予的所述接入凭证, 所述次级凭证直接或通过任一数目的其它次级凭证链接到主授权实体凭证, 且其中接收所述结果包括 : 接入被准予是基于所述接入鉴别过程验证了从所述次级凭证直到所述主授权实体凭证且包含所述主授权实体凭证的所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

3. 根据权利要求 1 所述的方法, 其中接收包含所述至少一个接入特权表示的所述接入凭证进一步包括接收可用于主授权实体的多个接入特权的子集的表示, 且进一步包括接收直接或通过任一数目的其它次级实体将所述所接收接入凭证链接到所述主授权实体的凭证链, 且其中接收所述鉴别过程的所述结果包括 : 接入被准予是基于所述接入鉴别过程验证了所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

4. 根据权利要求 3 所述的方法, 其中接收所述凭证链进一步包括接收主授权实体凭证和至少一个次级凭证, 其中接收所述接入凭证、所述主授权实体凭证和至少一个次级凭证在同一时间或在不同时间发生。

5. 根据权利要求 1 所述的方法, 其中接收包含所述至少一个接入特权表示的所述接入凭证进一步包括接收基于与所述接入者装置相关联的组织功能的特权。

6. 根据权利要求 1 所述的方法, 其中接收包含所述至少一个接入特权表示的所述接入凭证进一步包括接收实际特权、范围大于对应于所述外部授权实体的授权实体特权的特权或未知未来特权中的至少一者。

7. 一种获得对另一装置上的受限制资源的经授权接入的设备, 其包括 :

用于从外部授权实体接收接入凭证的装置, 所述外部授权实体与被接入者装置具有直接或间接信任关系, 其中所述接入凭证包含至少一个接入特权表示、接入者公钥和由所述外部授权实体创建的修改检测指示符 ;

用于向所述被接入者装置传达所述接入凭证、身份证据以及对与所述被接入者装置上的至少一个装置资源的交互的请求的装置 ; 以及

用于接收在所述被接入者装置处执行的接入鉴别过程的结果的装置, 其中所述接入鉴别过程基于由所述外部授权实体创建的所述修改检测指示符而验证所述接入凭证的真实性, 基于所述接入者公钥而验证所提供的所述身份证据, 且验证所述接入凭证中的所述至

少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权，且其中所述接入鉴别过程的所述结果包括所述接入者装置被准予或拒绝对所述被接入者装置上的所述至少一个装置资源的接入。

8. 根据权利要求 7 所述的设备，其中用于从外部授权实体接收接入凭证的装置包含用于接收由具有次级凭证的次级授权实体授予的接入凭证的装置，所述次级凭证直接或通过任一数目的其它次级凭证链接到主授权实体凭证，且其中所述结果包括：接入被准予是基于所述接入鉴别过程验证了从所述次级凭证直到所述主授权实体凭证且包含所述主授权实体凭证的所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

9. 根据权利要求 7 所述的设备，其中所述至少一个接入特权表示进一步包括可用于主授权实体的多个接入特权的子集的表示，且其中用于从外部授权实体接收接入凭证的装置包含用于接收直接或通过任一数目的其它次级实体将所述所接收接入凭证链接到所述主授权实体的凭证链的装置，且其中所述结果包括：接入被准予是基于所述接入鉴别过程验证了所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

10. 根据权利要求 9 所述的设备，其中所述凭证链进一步包括主授权实体凭证和至少一个次级凭证，其中所述接入凭证、所述主授权实体凭证和至少一个次级凭证是在同一时间或在不同时间被接收。

11. 根据权利要求 7 所述的设备，其中所述至少一个接入特权表示进一步包括基于与所述接入者装置相关联的组织功能的特权。

12. 根据权利要求 7 所述的设备，其中所述至少一个接入特权表示进一步包括实际特权、范围大于对应于所述外部授权实体的授权实体特权的特权或未知未来特权中的至少一者。

13. 一种提供对被接入者装置上的装置资源的接入的方法，其包括：

从接入者装置接收对应于所述接入者装置的接入凭证、身份证据和对与所述被接入者装置上的至少一个装置资源的交互的请求，其中所述接入凭证与授权实体相关联，所述授权实体与所述被接入者装置具有直接或间接信任关系，且其中所述接入凭证包含至少一个接入特权表示、接入者公钥和由所述授权实体创建的修改检测指示符；

在所述被接入者装置处执行接入鉴别过程，所述接入鉴别过程基于由所述授权实体创建的所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所提供的所述身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权；以及

向所述接入者装置传输所述接入鉴别过程的结果，其中所述接入鉴别过程的所述结果包括准予或拒绝所述接入者装置对所述被接入者装置上的所述至少一个装置资源的接入。

14. 根据权利要求 13 所述的方法，其中接收所述接入凭证进一步包括接收由具有次级凭证的次级授权实体授予的所述接入凭证，所述次级凭证直接或通过任一数目的其它次级凭证链接到主授权实体凭证，且其中传输包括所述接入准予的所述结果进一步包括：验证从所述次级凭证直到所述主授权实体凭证且包含所述主授权实体凭证的所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

15. 根据权利要求 14 所述的方法，其中接收包含所述至少一个接入特权表示的所述接入凭证进一步包括接收可用于主授权实体的多个接入特权的子集的表示，且进一步包括接

收直接或通过任一数目的其它次级实体将所述所接收接入凭证链接到所述主授权实体的凭证链,且其中传输所述鉴别过程的包括所述接入准予的所述结果进一步包括:验证所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

16. 根据权利要求 15 所述的方法,其中接收所述凭证链进一步包括接收主授权实体凭证和至少一个次级凭证。

17. 根据权利要求 13 所述的方法,其中接收包含所述至少一个接入特权表示的所述接入凭证进一步包括接收基于与所述接入者装置相关联的组织功能的特权。

18. 根据权利要求 13 所述的方法,其进一步包括使所述至少一个接入特权表示与至少一个通信接口相关联,以使得与所述接入特权表示相关联的与所述接入者装置的交互限于所述至少一个通信接口。

19. 根据权利要求 13 所述的方法,其中接收包含所述至少一个接入特权表示的所述接入凭证进一步包括接收实际特权、范围大于对应于所述授权实体的授权实体特权的特权或未知未来特权中的至少一者。

20. 一种提供对被接入者装置上的装置资源的接入的设备,其包括:

用于从接入者装置接收对应于所述接入者装置的接入凭证、身份证据和对与所述被接入者装置上的至少一个装置资源的交互的请求的装置,其中所述接入凭证与授权实体相关联,所述授权实体与所述被接入者装置具有直接或间接信任关系,且其中所述接入凭证包含至少一个接入特权表示、接入者公钥和由所述授权实体创建的修改检测指示符;

用于在所述被接入者装置处执行接入鉴别过程的装置,所述接入鉴别过程基于由所述授权实体创建的所述修改检测指示符而验证所述接入凭证的真实性,基于所述接入者公钥而验证所提供的所述身份证据,且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权;以及

用于向所述接入者装置传输所述接入鉴别过程的结果的装置,其中所述接入鉴别过程的所述结果包括准予或拒绝所述接入者装置对所述被接入者装置上的所述至少一个装置资源的接入。

21. 根据权利要求 20 所述的设备,其中所述接入凭证由具有次级凭证的次级授权实体授予,所述次级凭证直接或通过任一数目的其它次级凭证链接到主授权实体凭证,且其中传输包括所述接入准予的所述结果是基于所述接入鉴别过程验证从所述次级凭证直到所述主授权实体凭证且包含所述主授权实体凭证的所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

22. 根据权利要求 21 所述的设备,其中所述至少一个接入特权表示进一步包括直接或通过任一数目的其它次级实体而可用于主授权实体的多个接入特权的子集的表示,且其中传输包括所述接入准予的所述鉴别过程的所述结果是基于所述接入鉴别过程验证所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

23. 根据权利要求 20 所述的设备,其中所述接入凭证进一步包括凭证链,所述凭证链进一步包括主授权实体凭证和至少一个次级凭证。

24. 根据权利要求 20 所述的设备,其中所述至少一个接入特权表示包括基于与所述接入者装置相关联的组织功能的特权。

25. 根据权利要求 20 所述的设备,其进一步包含用于使所述至少一个接入特权表示与

至少一个通信接口相关联,以使得与所述至少一个接入特权表示相关联的与所述接入者装置的交互限于所述至少一个通信接口的装置。

26. 根据权利要求 20 所述的设备,其中所述接入凭证限制所述至少一个接入特权表示供与所述至少一个装置资源相关联地使用和经由至少一个通信接口而使用,以使得对所述至少一个装置资源的接入限于所述对应的至少一个通信接口。

27. 根据权利要求 20 所述的设备,其进一步包含用于经由预定通信信道而与所述接入者装置通信的装置。

28. 根据权利要求 20 所述的设备,其中所述至少一个接入特权表示包括实际特权、范围大于对应于所述授权实体的授权实体特权的特权或未知未来特权中的至少一者。

29. 一种用于授权外部接入者装置与被接入者装置上的资源交互的方法,其包括:

在授权实体处产生接入凭证,所述授权实体与所述被接入者装置具有直接或间接信任关系,其中所述接入凭证包含至少一个接入特权表示、接入者公钥和由所述授权实体创建的修改检测指示符;以及

向所述外部接入者装置传达所述接入凭证,其中所述接入凭证可操作以基于由所述被接入者装置执行的接入鉴别过程,根据所述至少一个接入特权表示而将所述外部接入者装置授权至所述被接入者装置且允许与所述被接入者装置上的至少一个装置资源的交互,所述接入鉴别过程基于由所述授权实体创建的所述修改检测指示符而验证所述接入凭证的真实性,基于所述接入者公钥而验证所述外部接入者装置的身份证据,且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权,其中所述接入鉴别过程的结果包括被准予或拒绝所述外部接入者装置对所述被接入者装置上的所述至少一个装置资源的接入。

30. 根据权利要求 29 所述的方法,其中产生所述接入凭证进一步包括在具有次级凭证的次级授权实体处产生所述接入凭证,所述次级凭证直接或通过任一数目的其它次级凭证链接到主授权实体凭证,且其中包括接入被准予的所述结果是基于所述接入鉴别过程验证从所述次级凭证直到所述主授权实体凭证且包含所述主授权实体凭证的所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

31. 根据权利要求 29 所述的方法,其中产生包含所述至少一个接入特权表示的所述接入凭证进一步包括基于可用于主授权实体的多个接入特权的子集来进行产生,且进一步包括附接直接或通过任一数目的其它次级实体将所述所接收接入凭证链接到所述主授权实体的凭证链,且其中所述鉴别过程的包括接入被准予的所述结果是基于所述接入鉴别过程验证所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

32. 根据权利要求 31 所述的方法,其进一步包括接收主授权实体凭证和至少一个次级凭证。

33. 根据权利要求 32 所述的方法,其中产生所述接入凭证进一步包括产生对应于所述至少一个接入特权表示的有效性指示符,其中所述有效性指示符可操作以界定以下各项中的至少一者:所述至少一个接入特权表示有效的时间周期、基于使用的限制、基于位置的限制、基于装置状态的限制,或通信接口限制。

34. 根据权利要求 29 所述的方法,其中产生包含所述至少一个接入特权表示的所述接入凭证进一步包括:包含基于与所述接入者装置相关联的组织功能的所述接入特权中的一

者或一者以上。

35. 根据权利要求 29 所述的方法,其进一步包括基于至少一个被接入者装置通信接口与所述至少一个接入特权表示或所述至少一个装置资源中的至少一者之间的关联来限制所述接入凭证的使用。

36. 一种用于授权外部接入者装置接入被接入者装置上的资源交互的装置,其包括:

用于在授权实体处产生接入凭证的装置,所述授权实体与所述被接入者装置具有直接或间接信任关系,其中所述接入凭证包含至少一个接入特权表示、接入者公钥和由所述授权实体创建的修改检测指示符;以及

用于向外部接入者装置传达所述接入凭证的装置,其中所述接入凭证可操作以基于由所述被接入者装置执行的接入鉴别过程,根据所述至少一个接入特权表示而将所述接入者装置授权至所述被接入者装置且允许与所述被接入者装置上的至少一个装置资源的交互,所述接入鉴别过程基于由所述授权实体创建的所述修改检测指示符而验证所述接入凭证的真实性,基于所述接入者公钥而验证所述外部接入者装置的身份证据,且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权,其中所述接入鉴别过程的结果包括被准予或拒绝所述外部接入者装置对所述被接入者装置上的所述至少一个装置资源的接入。

37. 根据权利要求 36 所述的装置,其中用于在授权实体处产生接入凭证的装置包含用于在具有次级凭证的次级授权实体处产生所述接入凭证的装置,所述次级凭证直接或通过任一数目的其它次级凭证链接到主授权实体凭证,且其中包括接入被准予的所述结果是基于所述接入鉴别过程验证从所述次级凭证直到所述主授权实体凭证且包含所述主授权实体凭证的所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

38. 根据权利要求 36 所述的装置,其中包含所述至少一个接入特权表示的所述接入凭证包括可用于主授权实体的多个接入特权的子集,且其中用于在授权实体处产生接入凭证的装置包含用于产生包含直接或通过任一数目的其它次级实体将所述接入凭证链接到所述主授权实体的凭证链的所述接入凭证的装置,且其中所述鉴别过程的包括接入被准予的所述结果是基于所述接入鉴别过程验证所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

39. 根据权利要求 38 所述的装置,其中所述凭证链进一步包括主授权实体凭证和至少一个次级凭证。

40. 根据权利要求 36 所述的装置,其中所述接入凭证进一步包括对应于所述至少一个接入特权表示的有效性指示符,其中所述有效性指示符可操作以界定以下各项中的至少一者:所述至少一个接入特权表示有效的时间周期、基于使用的限制、基于位置的限制、基于装置状态的限制,或通信接口限制。

41. 根据权利要求 36 所述的装置,其中所述至少一个接入特权表示是基于与所述接入者装置相关联的组织功能。

42. 根据权利要求 36 所述的装置,其进一步包含用于基于被接入者装置通信接口与所述至少一个接入特权表示或所述至少一个装置资源中的至少一者之间的关联来限制所述接入凭证的使用的装置,其中包含所述至少一个接入特权表示的所述接入凭证是基于所述关联而产生。

43. 一种获得对另一装置上的受限制资源的经授权接入的方法，其包括：

在接入者装置处从外部授权实体接收接入凭证的接入凭证识别符，所述授权实体与被接入者装置具有直接或间接信任关系；

向所述被接入者装置传达所述接入凭证识别符、身仹证据以及对与所述被接入者装置上的至少一个装置资源的交互的请求；以及

在所述接入者装置处接收在所述被接入者装置处执行的接入鉴别过程的结果，其中所述接入鉴别过程基于对应的由所述外部授权实体创建的修改检测指示符而验证所述接入凭证的真实性，基于对应的接入者公钥而验证所提供的所述身仹证据，且验证所述接入凭证中的至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权，且其中所述接入鉴别过程的所述结果包括被准予或拒绝所述接入者装置对所述被接入者装置上的所述至少一个装置资源的接入。

44. 根据权利要求 43 所述的方法，其中接收所述接入凭证识别符进一步包括接收由具有次级凭证的次级授权实体授予的所述接入凭证，所述次级凭证直接或通过任一数目的其它次级凭证链接到主授权实体凭证，且其中接收包括接入被准予的所述结果是基于所述接入鉴别过程验证从所述次级凭证直到所述主授权实体凭证且包含所述主授权实体凭证的所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

45. 根据权利要求 43 所述的方法，其中所述接入凭证识别符对应于可用于主授权实体的多个接入特权的子集的表示，且进一步包括接收直接或通过任一数目的其它次级实体将所述接入凭证链接到所述主授权实体的凭证链的链识别符，且其中接收所述鉴别过程的包括接入被准予的所述结果是基于所述接入鉴别过程验证所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

46. 根据权利要求 45 所述的方法，其中接收所述链识别符进一步包括接收主授权实体凭证识别符和至少一个次级凭证识别符，其中接收所述接入凭证识别符、所述主授权实体凭证识别符和至少一个次级凭证识别符在同一时间或在不同时间发生。

47. 根据权利要求 43 所述的方法，其中所述接入凭证识别符进一步对应于基于与所述接入者装置相关联的组织功能的特权。

48. 根据权利要求 43 所述的方法，其中所述接入凭证识别符进一步对应于实际特权、范围大于对应于所述授权实体的授权实体特权的特权或未知未来特权中的至少一者。

49. 一种获得对另一装置上的受限制资源的经授权接入的设备，其包括：

用于在接入者装置处从外部授权实体接收接入凭证的接入凭证识别符的装置，所述授权实体与被接入者装置具有直接或间接信任关系；

用于向所述被接入者装置的所述接入凭证识别符、身仹证据以及对与所述被接入者装置上的至少一个装置资源的交互的请求的装置；以及

用于在所述接入者装置处接收在所述被接入者装置处执行的接入鉴别过程的结果的装置，其中所述接入鉴别过程基于由所述外部授权实体创建的修改检测指示符而验证所述接入凭证的真实性，基于接入者公钥而验证所提供的所述身仹证据，且验证所述接入凭证中的至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权，且其中所述接入鉴别过程的所述结果包括被准予或拒绝所述接入者装置对所述被接入者装置上的所述至少一个装置资源的接入。

50. 根据权利要求 49 所述的设备, 其中所述接入凭证识别符由具有次级凭证的次级授权实体授予, 所述次级凭证直接或通过任一数目的其它次级凭证链接到主授权实体凭证, 且其中包括接入被准予的所述结果是基于所述接入鉴别过程验证从所述次级凭证直到所述主授权实体凭证且包含所述主授权实体凭证的所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

51. 根据权利要求 49 所述的设备, 其中所述接入凭证识别符对应于可用于主授权实体的多个接入特权的子集, 且其中所述设备进一步包含用于接收直接或通过任一数目的其它次级实体将所述接入凭证链接到所述主授权实体的凭证链的链识别符的装置, 且其中包括接入被准予的所述结果是基于所述接入鉴别过程验证所有所述链接的凭证皆允许对所述至少一个装置资源的接入。

52. 根据权利要求 51 所述的设备, 其中所述链识别符进一步包括主授权实体凭证识别符和至少一个次级凭证识别符, 其中所述接入凭证识别符、所述主授权实体凭证识别符和至少一个次级凭证识别符是在同一时间或在不同时间被接收。

53. 根据权利要求 49 所述的设备, 其中所述接入凭证识别符对应于基于与所述接入者装置相关联的组织功能的特权。

54. 根据权利要求 49 所述的设备, 其中所述接入凭证识别符对应于实际特权、范围大于对应于所述授权实体的授权实体特权的特权或未知未来特权中的至少一者。

## 用于提供经授权装置接入的设备和方法

[0001] 依据 35 U.S.C. § 119 主张优先权

[0002] 本专利申请案主张 2008 年 12 月 28 日申请的题目为“用于提供经授权装置接入的设备和方法 (APPARATUS AND METHODS FOR PROVIDING AUTHORIZED DEVICE ACCESS)” 的第 61/140,969 号临时申请案的优先权，所述临时申请案转让给本发明的受让人且特此以引用方式并入本文。

### 背景技术

[0003] 所描述的方面大体上涉及计算装置上的接入安全性。更特定来说，所描述的方面涉及授权对计算装置的接入以使得仅可由被授权方执行有特权的动作的设备和方法。

[0004] 技术的进步已带来更小且功能更强的个人计算装置。举例来说，当前存在多种便携式个人计算装置，包含无线计算装置，例如便携式无线电话、个人数字助理 (PDA) 和寻呼装置，其每一者均为体积小、重量轻且可容易由用户携带的。更具体来说，例如便携式无线电话进一步包含经由无线网络传达语音和数据包的蜂窝式电话。此外，许多此类蜂窝式电话正被制造成具有计算能力的相对大的增加，且因此正变得相当于小型个人计算机和手持式 PDA。

[0005] 在一些情况下，例如操作第一计算装置的软件开发者等的实体可能需要接入驻存在第二计算装置上的应用程序和数据。待接入的装置可能包含保护机制以控制对其装置资源的接入。举例来说，保护机制已包含仅提供对装置的简单的全接入或无接入的加密协议。

[0006] 提供客户端计算装置与外部装置之间的安全通信的其它系统已知是至少部分通过在制造时在客户端计算装置上安装安全凭证来提供所述安全通信。在一个实例中，服务提供者对客户端计算装置的制造者提供安全凭证，使得制造者可在制造过程期间安装安全凭证。

[0007] 在一些系统中，部分地通过由经授权代理对电话进行安装或编程来提供安全通信。此编程可在客户端计算装置已制造且装运之后发生。在一个实例中，安全凭证是在装置销售的时间和地点安装在客户端计算装置上。此处，在至少一个实例中，经授权代理将来自唯一安全码列表的码输入到客户端计算装置中。在其它实例中，使用自动化读取器来将个别安全码传送到每一客户端计算装置。此过程避免了与在制造时对此些计算装置进行编程相关联的难题中的一些，所述难题例如对通常静态的过程添加动态制造步骤。然而，此过程仍包含其自身的难题和脆弱性，包含对安全凭证列表的潜在未经授权接入的问题，所述接入将允许未经授权实体冒充原本经授权装置的身份。

[0008] 此外，使用凭证的典型硬连线或硬编码方法要求每一客户端装置在每当发生例如违反安全性等的情形时由维修技术员在物理上维修。此情形包含（例如）需要更换、添加和 / 或以另外方式更新一个或一个以上凭证。由维修技术员在物理上维修的要求的操作成本极高，尤其是在大量客户端装置受损时。

[0009] 更具体来说，用于授权经由串行连接对装置的有特权的接入的一种此类机制包含使用服务编程码 (SPC)。由于其缺少可表达性、容易被非法散布且缺少可跟踪性，SPC 不太

适于控制具有精细粒度或强力特权的接入。

[0010] 因此,将有利的是包含在一般的安全通信技术中固有的安全通信优点中的许多优点,例如与使用安全凭证相关联的那些优点,同时也避免这些现存系统的其它较不有利的方面,例如与在无线装置上存储加密算法、需要在制造时安装安全凭证或在销售点位置对安全凭证进行编程,以及在违反安全性的情况下更新或替换这些凭证的能力相关联的问题。

## 发明内容

[0011] 所描述的方面包含可操作以向接入者装置提供对被接入者装置上的受限制资源的接入的设备、方法、计算机程序产品和处理器。

[0012] 在一方面中,一种获得对另一装置上的受限制资源的经授权接入的方法包括在接入者装置处接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证。所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥。所述修改检测指示符由所述授权实体创建。此外,所述方法包含传达所述接入凭证、身份证据以及对与被接入者装置上的至少一个装置资源的交互的请求。另外,所述方法包含接收接入鉴别过程的结果,所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性,基于所述接入者公钥而验证所提供的所述身份证据,且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。所述接入鉴别过程的所述结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0013] 在另一方面中,至少一种经配置以获得对另一装置上的受限制资源的经授权接入的处理器包括第一模块,其用于接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证。所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥。所述修改检测指示符由所述授权实体创建。此外,所述至少一种处理器包含第二模块,其用于传达所述接入凭证、身份证据以及对与被接入者装置上的至少一个装置资源的交互的请求。另外,所述至少一种处理器包含第三模块,其用于接收接入鉴别过程的结果,所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性,基于所述接入者公钥而验证所提供的所述身份证据,且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。所述接入鉴别过程的所述结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0014] 额外方面包含一种计算机程序产品,其包括计算机可读媒体。计算机可读媒体包括可操作以致使计算机接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证的至少一个指令,其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥。所述修改检测指示符由所述授权实体创建。此外,所述计算机可读媒体包含可操作以致使所述计算机传达所述接入凭证、身份证据以及对与被接入者装置上的至少一个装置资源的交互的请求的至少一个指令。另外,所述计算机可读媒体包含可操作以致使所述计算机接收接入鉴别过程的结果的至少一个指令,所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性,基于所述接入者公钥而验证所提供的所述身份证据,且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。所述接入鉴别过程的所述结果包括被准予或拒绝对

所述至少一个装置资源的接入。

[0015] 另一方面包含一种通信装置，其包括用于接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证的装置。所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。此外，所述通信装置包含用于传达所述接入凭证、身份证据以及对与所述被接入者装置上的至少一个装置资源的交互的请求的装置。另外，所述通信装置包含用于接收接入鉴别过程的结果的装置，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所提供的所述身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。所述接入鉴别过程的所述结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0016] 在另一方面中，一种用于接入被接入者装置上的资源的接入者装置包括：处理器；和存储器，其与所述处理器通信。所述接入者装置进一步包含接入模块，其存储在所述存储器中且可由所述处理器执行。所述接入模块可操作以接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证，其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。所述接入模块进一步可操作以起始所述接入凭证、身份证据以及对与所述被接入者装置上的至少一个装置资源的交互的请求的传达。另外，所述接入模块进一步可操作以接收接入鉴别过程的结果，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所提供的所述身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权，其中所述接入鉴别过程的所述结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0017] 在一方面中，一种提供对被接入者装置上的装置资源的接入的方法包括接收对应于接入者装置的接入凭证、身份证据和对与所述被接入者装置上的至少一个装置资源的交互的请求，其中所述接入凭证与同所述被接入者装置具有直接或间接信任关系的授权实体相关联，且其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。所述方法进一步包含执行接入鉴别过程，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所提供的所述身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。另外，所述方法包含传输所述接入鉴别过程的结果，其中所述接入鉴别过程的所述结果包括准予或拒绝对所述至少一个装置资源的接入。

[0018] 在又一方面中，至少一种经配置以提供对装置资源的接入的处理器包括第一模块、第二模块和第三模块。第一模块用于接收对应于接入者装置的接入凭证、身份证据和对与被接入者装置上的至少一个装置资源的交互的请求，其中所述接入凭证与同所述被接入者装置具有直接或间接信任关系的授权实体相关联，且其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。第二模块用于执行接入鉴别过程，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所提供的所述身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装

置资源的特权。第三模块用于传输所述接入鉴别过程的结果，其中所述接入鉴别过程的所述结果包括准予或拒绝对所述至少一个装置资源的接入。

[0019] 在又一方面中，一种计算机程序产品包括计算机可读媒体。所述计算机可读媒体包括用于致使计算机接收对应于接入者装置的接入凭证、身份证据和对与被接入者装置上的至少一个装置资源的交互的请求的至少一个指令，其中所述接入凭证与同所述被接入者装置具有直接或间接信任关系的授权实体相关联，且其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。此外，所述计算机可读媒体包括用于致使所述计算机执行接入鉴别过程的至少一个指令，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所提供的所述身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。另外，所述计算机可读媒体包括用于致使所述计算机传输所述接入鉴别过程的结果的至少一个指令，其中所述接入鉴别过程的所述结果包括准予或拒绝对所述至少一个装置资源的接入。

[0020] 在另一方面中，一种通信装置包括用于接收对应于接入者装置的接入凭证、身份证据和对与所述被接入者装置上的至少一个装置资源的交互的请求的装置，其中所述接入凭证与同所述被接入者装置具有直接或间接信任关系的授权实体相关联，且其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。此外，所述通信装置包括用于执行接入鉴别过程的装置，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所提供的所述身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。另外，所述通信装置包括用于传输所述接入鉴别过程的结果的装置，其中所述接入鉴别过程的所述结果包括准予或拒绝对所述至少一个装置资源的接入。

[0021] 另一方面包含一种用于提供对资源的接入的被接入者装置。所述被接入者装置包括：处理器；至少一个装置资源，其与所述处理器通信；和存储器，其与所述处理器通信。另外，所述被接入者装置包含接入授权模块，其存储在所述存储器中且可由所述处理器执行，其中所述接入授权模块包括接入授权过程。所述接入授权模块可操作以接收对应于接入者装置的接入凭证、身份证据和对与所述被接入者装置上的至少一个装置资源的交互的请求，其中所述接入凭证与同所述被接入者装置具有直接或间接信任关系的授权实体相关联，且其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。此外，所述接入授权模块可操作以执行接入鉴别过程，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所提供的所述身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。另外，所述接入授权模块可操作以传输所述接入鉴别过程的结果，其中所述接入鉴别过程的所述结果包括准予或拒绝对所述至少一个装置资源的接入。

[0022] 在另一方面中，一种用于授权接入者装置与被接入者装置上的资源交互的方法包括产生与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证，其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检

测指示符由所述授权实体创建。另外，所述方法包含传达所述接入凭证，其中所述接入凭证可操作以基于由所述被接入者装置执行的接入鉴别过程，根据所述至少一个接入特权表示而授权所述接入者装置接入所述被接入者装置且允许与所述被接入者装置上的至少一个装置资源的交互，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所述接入者装置的身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。所述接入鉴别过程的结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0023] 此外，在一方面中，至少一种经配置以授权接入者装置与被接入者装置上的资源交互的处理器包括第一模块和第二模块。第一模块用于产生与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证，其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。第二模块用于传达所述接入凭证，其中所述接入凭证可操作以基于由所述被接入者装置执行的接入鉴别过程，根据所述至少一个接入特权表示而授权所述接入者装置接入所述被接入者装置且允许与所述被接入者装置上的至少一个装置资源的交互，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所述接入者装置的身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。所述接入鉴别过程的结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0024] 在另一方面中，一种计算机程序产品包括计算机可读媒体。所述计算机可读媒体包含用于致使计算机产生与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证的至少一个指令，其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。另外，所述计算机可读媒体包含用于致使计算机传达所述接入凭证的至少一个指令，其中所述接入凭证可操作以基于由所述被接入者装置执行的接入鉴别过程，根据所述至少一个接入特权表示而授权所述接入者装置接入所述被接入者装置且允许与所述被接入者装置上的至少一个装置资源的交互，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所述接入者装置的身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。所述接入鉴别过程的结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0025] 在又一方面中，一种授权装置包括用于产生与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证的装置，其中所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥，其中所述修改检测指示符由所述授权实体创建。另外，所述授权装置包含用于传达所述接入凭证的装置，其中所述接入凭证可操作以基于由所述被接入者装置执行的接入鉴别过程，根据所述至少一个接入特权表示而授权所述接入者装置接入所述被接入者装置且允许与所述被接入者装置上的至少一个装置资源的交互，所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性，基于所述接入者公钥而验证所述接入者装置的身份证据，且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。所述接入鉴别过程的结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0026] 另外,在另一方面中,一种用于授权接入者装置接入被接入者装置上的资源的装置包括:处理器;存储器,其与所述处理器通信;凭证管理模块;和通信模块。凭证管理模块存储在所述存储器中且可由所述处理器执行,且包含特权建立模块,所述特权建立模块可操作以产生与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证。所述接入凭证包含修改检测指示符、至少一个接入特权表示和接入者公钥。所述修改检测指示符由所述授权实体创建。另外,通信模块与所述处理器通信且可操作以传达所述接入凭证。所述接入凭证可操作以基于由所述被接入者装置执行的接入鉴别过程,根据所述至少一个接入特权表示而授权所述接入者装置接入所述被接入者装置且允许与所述被接入者装置上的至少一个装置资源的交互,所述接入鉴别过程基于所述修改检测指示符而验证所述接入凭证的真实性,基于所述接入者公钥而验证所述接入者装置的身份证据,且验证所述接入凭证中的所述至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权。所述接入鉴别过程的结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0027] 在另一方面中,一种获得对另一装置上的受限制资源的经授权接入的方法包括在接入者装置处接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证的接入凭证识别符。所述方法进一步包含传达所述接入凭证识别符、身份证据以及对与被接入者装置上的至少一个装置资源的交互的请求。另外,所述方法包含接收接入鉴别过程的结果,所述接入鉴别过程基于对应的修改检测指示符而验证所述接入凭证的真实性,基于对应的接入者公钥而验证所提供的所述身份证据,且验证所述接入凭证中的至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权,其中所述接入鉴别过程的所述结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0028] 在又一方面中,至少一种经配置以使得接入者装置能够获得对另一装置上的受限制资源的经授权接入的处理器包括第一模块,其用于接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证的接入凭证识别符。所述至少一种处理器进一步包含第二模块,其用于传达所述接入凭证识别符、身份证据以及对与被接入者装置上的至少一个装置资源的交互的请求。另外,所述至少一个处理器包含第三模块,其用于接收接入鉴别过程的结果,所述接入鉴别过程基于修改检测指示符而验证所述接入凭证的真实性,基于接入者公钥而验证所提供的所述身份证据,且验证所述接入凭证中的至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权,其中所述接入鉴别过程的所述结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0029] 在另一方面中,一种计算机程序产品包括计算机可读媒体,其具有多个指令。所述指令包含可操作以致使计算机接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证的接入凭证识别符的至少一个指令。此外,所述指令包含可操作以致使所述计算机传达所述接入凭证识别符、身份证据以及对与被接入者装置上的至少一个装置资源的交互的请求的至少一个指令。另外,所述指令包含可操作以致使所述计算机接收接入鉴别的结果的至少一个指令,所述接入鉴别基于修改检测指示符而验证所述接入凭证的真实性,基于接入者公钥而验证所提供的所述身份证据,且验证所述接入凭证中的至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权,其中所述接入鉴别过程的所述结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0030] 在又一方面中，一种通信装置包括用于接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证的接入凭证识别符的装置。此外，所述通信装置包含用于传达所述接入凭证识别符、身仹证据以及对与被接入者装置上的至少一个装置资源的交互的请求的装置。另外，所述通信装置包含用于接收接入鉴别过程的结果的装置，所述接入鉴别过程基于修改检测指示符而验证所述接入凭证的真实性，基于接入者公钥而验证所提供的所述身仹证据，且验证所述接入凭证中的至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权，其中所述接入鉴别过程的所述结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0031] 在一方面中，一种用于接入被接入者装置上的资源的接入者装置包括：处理器；存储器，其与所述处理器通信；以及接入模块，其存储在所述存储器中且可由所述处理器执行。所述接入模块可操作以接收与同被接入者装置具有直接或间接信任关系的授权实体相关联的接入凭证的接入凭证识别符。此外，所述接入模块可操作以起始所述接入凭证识别符、身仹证据以及对与被接入者装置上的至少一个装置资源的交互的请求的传达。另外，所述接入模块可操作以接收接入鉴别过程的结果，所述接入鉴别过程基于修改检测指示符而验证所述接入凭证的真实性，基于接入者公钥而验证所提供的所述身仹证据，且验证所述接入凭证中的至少一个接入特权表示对应于所述交互请求中的接入所述至少一个装置资源的特权，其中所述接入鉴别过程的所述结果包括被准予或拒绝对所述至少一个装置资源的接入。

[0032] 在审阅整个申请案之后将明了所描述方面的其它方面、优点和特征。

## 附图说明

[0033] 通过参考以下结合附图做出的详细描述将更容易明了本文描述的上述方面和所述方面的伴随的优点，附图中：

[0034] 图 1 是用于向经授权人员提供对客户端计算装置的有特权的接入的系统的一个方面的高级图；

[0035] 图 2 是多个特权委派层级的一个方面的示意图，所述层级包含主授权实体将凭证授予到一个或一个以上次级实体，其中每一次级实体可同样地将凭证授予较低层级的一个或一个以上次级实体，依此类推；

[0036] 图 3 是与接入被接入者装置上的一个或一个以上装置资源相关的在接入者装置与被接入者装置之间的交互的一个方面的示意图；

[0037] 图 4 是图 1 的接入凭证的一个方面的示意图；

[0038] 图 5 是图 1 的系统的蜂窝式电话网络的一个方面的示意图；

[0039] 图 6 是图 1 的系统的称为被接入者装置的客户端计算装置的一个方面的框图；

[0040] 图 7 是经配置以用于对根据图 1 的系统的客户端计算装置上的受限制特征的有特权的接入的称为接入者装置的外部计算装置的一个方面的框图；

[0041] 图 8 是如图 1 的系统中使用的可在服务器中实施的授权实体的一个方面的框图；

[0042] 图 9 和图 10 是根据图 1 的系统的方法的相应方面的消息流程图。

[0043] 图 11 是可在根据图 1 的系统的客户端计算装置上操作的方法的一个方面的流程图；以及

[0044] 图 12 是可在根据图 1 的系统的接入装置上操作的方法的一个方面的流程图。

### 具体实施方式

[0045] 以下具体实施方式描述用以授权对计算机装置上的一个或一个以上预定资源的接入以使得可在被接入装置上执行有特权的动作的方法、设备和计算机可读媒体。不同于可提供用以授予特权的完全授予或不授予途径的方法，所描述的方面准许受信任实体或具有来自受信任实体的委派授权的次级实体动态地产生仅具有执行预定任务所必要的那些特权而不损害正被接入的装置的其它方面的凭证。

[0046] 参见图 1，在一个方面中，系统 100 包含用于向一个装置提供对另一装置的一个或一个以上资源的经授权接入的设备和方法。举例来说，系统 100 可包含接入者装置 104，其尝试与被接入者装置 102 上的多个装置资源 103 中的一者或一者以上交互。如本文使用，接入者装置 104 指请求对另一装置的接入和 / 或与另一装置的交互的装置，而被接入者装置 102 指接收到接入和 / 或交互请求的装置。在典型操作中，被接入者装置 102 禁止或限制对所述多个装置资源 103 的外部接入，使得在没有本发明设备和方法的情况下，所述多个装置资源 103 将不可用于例如接入者装置 104 等的外部装置。

[0047] 举例来说，所述多个装置资源 103 可包含（但不限于）以下各项中的一者或任一组合：数据和 / 或文件和 / 或文件系统，例如用户输入数据，包含联系人姓名、联系人地址、联系人电话和 / 或传真号码、内容电子邮件地址、图片、音频文件、视频文件等；配置信息，例如装置相关配置数据、网络相关配置数据、服务编程码（SPC）、安全性策略、病毒扫描器、服务器地址等；服务，例如语音呼叫、数据呼叫、扬声器、麦克风、显示器、定位和 / 或地理定位系统服务、除错或故障查找服务、对预定通信端口的接入，和在相应装置上可用的任何其它服务和 / 或应用；以及操作系统级服务，例如过程创建能力、文件系统接入、启动和运行应用程序的能力等。

[0048] 在一些情况下，举例来说，装置资源 103 可能不可由被接入者装置 103 的所有者接入，而是仅可由经授权人员接入。此受限接入装置资源 103 的实例可包含（但不限于）有版权的内容、装置配置设定、遥测数据等中的一者或一者以上。然而可能需要允许经授权人员接入一个或一个以上装置资源 103。举例来说，当所有者获得新装置时，可授权技术员将有版权的内容从旧装置转移到用户的新装置。在另一实例中，无线装置可能具有锁定到给定无线网络和 / 或锁定到给定系统配置的订户身份模块（SIM），但可能需要允许经授权技术员修改设定或配置，同时避免装置所有者进行此动作。在又一实例中，无线装置可具有可能不允许用户改变但可授予例如技术员等的经授权用户受限特权以接入和验证和 / 或改变的网络相关数据和 / 或设定。应注意，本发明方面不限于这些情境，且可存在其它类似使用情况。

[0049] 此外，系统 100 可包含授权实体（AE）106，其具有与被接入者装置 102 和 / 或与一个或一个以上装置资源 103 的信任关系。授权实体 106 可包括或可操作以产生与多个装置资源 103 中的每一者相关联的一个或一个以上接入特权 105 的定义，其中每一接入特权 105 使得能够接入所述多个装置资源 103 中的至少一者并与其交互。举例来说，一个或一个以上接入特权 105 可包含（但不限于）除错和 / 或执行装置维护功能，例如无线装置的供应和再配置、管理用于同步工具程序的地址簿、文件系统接入、例如图片、音乐、铃声等内容的

上载和 / 或下载,以及数据在装置之间的传送。在一些方面中,接入特权 105 中的一者或一者以上可包含未知的未来特权,例如,特权可包含代码,且其中与所述代码相关联的特权的定义的确定可针对稍后日期而保留。此外,举例来说,对于每一被接入者装置 102, AE 106 可将每一接入特权 105 与所述多个装置资源 103 中的对应一者或一者以上之间的关系存储在接入控制数据库 128 中。由此,接入特权 105 可为个别特权,或可为特权集合的一部分,例如基于组织角色、地位、职务等。另外,应注意 AE 106 和所述多个装置资源 103 中的每一者或与相应资源相关联的操作者可具有关于每一接入特权 105 的定义以及关于如何授予这些特权的策略的预定协议。

[0050] 此外,AE 106 可包含授权产生器 116,其可操作以将接入凭证 126 颁予接入者装置 . 104 以使得能够接入被接入者装置 102 上的所述多个装置资源 103 中的一者或一者以上且与其交互。举例来说,接入凭证 126 可包含一个或一个以上颁予的接入特权 107(例如由 AE 106 基于接入者装置 104 的身份和 / 或目的所确定)和用以证明授权凭证 126 的真实性的授权实体 (AE) 数字签名 109(也称为修改检测指示器)。在一些方面中,例如,颁予的接入特权 107 可从可用的接入特权 105 中选择。在其它方面中,颁予的接入特权 107 可为隐式特权,而非包含于凭证中的有形特权。举例来说,隐式特权可简单地基于拥有接入凭证而允许对相应装置资源的接入。另外,AE 106 和 / 或验证产生器 116 可将 AE 凭证 123 转发到接入者装置 104,以便允许接入者装置 104 证明接入凭证 126 中的接入特权 107 在能够由 AE 106 授予的特权的可允许范围内。

[0051] 应注意,系统 100 可包含多个 AE 106,其中每一 AE 106 能够具有对应于一个或一个以上装置资源 103 的一个或一个以上接入特权 105 的相应集合。由此,在一些情况下,每一 AE 106 可在其关于被接入者装置 102 的一个或一个以上装置资源 103 可授予的特权的范围上受限。

[0052] 举例来说,参见图 2,在一个方面中,AE 106 可包括多个实体,例如主授权实体 (AE) 115 和一个或一个以上层级的一个或一个以上次级授权实体,例如实体 117、119 和 121。此外,主 AE 115 包含主凭证 123,其使得主 AE 115 中的授权产生器 116 能够产生一个或一个以上接入凭证 126 以供接入者装置 104(图 1) 使用,和 / 或一个或一个以上次级凭证,例如 129 和 131,以分别供在低于主 AE 115 的层级处的一个或一个以上次级授权实体(例如次级 AE 117 和 / 或 119) 使用。在此情况下,举例来说,次级 AE 117 被授予次级凭证 129,且次级 AE 119 被授予次级凭证 131。在一些方面中(但不限于这些方面),由每一相应凭证授予的特权可重叠或可相互排斥,但等于或少于可用于主 AE 115 的授权和特权。同样,在一些方面中,次级 AE 117 和 119 可进一步通过基于授予其的相应次级凭证而授予其自身的相应接入凭证和 / 或次级凭证来委派特权。由此,在一些方面中,每一连续的次级凭证包括等于或少于包含在用以产生相应次级凭证的凭证中的授权和特权的授权和特权。应注意,在层次结构的任一层级处,相应的次级凭证可关于特权而重叠,或相应的次级凭证可提供唯一的特权集合。举例来说,在一个使用情况下,手机芯片制造商可基于由每一相应接收实体执行的组织功能来授予各自具有单独特权集合的多个次级凭证。因此,建立了用于委派特权的系统,其允许任一数目层级的动态特权授予,其中授予相应次级实体的特权等于或少于进行授予的实体可用的特权。

[0053] 举例来说,主 AE 115 可将次级凭证 129 授予次级 AE 117 且将次级凭证 131 授予

次级 AE 119，其中次级凭证 129 和 131 中的授权和特权等于或少于包含在主凭证 123 中的授权和特权。同样，举例来说，次级 AE 117 可将次级凭证 133 授予另一被委派者，例如次级 AE 121，其中次级凭证 133 中的授权和特权等于或少于包含在次级凭证 129 中的授权和特权。应注意，每一进行授予的实体可授予任一数目的次级凭证。

[0054] 此外，仍参见图 2，在每一次级凭证的产生和 / 授予中使用的相应凭证可经由一个或一个以上较高层级凭证的链传递到相应的次级实体，进而提供相应次级凭证的有效性的证据和特权的范围有效的证据。在一些方面中，凭证链可不包含在相应接入凭证中，然而，可包含对其的参考或其指示器，或系统可提供用以发现返回到主授权实体的链接的机制。举例来说，当主 AE 115 授予次级凭证 129 和 131 时，相应的次级 AE 117 和 119 也从主 AE 115 或从另一装置接收主凭证 123。或者，主凭证 123 可在一个时间（例如在制造期间）加载到每一次级 AE（例如 117 和 119）上，且可在另一时间，例如授予或请求对应特权的时间提供相应的次级凭证 129 和 131。由此，可在同一时间或在不同时间接收凭证。类似地，当被委派者或次级实体颁予又一次级凭证时，接收实体接收直到主凭证 123 的所有凭证。举例来说，当次级 AE 121 授予次级凭证 135 时，接收实体也接收：(1) 授予次级 AE 121 的次级凭证 133；(2) 授予次级 AE 117 的次级凭证 129，次级 AE 117 授予次级凭证 133；以及 (3) 来自主 AE 115 的主凭证 123，主 AE 115 将次级凭证 129 授予次级 AE 117。由此，基于凭证提供信任链。类似地，当被接入者凭证 126 由任一次级实体授予时，相应的凭证链由被接入者装置 102（图 1）接收，进而允许接入者装置 104 验证相应特权的范围，且验证特权最终是（在一些情况下经由一个或一个以上委派层级）由接入者装置 104 了解的受信任方（例如，主 AE 115）授予。因此，本发明方面允许实现非常动态且多层次的凭证和特权产生和授予系统，其提供了验证任一颁予的凭证和特权的有效性和范围。

[0055] 另外，举例来说，上文描述的接入凭证中的任一者可存储在网络装置上，且凭证向装置的授予可通过将接入凭证识别符提供到接收授予的装置而传达到装置，所述识别符包含关于可在何处获得或接入凭证的信息。因此，当使用接入凭证时，装置可将相应的接入凭证识别符提供到另一装置，其使得接收装置能够从网络位置检索或以另外方式接入相应的接入凭证。举例来说，接入凭证识别符可包含以下各项中的一者或一者以上：个别接入凭证的接入凭证识别符；对应于主授权实体凭证的主授权实体凭证识别符；对应于一个或一个以上次级凭证的一个或一个以上次级凭证识别符；以及对应于直接或通过任一数目的其它次级实体将接入凭证链接到主授权实体的凭证链的链识别符。

[0056] 因此，系统 100 允许将特定的接入特权 105 授予和 / 或委派给特定的 AE 106，进而向系统 100 的管理者提供动态地控制系统内接入凭证 126 的产生的能力。

[0057] 返回参见图 1，在从 AE 106 接收到接入凭证 126 之后以及在例如经由网络 110 从 AE 106 接收到或获得 AE 凭证 123 之后，接入者装置 104 执行接入模块 134，接入模块 134 可操作以与被接入者装置 102 通信。举例来说，接入者装置 104 可通过网络 110 或通过本地有线或无线连接 122 而与被接入者装置 102 通信。在一些方面中，举例来说，接入模块 134 将接入凭证 126 和 AE 凭证 123 呈现给被接入者装置 102 以便基于所述一个或一个以上颁予的接入特权 107 而提供对接入所述多个装置资源 103 中的预定装置资源的授权。然而应注意，AE 凭证 123 可从其它源得到，且不要求接入者装置 104 提供 AE 凭证 123。作为响应，举例来说，被接入者装置 102 执行接入授权模块 124，接入授权模块 124 可操作以例如通过

用接入实体 (AE) 公钥 127 (或引导回到主 AE 的例如可由次级 AE 签名的经签名凭证链) 证实 AE 数字签名 109 且例如通过例如经由检查 AE 凭证 123 来确保接入特权 107 等于或少于 AE 凭证 123 中的特权的范围而证实接入特权 107 的范围, 来验证接入凭证 126。对 AE 数字签名 109 的验证和对 AE 凭证 123 的检查允许被接入者装置 102 信任与接入凭证 126 包含在一起的信息, 因为验证过程向被接入者装置 102 证明 AE 106 颁予接入凭证 126, 且因此已授权所述一个或一个以上颁予的接入特权 107。

[0058] 应注意, 在一些方面中, 接入授权模块 124 可能不知道和 / 或不关心授予何种接入特权 107, 因为接入授权模块 124 主要关注于验证接入凭证 126 是真实的。由此, 系统 100 允许特权的授予成为非常动态的过程, 因为不需要以关于哪些接入特权 105 与哪些装置资源 103 适当相关联的新信息来连续更新接入授权模块 124。

[0059] 如果接入凭证 126 未通过验证, 那么接入授权模块 124 拒绝接入者装置 104 的接入。如果接入凭证 126 通过验证, 那么接入授权模块 124 允许对所述多个装置资源 103 中的预定一者或一者以上的接入和交互, 其中相应装置资源基于包含在接入凭证 126 中的所述一个或一个以上颁予的接入特权 107 而限制所述交互。在一个方面中, 举例来说, 在验证之后, 接入者装置 104 能够执行接入模块 126 以向被接入者装置 102 提交与所述多个装置资源 103 中的一者或一者以上交互的请求 111。在其它方面中, 请求 111 可与接入凭证 126 在同时呈现。在接收到请求 111 后, 在验证接入凭证 126 且验证所述请求 111 属于所授予特权范围内之后, 被接入者装置 102 可基于包含在经验证接入凭证 126 内的所述一个或一个以上颁予的接入特权 107 而执行所请求的装置资源。因此, 如果经验证, 那么接入凭证 126 向接入者装置 104 提供根据所述一个或一个以上颁予的接入特权 107 的与所述多个装置资源 103 中的一者或一者以上的经授权交互。

[0060] 虽然分别说明为膝上型计算机和蜂窝式电话, 但应注意, 接入者装置 104 和被接入者装置 102 可为任一类型的计算机装置。此外应注意, 授权实体 106、接入者装置 104 和被接入者装置 102 可通过包含网络 110 和本地连接 122 的任一类型的通信链路互连 (但不一定同时互连), 所述通信链路可包含直接串行连接或无线连接。

[0061] 因此, 系统 100 提供用于允许接入者装置 104 基于由 AE 106 颁予的接入凭证 126 而接入被接入者装置 102 且与其交互的动态机制。由此, 虽然如同当涉及次级 AE (见图 2) 时的情况, 被接入者装置 102 可能不知道和 / 或不信任接入者装置 104, 但系统 100 允许被接入者装置 102 基于被接入者装置 102 对通过 AE 数字签名 109 和 AE 凭证 123 (或凭证链) 验证的 AE 106 的信任而与接入者装置 104 的一个或一个以上装置资源 103 交互。此外, 接入凭证 126 可被动态产生, 且有利地可特定识别多个接入特权 105 中与多个装置资源 103 中被 AE 106 授权供接入的特定装置资源相关联的选定接入特权, 以便按需要来限制接入。

[0062] 参见图 3, 在可借以获得对被接入者装置 102 的接入的程序的一个特定实例中, 在事件 201 处, 接入者装置 104 将接入凭证 126 和 AE 凭证 123 传递到装置资源 103 以便起始交互。如上所述, 接入凭证 126 是先前从 AE 106 请求或由 AE 106 另外提供 (图 1)。此外, 如上所述, 被接入者装置 102 可从另一源获得 AE 凭证 123。接入凭证 126 和 AE 凭证 123 由计算机平台 203 接收且转发到资源应用程序 205。在允许与装置 103 的交互之前, 在事件 207 处, 资源应用程序将接入凭证 126 和 AE 凭证 123 传递到接入授权模块 124 以便验证特权的真实性和范围。在事件 209 和 211 处, 接入授权模块 124 以 AE 公钥 625 验证 AE 数字

签名 109,且验证关于 AE 凭证 123 的颁予的接入特权 107 的范围。在事件 213 处,基于验证检查,接入授权模块 124 向资源应用程序 205 返回响应,所述响应验证或拒绝接入凭证 126 和 / 或颁予的接入特权 107 的真实性。在事件 215 处,资源应用程序 205 又将指示验证检查的结果的响应转发到接入者装置 104 的接入模块 134。在事件 217 处,如果接入凭证 126 和颁予的接入凭证 107 通过验证,那么作为响应,接入模块 134 将请求 111 发送到资源应用程序 205。如上所述,在一些方面中,请求 111 可连同接入凭证 126 一起包含在初始通信中。在事件 219 处,资源应用程序 205 又在请求 111 包括颁予的接入特权 107 内的动作的情况下将请求 111 或请求 111 的经重新格式化表示或一部分传递到特定资源 221。任选地,取决于请求 111 的性质,在事件 223 和 225 处,可由特定资源 221 和资源应用程序 205 将请求响应返回到接入模块 134。举例来说,此请求响应可包括请求 111 经执行的验证和 / 或请求响应可包括与请求 111 相关联的数据。因此,被接入者装置 102 可基于验证了接入凭证 126 由 AE 106 颁予到接入者装置 104 或在 AE 106(被接入者装置 102 和 / 或相应装置资源 103 与其具有信任关系)的授权下由次级授权实体(见图 2)颁予到接入者装置 104,在所识别接入特权 107 的范围内向未知且不受信任的接入者装置 104 提供对一个或一个以上装置资源 103 的接入。

[0063] 在一些方面中,接入者装置 104 与被接入者装置 102 之间的通信交换可包括发送接入凭证 126 和请求 111 和接收结果的单次往返行程,所述结果例如为基于请求而返回的数据或拒绝接入或拒绝所述请求的通知。在其它方面中,通信会话可在一旦接入凭证 126 通过验证时就建立,包含多个请求和结果的交换。在此通信会话中,虽然被接入者装置 102 信任接入者装置 104,但被接入者装置 102 可能仍要基于接入凭证 126 而验证每一请求 111 属于所授予特权的范围内。此外,应注意,接入者装置 104 可能在与被接入者装置 102 的每次交互时都呈现接入凭证 126。举例来说,在接入凭证 126 的初始呈现和验证之后,在一些方面中,接入者装置 104 可仅例如通过使用先前产生且先前交换的公钥 / 私钥对而将身份的证据提供到被接入者装置 102,被接入者装置 102 随后可参考计算机平台 203 上的先前经验验证凭证真实性和特权范围的所存储指示。

[0064] 参见图 4,在一些方面中,接入凭证 126 可任选地包含额外信息,如虚线所指示,其由 AE 106 输入以用于识别和 / 或验证目的。举例来说,除了一个或一个以上颁予的接入特权 107 和 AE 数字签名 109 外,接入凭证 126 还可包含(但不限于)颁予者识别符 202、凭证识别符 204、接入者识别符 206、接入者公钥 208 的指示、有效性指示符 210 或既定被接入者识别符 212 中的一者或任一组合。

[0065] 颁予者识别符 202 可包含名称、代码、号码或任一其它类型的信息,其指示颁予源,例如授权实体 106 的名称或硬件识别,或例如实体的 X.500 系列计算机联网标准名称,例如签署接入凭证 126 的证书授权方。颁予者识别符 202 可进一步包含识别由 AE 106 使用以签署接入凭证 126 的算法的信息。

[0066] 凭证识别符 204 可包含名称、代码、号码或任一其它类型的信息,其提供接入凭证 126 的唯一识别以例如跟踪颁予的和 / 或期满的接入凭证,且还例如为用以区别接入凭证 126 与其它证书的序列号。此外,举例来说,凭证识别符 204 还可包含不可预测和 / 或随机的数据。另外,举例来说,凭证识别符 204 可包含识别接入凭证存储的位置(例如网络装置上)的指针或其它信息,进而使得进行授予的实体能够将凭证识别符转发到接收实体,而

非必须传递实际的凭证。在一些方面中,接收实体可将凭证识别符 204 提供到待接入的装置,且待接入的装置可利用所述指针或其它位置信息来获得或接入对应的接入凭证 126 以便确定接入是被准予还是被拒绝。

[0067] 接入者识别符 206 可包含名称、代码、号码或任一其它类型的信息,其提供接入凭证 126 被颁予到的接入者装置 104 的唯一识别,进而帮助将相应接入凭证绑定到所识别的接入者装置。

[0068] 接入者公钥 208 的指示可包含对对应于仅由接入者装置 104 已知的专用加密机制的公开可用加密机制的参考或其实际副本,例如接入者公钥 208 的包含可允许被接入者装置 102 进一步验证接入者装置 104 的身份和 / 或可允许建立与接入者装置 104 的安全通信。接入者公钥 208 可进一步包含算法识别符,其指定密钥属于哪一公钥加密系统和任何相关联的密钥参数。在一些方面中,AE 106 可在所授予且数字签署的接入凭证 126 内包含接入者公钥 208 以使被接入者装置 102 能够确保请求接入的装置是接入凭证被授予到的适当被接入者装置,如下文更详细论述。

[0069] 有效性指示符 210 可包含关于接入凭证 126 的有效性的限制的指示符。举例来说,有效性指示符 210 可包含基于时间的限制,例如日、日期、时间、开始日期和 / 或时间以及结束日期和 / 或时间、使用次数等中的一者或任一组合。另外,举例来说,有效性指示符 210 可包含基于使用的限制,例如预定使用次数。此外,举例来说,有效性指示符 210 可包含基于位置的限制,例如可与地理位置和 / 或基于网络的位置相关联。另外,举例来说,有效性指示符 210 可包含基于装置状态的限制,例如基于与相应被接入者装置和 / 或相应接入者装置的任一功能或组件相关联的任一状态的值中的一者或任一组合。

[0070] 既定被接入者识别符 212 可包含名称、代码、号码或任一其它类型的信息,其指示接入凭证 126 针对其有效的特定被接入者装置 102,例如被接入者装置 102 的名称或硬件识别。此外,关于接入凭证 126,AE 106 可将 AE 数字签名 109 应用到上述参数中的任一者或任一组合。另外,在一些方面中,接入凭证 126 可包含 AE 凭证 123 和 / 或 AE 公钥的指示符 204 或可与 AE 凭证 123 和 / 或 AE 公钥的指示符 204 相关联,AE 公钥的指示符 204 可用以鉴别 AE 凭证 123 和 / 或 AE 数字签名 109。

[0071] 在一些方面中,接入凭证 126 可包含所有上述参数。在其它方面中,例如在非常短寿命的接入凭证 126 的情况下,可不包含接入者公钥 208,因为其对于进一步验证接入者装置 104 可能不是必要的,和 / 或可能不必利用接入者公钥 208 来建立安全通信,因为接入凭证 126 的有效性的持续时间可有效地使对被接入者装置 102 的安全性威胁最小。举例来说,非常短寿命的有效性持续时间可包含具有有效性指示符 210 的接入凭证 126,有效性指示符 210 表示使用次数或在其它情况下表示时间周期,例如从约 1 分钟到约 10 分钟。对于基于时间的有效性指示符 210,可利用在 AE 106 与被接入者装置 102 和 / 或接入者装置 104 之间同步的时钟。另外,所述时钟可为逻辑时钟或实时时钟。此外,在一些方面中,例如当接入者装置 104 不具有建立的公钥 / 私钥对时,AE 106 可为接入者装置 104 建立此密钥对以与本文论述的装置接入设备和方法一起使用。

[0072] 参见图 5,系统 100 的一方面可并入有无线网络 302,且可包含例如无线客户端计算装置(例如被接入者装置 102)等的远程模块借以在彼此之间和 / 或在经由无线网络 302 连接的组件(包含但不限于无线网络运营商和 / 或服务器)之间无线地通信的任何系统。

[0073] 在一些方面中, AE 106 可为较高授权基础结构 304 的一部分, 其可包含充当根 CA 或受信任第三方的一个或一个以上证书授权方 (CA)。然而应注意, AE 106 大体上被视为某种形式的 CA。当适当时, AE 106 可从授权基础结构 304 内的另一服务器 /CA 获得证书。

[0074] 此外, 在一些方面中, 系统 100 包含接入凭证的委派, 使得例如 AE 106 等的一个实体或组织可将接入凭证 126 颁予到例如接入者装置 104 等的其它实体, 所述其它实体可进一步将额外接入凭证颁予到额外实体。举例来说, 授权基础结构 304 可包含可将接入凭证颁予到运营商网络的根 CA, 其中所述接入凭证可包含对一个或一个以上给定被接入者装置和 / 或装置资源的一个或一个以上接入特权。运营商网络又可动态地产生用于雇员、服务承包者等的委派的接入凭证, 其中所委派接入凭证包含与由根 CA 所授予的原始颁予的特权相比不更宽且通常更窄的接入特权。特权的委派提供了授予特权时的组织灵活性, 由此委派允许中间组织基于所述组织可用的特权而颁予凭证。此外, 此委派允许中间组织控制凭证, 因为凭证可限于特定用于所需接入的预定特权, 进而减少了接入特权的潜在滥用。

[0075] 在一些方面中, AE 106 连同包含授权基础结构 304 的任何其它服务器一起可为运营商网络 306 的一部分, 且可操作以动态地产生接入凭证, 从而允许经授权接入者装置 104 接入一个或一个以上被接入者装置 102 上的受限制特征, 例如所述多个装置资源 103(图 1)。

[0076] 在系统 100 中, 运营商网络 306 控制发送到无线网络 302 且更特定来说发送到移动交换中心 (MSC) 308 的消息 (作为数据包发送)。运营商网络 306 通过例如因特网和 / 或 POTS(老式普通电话系统) 等的网络 310 与 MSC 308 通信。通常, 网络或因特网连接在运营商网络 306 与 MSC 310 之间传送数据信息, 且 POTS 传送语音信息。

[0077] MSC 308 连接到多个基站 (BTS) 312, 基站 312 与一个或一个以上被接入者装置 102(在此实例中为无线装置) 通信。以类似于运营商网络的方式, MSC 308 通常通过用于数据传送的网络和 / 或因特网以及用于语音信息的 POTS 两者连接到每一 BTS 312。每一 BTS 312 最终通过短消息接发服务 (SMS) 和 / 或其它无线方法而无线地与例如蜂窝式电话等的被接入者装置 102 交换语音和数据呼叫。

[0078] 参见图 6, 被接入者装置 102 可包含例如一个或一个以上计算装置组件, 包含执行驻存的经配置逻辑的处理电路, 其中此计算装置包含例如微处理器、数字信号处理器 (DSP)、微控制器、便携式无线电话、个人数字助理 (PDA)、寻呼装置、无线调制解调器、PCMCIA 卡、接入终端、个人计算机, 和含有经配置以至少执行本文描述的操作的处理器和逻辑的硬件、软件和 / 或固件的任一合适组合。

[0079] 在一些方面中, 被接入者装置 102 包含存储器 402、通信模块 404 和处理器 406, 其各自经由总线 408 以通信方式耦合。存储器 402 可包含任一类型的易失性和 / 或非易失性存储器中的一者或一者以上, 包含所有已知类型的存储器, 其提供经配置逻辑的存储。另外, 虽然存储器 402 被展示为一种类型的存储器的一个连续单元, 但其它方面使用多个位置和 / 或多种类型的存储器作为存储器 402。另外, 存储器 402 可进一步包含装置识别符 410, 例如序列号、硬件识别符、全局识别符 (GID) 和 IP 地址、例如现时等的瞬态识别符等, 其可操作以唯一地识别被接入者装置 102。此外, 通信模块 404 经由总线 408 提供对装置 102 上的资源的输入和输出, 以及提供被接入者装置 102 与外部装置之间的输入和输出。另外, 处理器 406 根据经由总线 408 提供的指令和数据操作。

[0080] 另外,在一些方面中,被接入者装置 102 可包含运行时环境,其执行以提供在装置上运行的应用程序与处理器 412 和 / 或所述多个装置资源 103 中的预定装置资源之间的接口。此运行时环境可称为应用程序编程接口 (API) 412。一种此类运行时环境或 API 412 为由加利福尼亚圣地亚哥市的高通公司开发的 BREW® 软件平台。然而,在其它方面中,被接入者装置 102 适合于与例如操作以控制被接入者装置上的应用程序的执行的其它类型的运行时环境 (API) 一起使用。

[0081] 在一些方面中,通信模块 404 可包含多个通信接口 414,其各自提供到所述多个装置资源 103 中的对应一者或一者以上的连接。举例来说,多个通信接口 414 包含 (但不限于) 以下各项中的一者或任一组合:串行端口、除错端口、红外端口、Bluetooth™ 端口、网络套接字连接、通用串行总线 (USB)、FireWire™ 接口和高频无线局域网连接,例如无线保真度 (WiFi) 路径。

[0082] 此外,被接入者装置 102 可包含一个或一个以上输入装置 409 和一个或一个以上输出装置 411 以允许与被接入者装置 102 的用户交互。输入装置 409 可包含 (但不限于) 例如端口、键、麦克风、触敏显示器、鼠标等的装置。输出装置 411 可包含 (但不限于) 例如音频扬声器、显示器、触觉接口、机械振动器等的装置。输入装置 409 和输出装置 411 可通过总线 408 与其它装置组件以通信方式耦合。

[0083] 接入者装置 104 可例如经由本地连接 122 和通过网络 110 的远程路径中的任一者或两者,通过通信接口 414 来接入被接入者装置 102。通常,物理上连接的本地连接,例如硬连线串行连接,不需要用于交换数据的完整性保护或加密。此外,本地连接可能不需要鉴别协议,例如可防范中间人攻击的零知识证据 (zero-knowledge proof)。因此,虽然远程连接可能需要安全套接字层 (SSL) 或等效物,但较低安全性的通信协议对于本地连接来说为够用的。

[0084] 为了可在被接入者装置 102 上执行经由本地连接 122 和 / 或通过网络 110 的远程连接的有特权的动作而不损害装置的完整性,存储器 402 可包含动态接入授权模块 124。基于由接入者装置 104 供应的接入凭证 126,且进一步基于 AE 凭证 123,接入授权模块 124 可经配置以允许经授权用户 (例如,接入者装置 104) 具有关于被接入者装置 102 的高粒度的有特权特征。

[0085] 在一些方面中,接入授权模块 124 可预先加载到被接入者装置 102 的存储器 402 中。在其它方面中,接入授权模块 124 可为稍后添加的模块,其可经数字签署以用于鉴别目的。举例来说,接入授权模块 124 可由例如接入者装置 104 等的另一装置下载到被接入者装置 102。

[0086] 在接入授权模块 124 的加载之前,由被接入者装置 102 提供的操作环境大体上限制授予例如接入者装置 104 等的外部连接的装置的特权。一旦加载,接入授权模块 124 便变为看门人,从而提供在准予对与所述多个装置资源 103 中的一者或一者以上的有特权交互的接入方面的高粒度。特定来说,接入授权模块 124 与接入装置 (例如,接入者装置 104) 通信以接收授予特定接入特权 107 的 AE 颁予的接入凭证 126,其可特定联系到所述多个装置资源 103 中的一者或一者以上。举例来说,如上所述,AE 106 (图 1) 和被接入者装置 102 和 / 或装置资源 103 可预先就所述多个可用接入特权 105 中的每一者的定义,以及每一可用特权与对所述多个装置资源 103 中的至少一者的接入或交互之间的关联达成一致。此外,被

接入者装置 102 可另外基于所述多个通信接口 414 中的哪一者正被接入而限制对所述多个装置资源 103 中的预定装置资源的接入。在一些方面中,举例来说,接入授权模块 124 或每一装置资源 103 可包含接入控制数据库 418,以存储所述多个可用接入特权 105、相应装置资源 103 和(任选地)所述多个通信接口 414 之间的各种达成一致的关系。

[0087] 接入授权模块 124 可包含可操作以实施本文描述的功能性的硬件、软件、可执行指令和数据中的一者或任一组合。在一些方面中,接入授权模块 124 可包含接入授权逻辑 416,其可由处理器 406 执行以管理接入授权模块 124 的操作。

[0088] 在一些方面中,接入授权模块 124 可包含验证模块 420,其可操作以检查所接收接入凭证 126 和 AE 凭证 123,且确定真实性和特权范围。举例来说,验证模块 420 使用 AE 公钥 625 验证接入凭证 126 中含有的 AE 数字签名 109。此外,举例来说,验证模块 420 验证颁予的特权 107 在 AE 凭证 123 的范围内。基于此验证过程,验证模块 420 可颁予鉴别确定 422。鉴别确定 422 表示验证过程的结果,例如关于接入凭证和颁予的特权中的任一者或两者的“经鉴别”结果或“未经鉴别”结果。在对应于“经鉴别”结果的鉴别确定 422 的情况下,接入授权模块 124 接受接入凭证 126,进而基于包含在接入凭证 126 中的一个或一个以上颁予的接入特权 107 而允许相应装置资源 103 向接入者装置 104 提供接入。在对应于关于凭证的“未经鉴别”结果的鉴别确定 422 的情况下,接入授权模块 124 拒绝接入凭证 126,进而使得相应装置资源 103 不允许接入者装置 104 的接入。在对应于关于颁予的特权 107 的“未经鉴别”结果的鉴别确定 422 的情况下,取决于可配置的系统策略,接入授权模块 124 可完全拒绝接入,或可仅基于属于经批准的范围内的特权而允许接入。在任一情况下,验证模块 420 可以可操作以产生接入通知消息 424,且起始其经由通信模块 404 向提供接入凭证 126 的装置(例如,接入者装置 104)的传输,其中通知消息 424 传达凭证授权过程的结果。

[0089] 此外,接入授权模块 124 可检查由接入者装置 104 供应的身份证据以验证接入者装置 104 的身份。举例来说,身份证据可包含通信的交换,其中被接入者装置 102 可基于接入者公钥 208 而验证接入者装置的身份,接入者公钥 208 可被包含在接入凭证 126 内以便用以验证经授权接入者的身份。特定来说,接入授权模块 124 将能够基于使用接入者装置的对应私钥加密的所接收消息来验证接入者装置 104 的身份。另外,由接入者装置 104 提供的身份证据可初始与接入凭证 126 包含在一起。

[0090] 另外,在一些任选方面中,接入授权模块 124 可进一步包含控制模块 426,控制模块 426 可操作以确保向被准予接入的装置(例如,接入者装置 104)提供包含在“经鉴别”接入凭证 126 中的一个或一个以上颁予的接入特权 107 的界限或范围内的接入。举例来说,控制模块 426 检查从被准予接入的装置(例如,接入者装置 104)接收的请求 111 以确保包含在请求 111 中的每一所请求动作 428 属于至少一个颁予的特权 107 的范围内。举例来说,控制模块 426 可参考接入控制数据库 418,且将所请求动作 428 与基于所述一个或一个以上颁予的接入特权 107 而允许与之交互的一个或一个以上装置资源 103 进行比较。此外,在一些任选方面中,控制模块 426 可另外考虑所述多个通信接口 414 中的哪一者正由接入者装置 104 使用且进一步基于其而限制接入。由此,基于此控制过程,控制模块 426 可颁予控制确定 430。控制确定 422 表示控制过程的结果,例如“有效”结果或“无效”结果,例如所请求动作 428 分别属于一个或一个以上颁予的特权 107 的范围内或位于一个或一个以上颁予的特权 107 的范围外。在对应于“有效”结果的控制确定 430 的情况下,接入授权模

块 124 接受所请求动作 428 且允许被接入者装置 102 执行动作。在对应于“无效”结果的控制确定 430 的情况下,接入授权模块 124 拒绝所请求动作 428 且不允许动作发生。在任一情况下,但在“无效”结果情况下较为可能地,控制确定 430 可以可操作以产生控制消息 432 且起始经由通信模块 404 传输控制消息 432 到提供接入凭证 126 的装置(例如,接入者装置 104),其中控制消息 432 传达动作控制过程的结果。

[0091] 在其它方面中,接入授权模块 124 可不包含控制模块 426 和接入控制数据库 418,但控制接入的上述功能性可并入到相应装置资源 103 内。举例来说,每一装置资源 103 可包含控制模块 426 和接入控制数据库 418 的上述功能性中的全部或某部分。由此,在这些方面中,每一相应装置资源 103 可操作以确定所接收请求 111 是否在经验证接入凭证 126 的颁予的接入特权 107 的界限内,且相应地进行响应。在此情况的一些方面中,每一装置资源 103 具有与 AE 106 的信任关系,且进而已知关于装置资源 103 的所述多个接入特权 105(图 1)中的每一者的定义且就其达成一致,例如,其在颁予接入凭证 126 之前被预先确定。在此情况的其它方面中,每一特权 105(图 1)对应于相应装置资源 103 的已知方面,且因此无需建立预定关系,而是可仅基于接入凭证 126 的信任关系和验证而准予对相应装置资源 103 的一些方面的接入。

[0092] 另外,在一些方面中,接入授权模块 124 或每一相应装置资源 103 可以可操作以管理响应于请求 111 而向接入者装置 104 传输请求结果 434。请求结果 434 可包含与所述多个装置资源 103 中的相应一者对所请求动作 428 的处理相关的信息。举例来说,请求结果 434 可识别所请求动作中的一者或任一组合、与所述交互通联的所述多个装置资源 103 中的一者或一者以上和 / 或所请求动作的结果。

[0093] 另外,在一些方面中,接入授权模块 124 或每一装置资源 103 可以可操作以维护接入日志 436,其可存储和与 AE 106 和 / 或接入者装置 104 的通信相关的信息。举例来说,接入日志 436 可提供所述多个装置资源 103 与所述多个接入特权 105 之间的达成一致的关系、所接收接入凭证 126 以及关于与相应接入者装置 104 的交互的请求 111、所请求动作 428 和请求结果 434 的审计轨迹。类似的日志可由接入者装置 104 和 AE 106 维护以便使系统 100 内的动作相关,进而潜在地识别系统 100 的安全性违反。

[0094] 参见图 7,在至少一个方面中,接入者装置 104 可操作以从 AE 106 获得接入凭证 126 且将其转发到被接入者装置 102,被接入者装置 102 可操作以鉴别接入凭证 126 且基于颁予的接入特权 107 而允许与所述多个装置资源 103 的一个或一个以上预定交互。虽然说明为膝上型计算机,但接入者装置 104 可包含任一类型的有线或无线计算机化装置,例如蜂窝式电话、PDA、寻呼机和桌上型计算机。

[0095] 在一个方面中,举例来说,接入者装置 104 可包含存储器 502,其可操作以存储可由处理器 504 执行的应用程序和 / 或程序。存储器 502 和处理器 504 可经由总线 506 以通信方式耦合,总线 506 可进一步与通信模块 508 以通信方式耦合。

[0096] 通信模块 508 可包含允许实现接入者装置 104 内以及接入者装置 104 与外部装置之间的信息接收、传输和 / 或交换的硬件、软件、可执行指令和数据。举例来说,通信模块 508 可提供接入者装置 104 的组件之间以及接入者装置 104 与外部通信网络(例如网络 110)和外部装置(例如被接入者装置 102 和授权实体 106)之间的数据交换。举例来说,通信模块 508 可以可操作以经由本地连接 122 和 / 或经由网络 110 与被接入者装置 102 和 /

或 AE 106 通信。另外，通信模块 508 可包含分别用于向外部装置传输信息和从外部装置接收信息的传输和接收链组件。

[0097] 此外，接入者装置 104 可包含一个或一个以上输入装置 509 和一个或一个以上输出装置 511 以允许与接入者装置 104 的用户交互。输入装置 509 可包含（但不限于）例如端口、键、麦克风、触敏显示器、鼠标等的装置。输出装置 511 可包含（但不限于）例如音频扬声器、显示器、触觉接口、机械振动器等的装置。输入装置 509 和输出装置 511 可通过总线 506 与其它装置组件以通信方式耦合。

[0098] 此外，在一些任选方面中，接入者装置 104 可包含运行时环境，其执行以提供在装置上运行的应用程序和 / 或模块与处理器 504 之间的接口。此运行时环境可称为应用程序编程接口 (API) 510。一种此类运行时环境或 API 510 为由加利福尼亚圣地亚哥市的高通公司开发的 BREW® 软件平台。然而在其它方面中，接入者装置 104 可利用例如操作以控制接入者装置上的应用程序的执行的其它类型的运行时环境。

[0099] 另外，存储器 502 可包含装置识别符 512，例如序列号、硬件识别符、全局识别符 (GID)、全局唯一识别符 (GUID)、芯片识别符等，其可操作以唯一地识别接入者装置 104。

[0100] 此外，存储器 502 可包含接入模块 134，其可操作以提供与被接入者装置 102 和 / 或 AE 106 的通信。接入模块 134 可包含接入逻辑 514 以实施本文关于接入模块 134 描述的功能性的全部或某部分。举例来说，接入逻辑 514 可以可操作以接收接入凭证 126，且任选地接收 AE 凭证 123，且将其转发到被接入者装置 102 以便获得对被接入者装置 102 上的所述多个装置资源 103 中的一者或一者以上的接入。此外，接入逻辑 514 可以可操作以在一旦对被接入者装置 102 的接入经授权时便产生请求 111 和所请求动作 428。举例来说，接入逻辑 514 可经由通信模块 508 接收来自接入者装置 104 的用户的表示所请求动作 428 的输入，以便产生请求 111。另外，接入逻辑 514 可以可操作以接收和分析或进一步处理请求结果 434（如果存在）。

[0101] 另外，在一些方面中，接入模块 134 可以可操作以产生凭证请求 520 且经由通信模块 508 将请求 520 传输到 AE 106。举例来说，凭证请求 520 可例如经由装置识别符 512 识别接入者装置 104，以及所述多个接入特权 105（图 1）中的所请求的一者或一者以上。然而应注意，凭证请求 520 可能不是必要的，且 AE 106 和 / 或具有授权基础结构 304（图 4）的另一装置可单方面地将接入凭证 126 指派或颁予到接入者装置 104。

[0102] 在一些方面中，接入模块 134 可包含安全通信信息 516，其可操作以允许实现与例如 AE 106 和 / 或被接入者装置 102 等的外部装置的安全通信。举例来说，安全通信信息 516 可包含用于建立接入者装置 104 的身份且用于在一旦已建立身份时便以安全方式交换信息的协议。举例来说，可在接入者装置 104 将凭证请求 520 传输到 AE 106 的实例中使用这些协议。此外，举例来说，这些协议可用以在接入凭证 126 已被鉴别之后与被接入者装置 102 交换信息。举例来说，安全通信信息 516 可包含加密和解密机制 517，例如对称密钥，其可允许与例如使用公钥 / 私钥对等的其它加密机制相比较快的信息交换。另外，安全通信信息 516 可包含接入者装置私钥 518，其可用以加密和 / 或数字签署消息，和 / 或对以对应接入者装置公钥加密的所接收消息进行解密。接入者私钥 518 连同接入者公钥 208 是密钥对的一部分，其可存储在存储器 502 的非安全区域中。在一些方面中，可不利用接入者装置 104 与被接入者装置 102 之间的加密。举例来说，基于有效性指示符 210，在接入凭证 126

具有充分短寿命的情况下可不利用加密。另一方面,在一些其它方面中,可例如使用安全套接字层(SSL)来加密经由接口传输的数据。

[0103] 另外,在一些方面中,接入模块 134 可以操作以维护接入日志 522,其可存储和与 AE 106 和 / 或被接入者装置 102 的通信相关的信息。举例来说,接入日志 522 可提供凭证请求 520、所接收接入凭证 126 以及关于与相应被接入者装置 102 的交互的请求 111、所请求动作 428 和请求结果 434 的审计轨迹。如上所述,类似的日志可由被接入者装置 102 和 AE 106 维护以便使系统 100 内的动作相关,进而潜在地识别系统 100 内的安全性漏洞。

[0104] 参见图 8,在一个方面中,AE 106 可操作以动态地产生接入凭证 126,其授权接入者装置 104 执行与被接入者装置 102 的所述多个装置资源 103 中的一者或一者以上的通常受限的交互。虽然参见接入者装置 104 和被接入者装置 102 来论述,但应了解,AE 106 可操作以关于每一被接入者装置产生给多个接入者装置的接入凭证 126,且 / 或产生用于接入多个被接入者装置的接入凭证 126,和 / 或产生给一个或一个以上次级 AE 的一个或一个以上次级凭证(例如,次级凭证 129(图 2)),所述一个或一个以上次级 AE 可随后又自身授予接入凭证 126 或可授予可用以授予接入凭证 126 的一个或一个以上另外的次级凭证,等等。

[0105] AE 106 可包含任一类型的服务器、个人计算机、微型计算机、大型计算机或任一计算装置(专用或通用计算装置)中的至少一者。此外,可存在与 AE 106 相关联的单独的服务器或计算机装置,其协同工作以提供呈可用格式的数据给各方,且 / 或提供接入装置 102 与 AE 106 之间的数据流中的单独控制层。

[0106] 在一个方面中,AE 106 可包含存储器 602,其可操作以存储可由处理器 604 执行的应用程序和 / 或程序。存储器 602 和处理器 604 可经由总线 606 以通信方式耦合,总线 606 可进一步与通信模块 608 以通信方式耦合。

[0107] 通信模块 608 可包含允许实现在 AE 106 内以及 AE 106 与外部装置之间的信息接收、传输和 / 或交换的硬件、软件、可执行指令和数据。举例来说,通信模块 608 可提供 AE 106 的组件之间以及 AE 104 与外部通信网络(例如网络 110)和外部装置(例如被接入者装置 102 和接入者装置 104)之间的数据交换。举例来说,通信模块 608 可以操作以经由本地连接和 / 或经由网络 110 与被接入者装置 102 和 / 或接入者装置通信。另外,通信模块 608 可包含分别用于向外部装置传输信息和从外部装置接收信息的传输和接收链组件。

[0108] 此外,AE 106 可包含一个或一个以上输入装置 609 和一个或一个以上输出装置 611 以允许与 AE 106 的用户交互。输入装置 609 可包含(但不限于)例如端口、键、麦克风、触敏显示器、鼠标等的装置。输出装置 611 可包含(但不限于)例如音频扬声器、显示器、触觉接口、机械振动器等的装置。输入装置 609 和输出装置 611 可通过总线 606 与其它装置组件以通信方式耦合。

[0109] 另外,存储器 602 可包含凭证管理器模块 610,其可操作以基于 AE 凭证 123 为一个或一个以上接入者装置 104 和 / 或次级 AE 117(图 2)产生接入凭证 126 和 / 或次级凭证 129(图 2)以分别允许对一个或一个以上被接入者装置 102 的资源的接入且允许进一步的特权委派。在一些方面中,凭证管理器模块 610 包含凭证管理逻辑 612,其可由处理器 604 执行以执行本文描述的功能性。

[0110] 在一些方面中,凭证管理器模块 610 可包含特权建立模块 614,其可操作以与被接

入者装置 102 和 / 或每一相应装置资源 103 交互以建立所述多个装置资源 103 中的每一者与所述多个接入特权 105 中的相应接入特权之间的关系。任选地, 特权建立模块 614 可另外基于相应被接入者装置 102 上的所述多个通信接口 414 中的一者或一者以上来限制这些关系。此外, 此些关系也可取决于接入者装置信息 616 而变化, 接入者装置信息 616 例如为接入者装置识别符 410 (图 5)、接入者装置 104 的角色和 / 或接入者装置的用户、与接入者装置相关联的实体 (例如公司名称)、与接入者装置相关联的登录信息、与接入者装置相关联的安全性或加密机制等。特权建立模块 614 可将用于多个被接入者装置 618 中的每一者的这些关系存储在接入控制数据库 418 中。如上所述, 可关于每一被接入者装置 102 和 / 或每一装置资源 103 供授予的特权可例如当在系统 100 (图 1) 中实施特权委派时在 AE 106 之间变化。

[0111] 另外, 凭证管理模块 610 可进一步包含验证模块 620 以确认所述多个接入特权 105 中的哪一者可被授予相应的接入者装置 104 和 / 或次级授权实体 117 (图 2) 作为颁予的接入特权 107。验证模块 620 可响应于凭证请求 520 或基于 AE 106 的用户指派接入凭证 126 和 / 或次级凭证的动作来操作。举例来说, 验证模块 620 可例如基于与凭证请求 520 包含在一起的信息而验证接入者装置 104 和 / 或次级授权实体 117 (图 2) 的身份, 和 / 或可确认所述多个接入特权 105 中将被授予权单方面提出的接入者装置 104 的可允许接入特权。举例来说, 在凭证获取期间, 鉴别接入者装置 104 可允许对人员接入哪些装置 102 以及接入多少装置 102 的控制和可跟踪性。在例如在线服务器的情况下, 可使用例如需要对适当鉴别服务器的在线接入的 RSA 安全令牌验证来实施接入者装置的两因数鉴别。

[0112] 此外, 凭证管理模块 610 可进一步包含凭证产生器 622, 其可操作以产生接入凭证 126 和 / 或次级凭证 129 (图 2), 包含将接入实体 (AE) 私钥 624 应用于接入凭证 126 以形成 AE 数字签名 109, 且任选地附加 AE 凭证 123。应注意, AE 私钥 624 可由对应的 AE 公钥 625 证实。凭证产生器 622 可随后进一步可操作以起始经由通信模块 608 将接入凭证 126 传输至相应接入者装置 104。

[0113] 在一些方面中, AE 106 与接入者装置 104 之间的通信信道 (例如包含网络 110) 可利用例如安全套接字层 (SSL) 等的安全通信协议来保护传输到接入者装置 104 的接入凭证 126 的内容。

[0114] 另外, 在一些方面中, 凭证管理模块 610 可以可操作以维护接入日志 626, 其可存储和与接入者装置 104 和 / 或被接入者装置 102 和 / 或次级授权实体的通信相关的信息。举例来说, 接入日志 626 可提供凭证请求 520 和传输的接入凭证 126 以及关于每一被接入者装置的接入特权与装置资源之间的经建立关系的审计轨迹。如上所述, 类似的日志可由被接入者装置 102 和 / 或接入者装置 104 和 / 或次级授权实体维护以便使系统 100 内的动作相关, 进而潜在地识别系统 100 内的安全性漏洞。

[0115] 参见图 9, 系统 100 内的消息流程的一方面向接入者装置 104 提供预定特权以在被接入者装置 102 上执行通常受限的动作。在任选的事件 702 处, 接入者装置 104 可将包含凭证请求 520 (图 7) 的消息传输到 AE 106, 或传输到具有从主 AE 委派的凭证和特权的次级 AE。凭证请求消息可进一步包含额外的接入者装置相关信息。举例来说, 口令和 / 或密码、识别接入者装置 104 的数据、识别一个或一个以上被接入者装置 102 的数据、识别一个或一个以上所需特权的数据和 / 或识别在每一相应被接入者装置或关于每一装置资源执

行的所需动作的数据。在一些方面中,接入者装置 104 以用户名 / 口令组合 430 登录到 AE 106 上,随后使用口令鉴别逻辑来鉴别所述用户名 / 口令组合 430。在经鉴别后,接入者装置 104 可传输接入凭证请求以获取用于相应被接入者装置和 / 或相应装置资源的接入凭证 126。

[0116] 与 AE 106 的通信可例如使用驻存在接入者装置 104 上的市售网络浏览器来经由网络 110 进行。通过使用例如 HTTPS 等的安全协议(包含用户名 / 口令交换机制),可允许实现安全通信。

[0117] 在事件 704 处,AE 106 可通过在接收到凭证请求消息 520 时或在如由用户指示的独立操作时执行凭证管理模块 610(图 7)来产生接入凭证 126。举例来说,AE 106 可如上论述执行凭证管理模块 610(图 8)以处理凭证请求 520、验证接入者装置 104 和 / 或所请求动作 / 特权,且 / 或产生接入凭证 126(图 7)。

[0118] 在一个或一个以上替代方面中,例如当 AE 106 不包含用以准予对接入凭证 126 的请求 520 的适当机制和 / 或授权时,AE 106 可将凭证请求 520 转发到另一网络实体,例如较高层级次级 AE 和 / 或主 AE,或从具有较大授权的另一网络实体请求额外机制或授权。此过程在图 9 中在事件 706、708 和 710 处说明。举例来说,为了产生与被接入者装置 102 的运行时环境(例如,BREW®)兼容的动态产生的短期凭证,AE 106 接入与特权的授予相关的授权策略。因此,如事件 706、708 和 710 说明,如果 AE 106 不包含适当的策略 / 特权,那么其自身无法产生凭证 126,且因此其可连接到运营商授权基础结构 304 内的特定授权实体,例如较高层级次级或例如主 AE,且颁予对相应凭证的请求。因为并非所有特权 / 策略皆在所有服务器上可用,所以运营商授权基础结构 304 可包含多个服务器,包含根证书授权方(CA)(例如主授权实体)和一个或一个以上其它受信任 CA(例如次级授权实体),其各自可提供不同策略的子集,例如除错、语音邮件和内容传送等。

[0119] 举例来说,在任选的事件 706 处,AE 106 可将凭证请求消息传输到授权基础结构 304(图 5),凭证请求消息可包含对额外机制和 / 或授权的请求。在事件 706 处传输的凭证请求可为将从接入者装置 104 原始传输的凭证请求转发到 AE 106,或凭证请求可为例如新产生的消息,其可另外包含用以处理凭证请求 520 的额外机制 / 授权的请求。

[0120] 此外,举例来说,在任选的事件 708 处,授权基础结构 304 分析所接收的凭证请求消息,产生接入凭证,且 / 或提供用以处理凭证请求 520 的额外机制 / 授权。在任选的事件 710 处,授权基础结构 304 将凭证请求响应消息传输回到 AE 106。事件 710 的凭证请求响应消息可包含接入凭证 126、事件 708 处的分析的结果的通知(例如对凭证请求 520 的拒绝),和 / 或用于由 AE 106 使用以执行如上文论述的事件 704 的额外机制和 / 或授权。接入凭证响应消息可包含所授予特权的指示,且可经数字签署以保证数据的完整性和发送者的真实性。可在首先加密消息或不加密消息的情况下发送数字签名。如果像在使用 HTTPS 建立的连接时,授权基础结构 304 与 AE 106 之间的链路是安全的,或者如果证书的有效性周期极短,那么可不加密数字签署的接入凭证 126。

[0121] 在一些任选方面中,在 AE 106 上运行的加密模块 512(例如)经由 CA 的公钥验证与加密的所接收接入凭证相关联的散列。如果所接收散列通过验证,那么 AE 106 知道凭证尚未经修改且其是由私钥的所有者(例如,CA)发送。

[0122] 接入凭证 126 可包含数据字段且可如上所述格式化。另外,接入凭证 126 可包含

由 CA 授予的特权的列表。

[0123] 在事件 712 处,AE 106 将消息传输到接入者装置 104,所述消息包含接入凭证 126 且任选地包含 AE 凭证 123 或对其的某种参考,或在一些方面中,包含对所请求凭证的拒绝。因此,AE 106 进而向接入者装置 104 授予来自对应于所述多个装置资源 103 中的一者或一者以上的多个可用接入特权 105 的且在一些方面中关于给定被接入者装置 102 的一个或一个以上预定接入特权 107。

[0124] 在事件 714 处,接入者装置 104 可例如经由网络 110 和 / 或连接 122 建立与被接入者装置 102 的通信,且将接入凭证 126 且任选地将 AE 凭证 123 转发到被接入者装置 102 以尝试获得对被接入者装置 102 的所述多个装置资源 103 中的一者或一者以上的接入。此外,可关于接入者装置 104 的多个通信接口 414(图 5)中的预定一者来建立此通信,所述通信接口可与是否准予接入相关。大体上,物理上连接的本地路径,例如经由硬连线 USB 端口的连接,不需要对成批数据传送的完整性保护或加密。本地硬连线路径可能不需要可防范中间人情境的鉴别协议(例如,零知识证据)。因此,经由远程路径连接到被接入者装置 102 的接入者装置 104 可能需要 SSL 或等效物,而经由本地路径与被接入者装置 102 通信的接入者装置 104 可实施简单得多的鉴别和 / 或加密方法。

[0125] 在任选的事件 716 处,授权模块 124(图 5)可在被接入者装置缺少此模块的情况下被从接入者装置 104 传输到被接入者装置 102。在一些方面中,与接入凭证 126 的传输一致地传输授权模块 124,然而在替代方面中,可在任一时间点从接入者装置 104 或从另一网络装置传达授权模块 124。如先前论述,被接入者装置 102 可在制造时或销售点处预先配置有授权模块 124,且由此可能无需将授权模块 124 传达到被接入者装置 102。

[0126] 当经由非安全接入路径与被接入者装置 102 通信时,下载装置(在此实例中为接入者装置 104)可充当安全套接字层(SSL)服务器。因此,接入者装置 104 打开到被接入者装置 102 的连接,收听 SSL 请求,且协商 SSL。接入凭证 126 的转发(事件 714)或授权模块 124 的传达(事件 716)可包含对被接入者装置 102 的命令,例如再引导命令,其致使装置 102 发现且安装接入授权模块 124。

[0127] 一旦接入授权模块 124 安装在被接入者装置 102 上作为原始安装的部分或作为上述下载程序的部分,接入授权模块 124 便可操作以接收来自接入者装置 104 的通信,所述通信可包含允许接入者装置 104 在被接入者装置 102 上执行原本受限的动作的接入凭证 126。

[0128] 在事件 718 处,被接入者装置 102 通过以对应 AE 公钥 625 证实 AE 数字签名 109(图 3)且通过验证关于 AE 凭证 123 的颁予的特权 107 来鉴别 / 验证接入凭证 126。此外,被接入者装置 102 基于接入者公钥 208 而验证接入者装置 104 的身份。鉴别过程可导致接入者装置 104 和 / 或接入凭证 126 通过鉴别或部分通过鉴别,进而致使被接入者装置 102 接受接入凭证 126,且允许(例如)在接入凭证中的特权少于或等于 AE 凭证中的特权范围的情况下,根据基于 AE 凭证 123 批准的范围内的一个或一个以上颁予的接入特权 107 而对一个或一个以上装置资源 103 的接入。或者,鉴别过程可导致接入者装置 104 和 / 或接入凭证 126 被拒绝鉴别,在此情况下不接受接入凭证且拒绝对所述一个或一个以上装置资源 103 的接入。在事件 720 处,被接入者装置 102 传达表示鉴别过程的结果的通知消息 422(图 6),所述结果例如为“通过鉴别”结果、“部分通过鉴别”结果或“未通过鉴别”结果。

[0129] 在事件 722 处,如果接入者装置 104 接收到指示接入凭证已通过鉴别或部分通过

鉴别的通知消息,那么接入模块 134(图 7)可产生包含接入动作 428(图 7)的请求 111(图 7)。举例来说,接入逻辑 514(图 7)可经由输入装置 509(图 7)从接入者装置 104 的用户接收表示所请求动作 428 的输入以便产生请求 111。在事件 724 处,将请求 111 传输到被接入者装置 102。

[0130] 在事件 726 处,被接入者装置 102 检查从接入者装置 104 接收的请求 111 以确保包含在请求 111 中的每一所请求动作 428 均属于至少一个颁予的特权 107 的范围内。举例来说,对应于所请求动作 428 的每一相应装置资源 103 或接入授权模块 124 可实施动作控制功能。举例来说,控制功能包含每一相应装置资源 103 或控制模块 426(图 6)操作以参考接入控制数据库 418(图 6),且控制功能将所请求动作 428 与所述一个或一个以上颁予的接入特权 107 进行比较。在任选的事件 728 处,被接入者装置 728 可将控制消息 432(图 6)传输到接入者装置 104,其中控制消息 432 传达动作控制过程的结果。

[0131] 参见图 10,在一个方面中,被接入者装置确保例如在初始接入尝试时或在授权之后的接入尝试时与经授权接入者装置发生交互的方法包含要求接入者装置证明其身份。任选地,在事件 740 处,方法包含接入者装置 104 请求对一个或一个以上装置资源 103 的接入特权,其可针对给定被接入者装置 102 而进一步指定。举例来说,此请求可包含接入者装置 104 将接入者公钥 208 和身份证据转发到 AE 106。

[0132] 在事件 742 处,AE 106 独立地或响应于经由事件 740 接收的请求而产生凭证 126。举例来说,如果响应于请求,那么 AE 106 可验证由接入者装置 104 供应的身份证据,且可进一步在颁予的接入凭证 126 中包含接入者公钥 208。

[0133] 在事件 744 处,AE 106 将接入凭证 126 颁予到接入者装置 104。

[0134] 在事件 746 处,接入者装置 104 接收接入凭证 126,且产生消息以发送到被接入者装置 102。

[0135] 在事件 748 处,通过接入模块 134,接入者装置 104 将包含接入凭证 126 的消息转发到被接入者装置 102。任选地,所述消息可包含 AE 凭证 123 和 / 或对其的某种参考。

[0136] 在事件 750 处,被接入者装置 102 接收消息和接入凭证 126,验证接入凭证 126,且随后产生响应消息以验证接入者装置 104 的身份。举例来说,响应消息可包含现时或某种其它随机数据,其在事件 752 处传输到接入者装置 104。

[0137] 在事件 754 处,接入者装置 104 以接入者私钥签署现时或随机数据,且在事件 756 处将此信息发送回到被接入者装置 102。

[0138] 在事件 758 处,被接入者装置 102 以例如包含在经验证接入凭证 126 中的被接入者公钥 519 对经签署的现时或随机数据进行解密。如果经解密现时或随机数据匹配于来自事件 750 的原始现时或随机数据,那么被接入者装置 102 具有接入者装置 104 的身份证据,且进一步交换可发生。如果不存在匹配,那么接入者装置 104 的身份未通过验证,且将不允许对装置资源的接入。

[0139] 在事件 760 处,被接入者装置 102 向接入者装置 104 发送确认身份证据或拒绝确认的消息。

[0140] 在事件 762 处,如果接入者装置 104 的身份经证明,那么可根据经验证接入凭证 126 内的一个或一个以上接入特权 107 发生与一个或一个以上装置资源 103 的交互。

[0141] 应注意,在接入凭证 126 的初始身份验证和批准之后,可在执行与身份证据相关

的以上过程的某个部分之后实施进一步接入尝试,例如接入凭证可能无需每次都被再提交。

[0142] 因此,方法的此方面允许被接入者装置 102 确认其正在与被颁予接入凭证 126 的适当接入者装置 104 打交道。然而应注意,可利用其它方法来确认接入者装置 104 的身份。

[0143] 参见图 11,提供在接入者装置处获得对被接入者装置资源的接入的方法 800 的流程图。应了解,所列出的动作排序是用于阐释目的,且这些动作可以任一次序发生。在任选事件 802 处,向授权实体做出对接入凭证的请求。授权实体可为主 AE 或具有从主 AE 委派的授权 / 特权的次级 AE。请求可另外包含额外的接入者装置相关信息,例如口令和 / 或密码、识别接入者装置 104 的数据、识别一个或一个以上被接入者装置 102 的数据和 / 或识别执行每一相应被接入者装置的所需动作的数据。对接入凭证的请求是任选事件,因为在一些方面中,可在无需传输请求的情况下将接入凭证传达到接入者装置。

[0144] 在事件 804 处,接收接入凭证,例如由授权实体授予的接入凭证。如先前提及,可响应于请求而接收接入凭证,或 AE 106 和 / 或授权基础结构 304 可单方面地将接入凭证 126 授予和颁予到接入者装置 104。或者,AE 106 可在装置上预加载一个或一个以上接入凭证。而且,或者,可接收接入凭证识别符而非实际的接入凭证。接入凭证可包含由被接入者装置在鉴别接入凭证时使用的一个或一个以上接入特权和 AE 数字签名。在事件 806 处,传输接入凭证且任选地相应的 AE 凭证或对其的参考以例如用于尝试接入被接入者装置的目的。举例来说,在一个方面中,例如经由网络 110 和 / 或连接 122 而与被接入者装置 102 建立通信,且将接入凭证 126 转发到被接入者装置 102 以尝试获得对被接入者装置 102 的所述多个装置资源 103 中的一者或一者以上的接入。所建立的通信可关于接入者装置 104 的多个通信接口 414(图 6)中的预定一者,所述通信接口可与是否准予接入相关。或者,在事件 806 处,可传输接入凭证识别符而非实际接入凭证。

[0145] 在任选的事件 808 处,可从授权实体接收授权模块。举例来说,在一些方面中,被接入者装置 102 可能尚未具有用于评估所接收接入凭证 126 的接入授权模块 124,且如果接入者装置 104 未预加载有接入授权模块 124,那么接入者装置 104 可例如从 AE 106 和 / 或从授权基础结构 304 接收此模块。在任选事件 810 处,又可将授权模块传输到被接入者装置 102。在替代方面中,授权模块可从 AE 106 直接或从授权基础结构 304 传达到被接入者装置 102。如先前提及,授权模块可由被接入者装置在证实接入凭证之前的任一时间点且不一定以上文论述的次序接收。举例来说,在传输接入凭证 126 之前,接入者装置 104 可了解到被接入者装置 102 需要接入授权模块 124,且因此接入者装置 104 可在凭证传输之前或与凭证传输一起传输所述模块。

[0146] 在事件 812 处,接收接入授权的结果。接入授权的结果将指示授权已经授予、部分授予或授权已被拒绝。如果接入凭证授权已经授予或部分授予,那么在事件 814 处,可产生交互 / 接入的请求 111(图 6)且传输到被接入者装置 102。举例来说,可经由通信模块 508(图 6)接收表示所请求动作 428(图 6)的用户输入以便产生请求 111。

[0147] 在任选的事件 816 处,可接收请求结果 434(图 6)和 / 或应答。请求结果 434 可包含与所述多个装置资源 103 中的相应一者对所请求动作 428 的处理相关的信息。举例来说,请求结果 434 可识别所请求动作中的一者或任一组合、所述多个装置资源 103 中与交互相关联的一者或一者以上和 / 或所请求动作的结果。

[0148] 参见图 12, 提供根据一个方面的准予被接入者装置处的装置资源接入的方法 900 的流程图。在任选事件 902 处, 接收且加载授权模块。如先前提及, 可在授权接入凭证之前的任一时间点从接入者装置 104、AE 106 或任一其它联网装置传达授权模块。在替代方面中, 授权模块可在制造时或在销售点被预先配置。

[0149] 在事件 904 处, 接收接入凭证。接入凭证至少将包含与一个或一个以上装置资源相关联的一个或一个以上接入特权以及与 AE 106 相关联的数字签名。在一些方面中, 应注意, 可接收接入凭证识别符, 且接入凭证的接收可基于从在接入凭证识别符中识别的位置或网络装置检索接入凭证。在事件 906 处, 例如通过用 AE 公钥证实 AE 数字签名、通过验证关于 AE 凭证 123 的颁予的特权 107 的范围以及任选地通过验证接入者装置 104 的身份来授权 / 验证接入凭证, 且将授权的结果传输到接入者装置 104。

[0150] 一旦授予授权且已将相关验证通知 422(图 6) 传输到接入者装置 104, 那么在事件 908 处, 可从接入者装置 104 接收对接入 / 交互的请求 111(图 6) 且随后进行证实。需要对请求的证实以确保对接入者装置 104 提供在包含于“经鉴别”接入凭证 126 中的所述一个或一个以上颁予的接入特权 107 的界限内的接入。举例来说, 证实可包含参考接入控制数据库 418(图 6) 以将所请求的交互 / 接入与基于所述一个或一个以上颁予的接入特权 107 而允许与之交互的一个或一个以上装置资源 103 进行比较。在任选事件 910 处, 可产生证实结果且传输到接入者装置 104, 从而向接入者装置 104 告知请求证实的结果。

[0151] 在事件 912 处, 一旦已证实对接入 / 交互的请求, 便基于请求执行与装置资源的所请求交互。交互的实例包含(但不限于)利用经授权除错工具且执行装置维护功能, 例如无线装置的供应和再配置、管理用于同步工具程序的地址簿、文件系统接入、例如图片、音乐、铃声等的内容的上载和 / 或下载, 以及数据在装置之间的传送。在任选事件 914 处, 可响应于请求 111 而产生请求结果 434(图 6) 或应答且将其传输到接入者装置 104。请求结果 434 可包含与对接入 / 交互的请求的处理相关的信息。举例来说, 请求结果 434 可识别所请求动作中的一者或任一组合、所述多个装置资源 103 中与交互相关联的一者或一者以上和 / 或所请求动作的结果。

[0152] 上文揭示的设备和方法呈现用于向未知的第一计算装置提供对例如无线手持机等的第二计算装置的有特权的接入的受控机制。举例来说, 本文论述的设备和方法可用以允许第一装置能够从第二装置复制内容以传送到新装置, 和 / 或将新内容传送到第二装置上。此外, 举例来说, 本文论述的设备和方法可允许第一装置在第二装置上执行受限制的系统配置管理功能。另外, 举例来说, 本文论述的设备和方法可允许第一装置接入和操纵存储在第二装置上的专用用户数据和 / 或网络配置数据。此外, 应了解, 可实施许多其它情境以利用由本发明设备和方法提供的经授权接入功能性。

[0153] 结合本文所揭示的方面描述的各种说明性逻辑、逻辑块、模块、处理器和电路可用通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件或其经设计以执行本文描述的功能的任何组合来实施或执行。通用处理器可以是微处理器, 但在替代方案中, 所述处理器可以是任何常规处理器、控制器、微控制器或状态机。处理器还可实施为计算装置的组合, 例如 DSP 与微处理器的组合、多个微处理器、结合 DSP 核心的一个或一个以上微处理器或任何其它此类配置。

[0154] 此外,结合本文所揭示的方面描述的方法或算法的步骤和 / 或动作可直接在硬件中、在由处理器执行的软件模块中或在所述两者的组合中体现。软件模块可驻留在 RAM 存储器、快闪存储器、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可装卸盘、CD-ROM 或此项技术中已知的任何其它形式的存储媒体中。实例存储媒体可耦合到处理器,使得处理器可从存储媒体读取信息和向存储媒体写入信息。在替代方案中,存储媒体可与处理器成一体式。此外,在一些方面中,处理器和存储媒体可驻留在 ASIC 中。另外,ASIC 可驻留在用户终端中。在替代方案中,处理器和存储媒体可作为离散组件驻留在用户终端中。另外,在一些方面中,方法或算法的步骤和 / 或动作可作为代码或指令中的一者或任一组合或集合而驻留在可为计算机程序产品的全部或部分的机器可读媒体和 / 或计算机可读媒体上。此外,在一些方面中,方法或算法的步骤和 / 或动作可体现在一个或一个以上处理器的一个或一个以上模块中。

[0155] 虽然以上揭示内容展示说明性方面和 / 或方面,但应注意,可在不脱离所附权利要求书所界定的所描述方面和 / 或方面的范围的情况下在本文中作出各种变化和修改。此外,尽管可能以单数形式描述或主张所描述的方面的元件,但除非明确规定限于单数形式,否则也预期复数形式。另外,除非另外规定,否则任何方面和 / 或方面的全部或一部分可与任何其它方面和 / 或方面的全部或一部分一起利用。

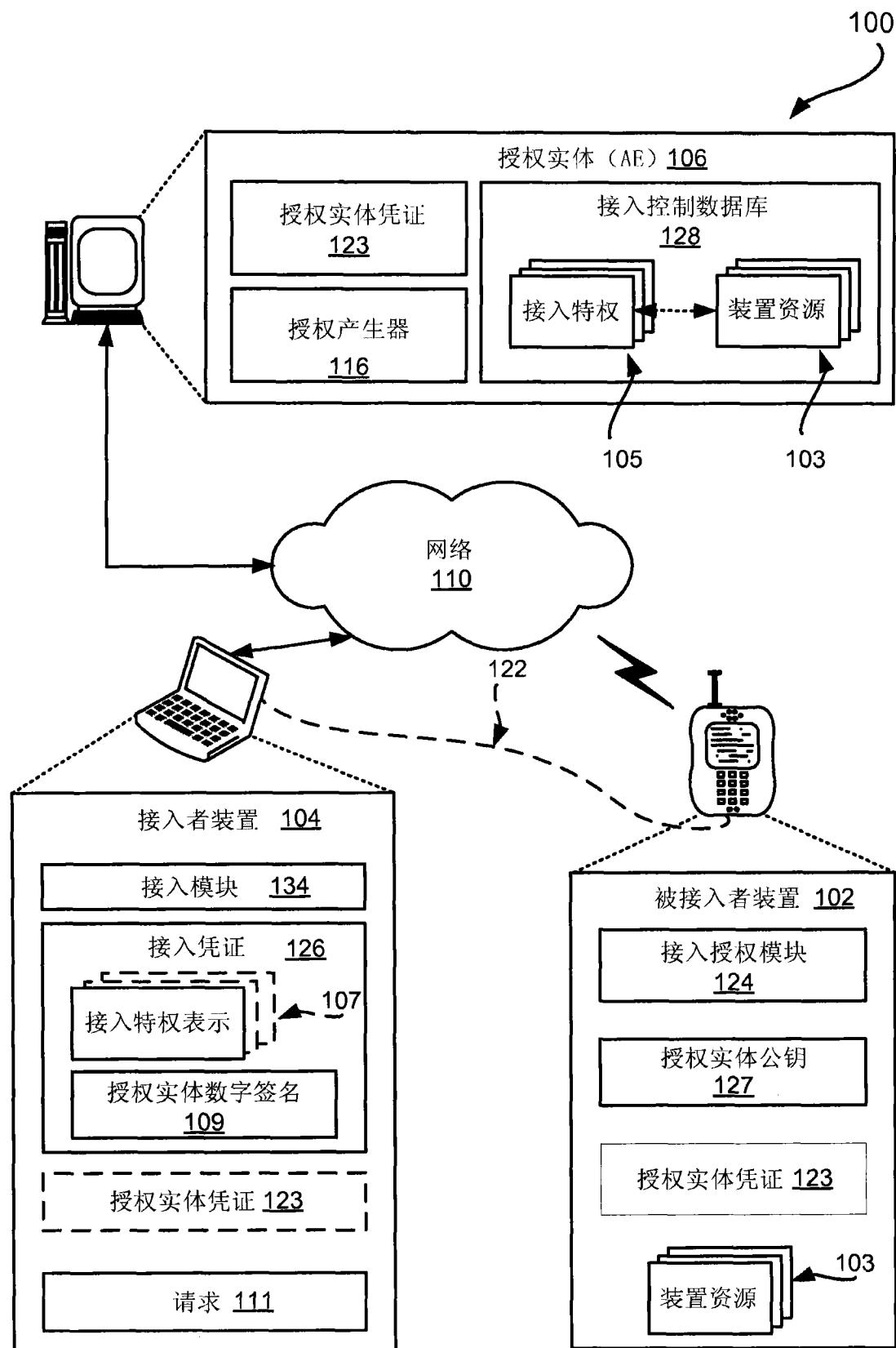


图 1

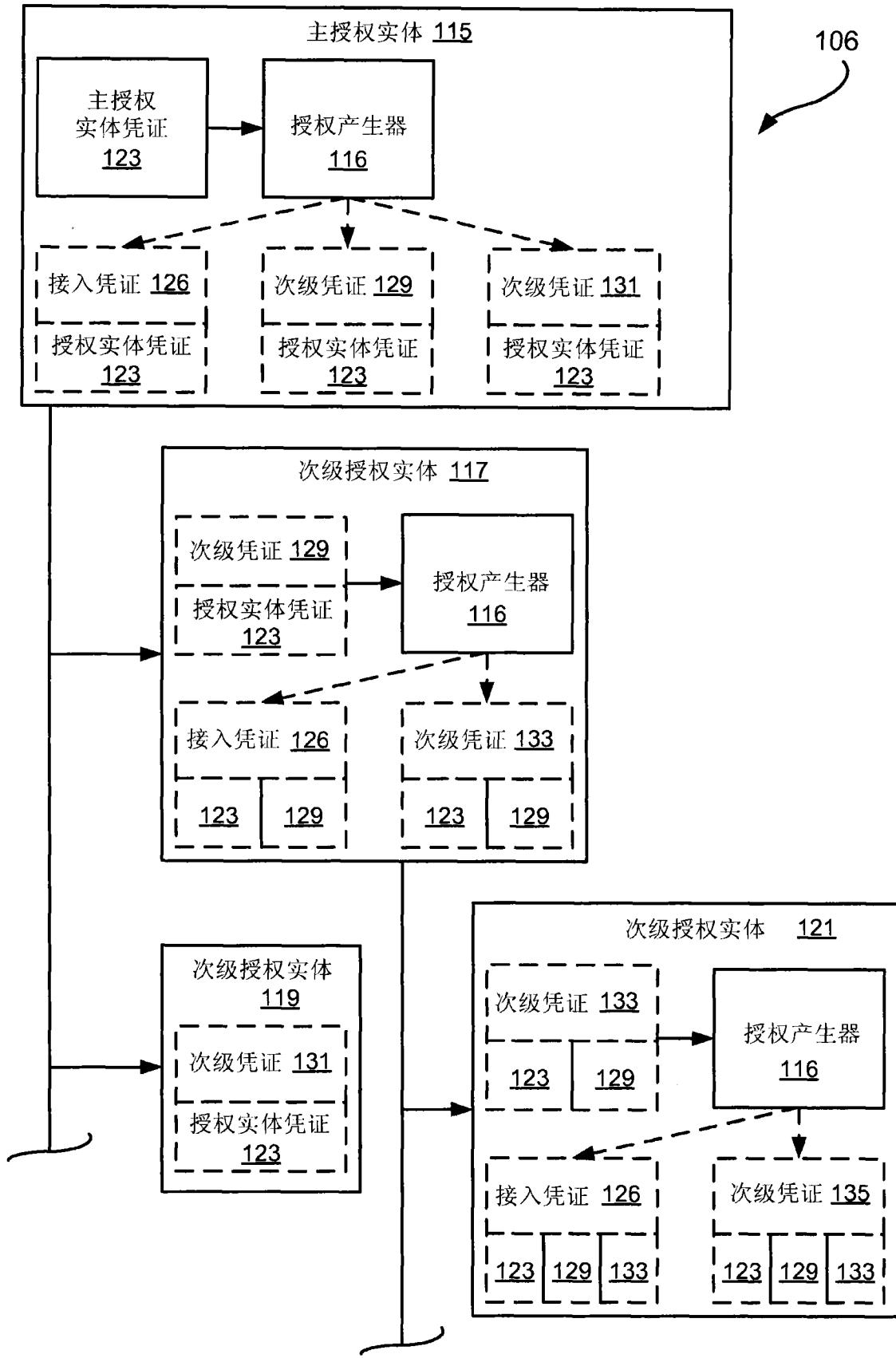


图 2

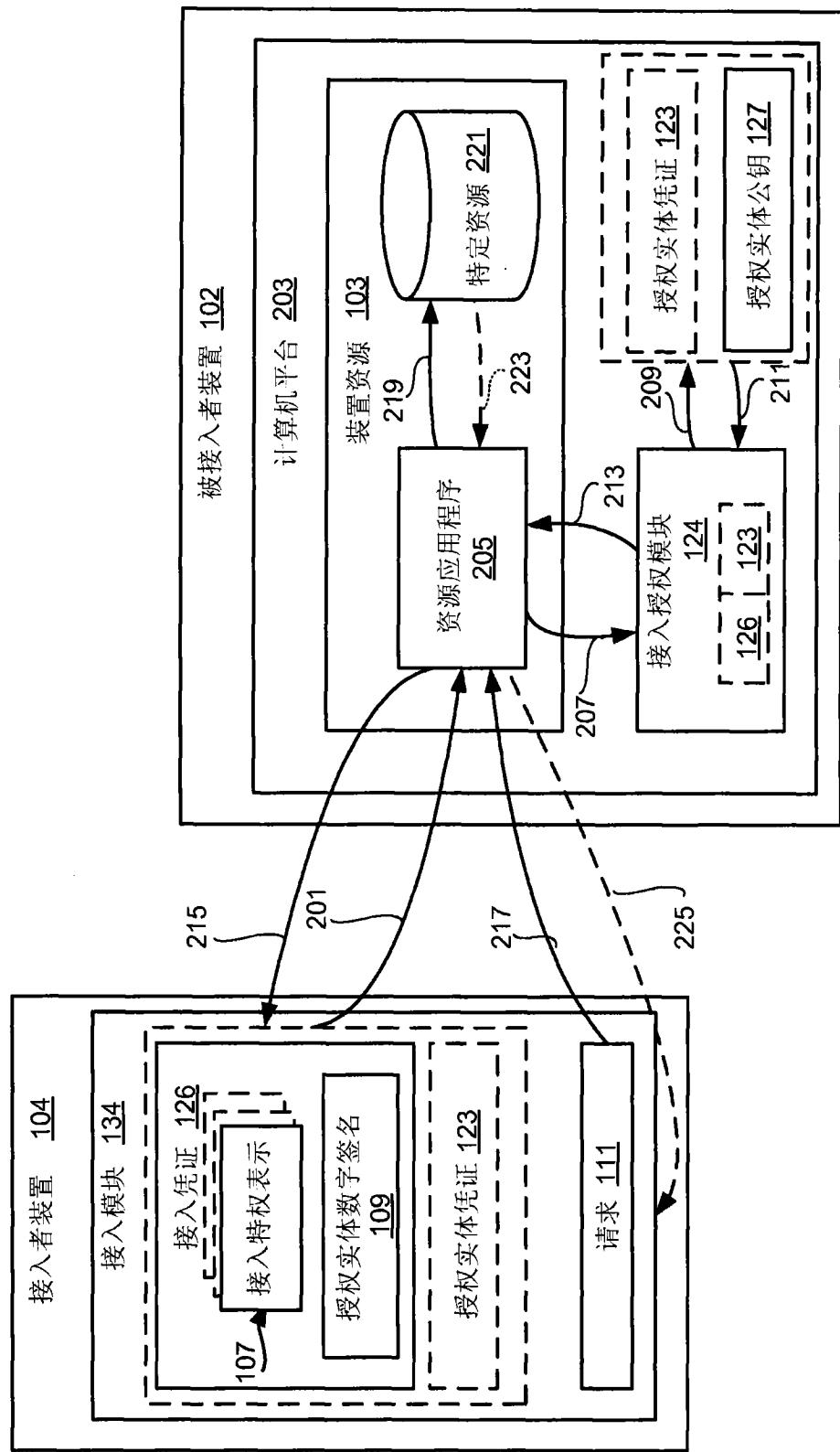


图 3

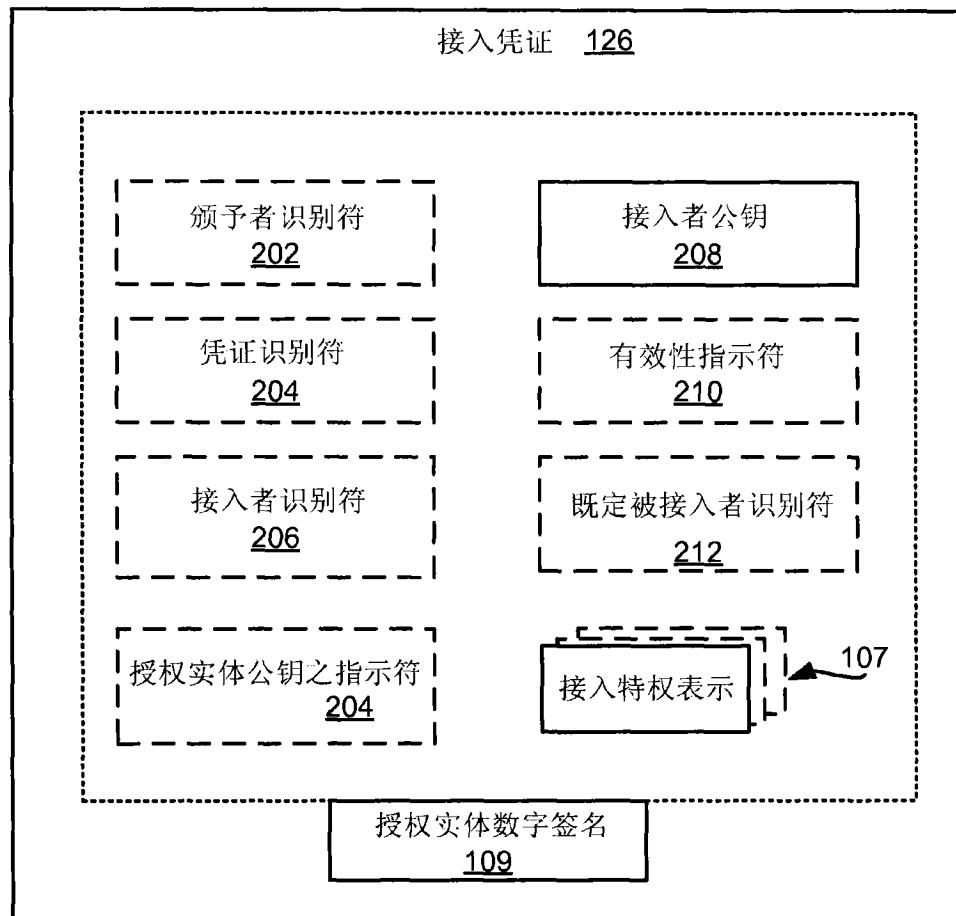


图 4

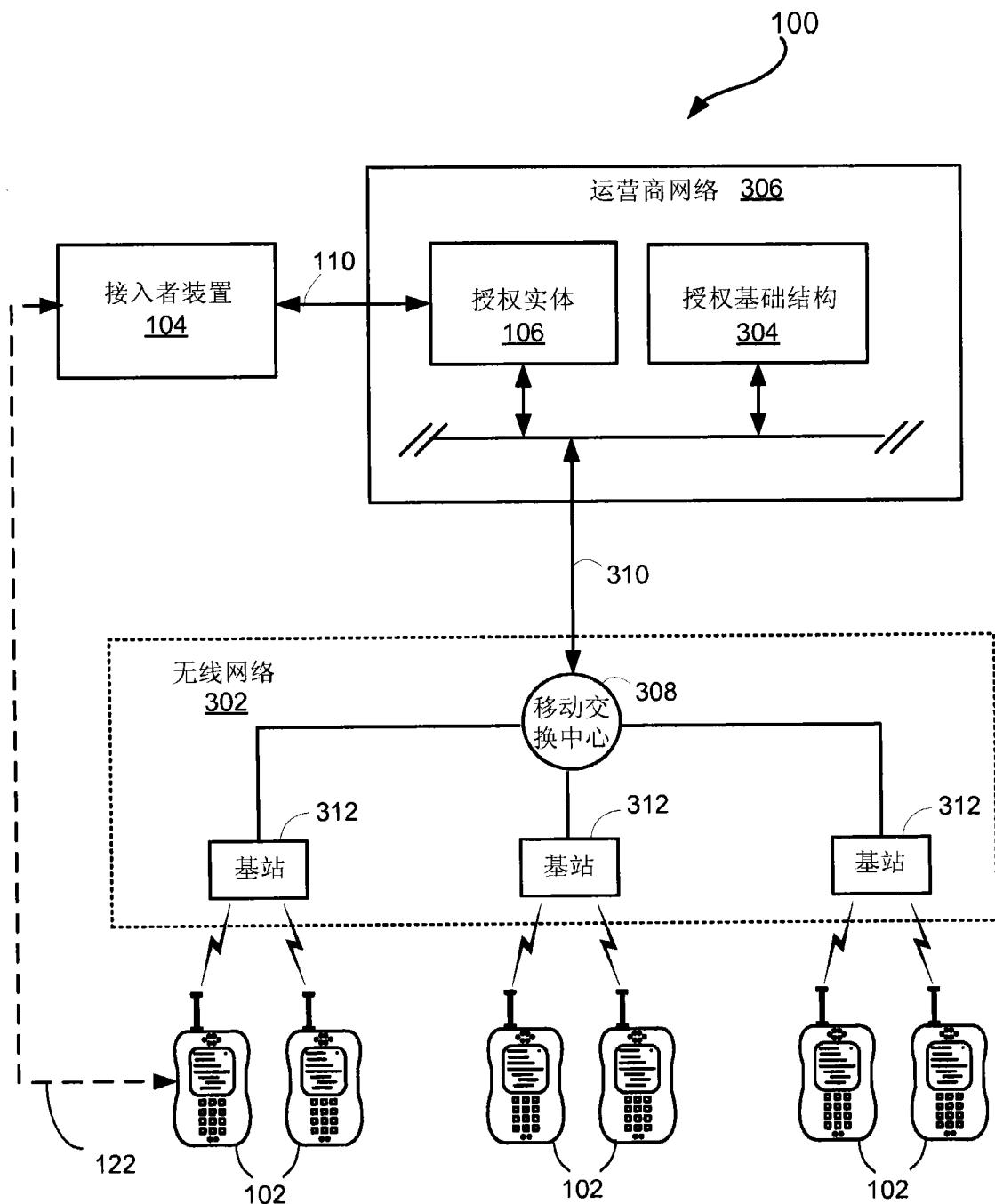


图 5

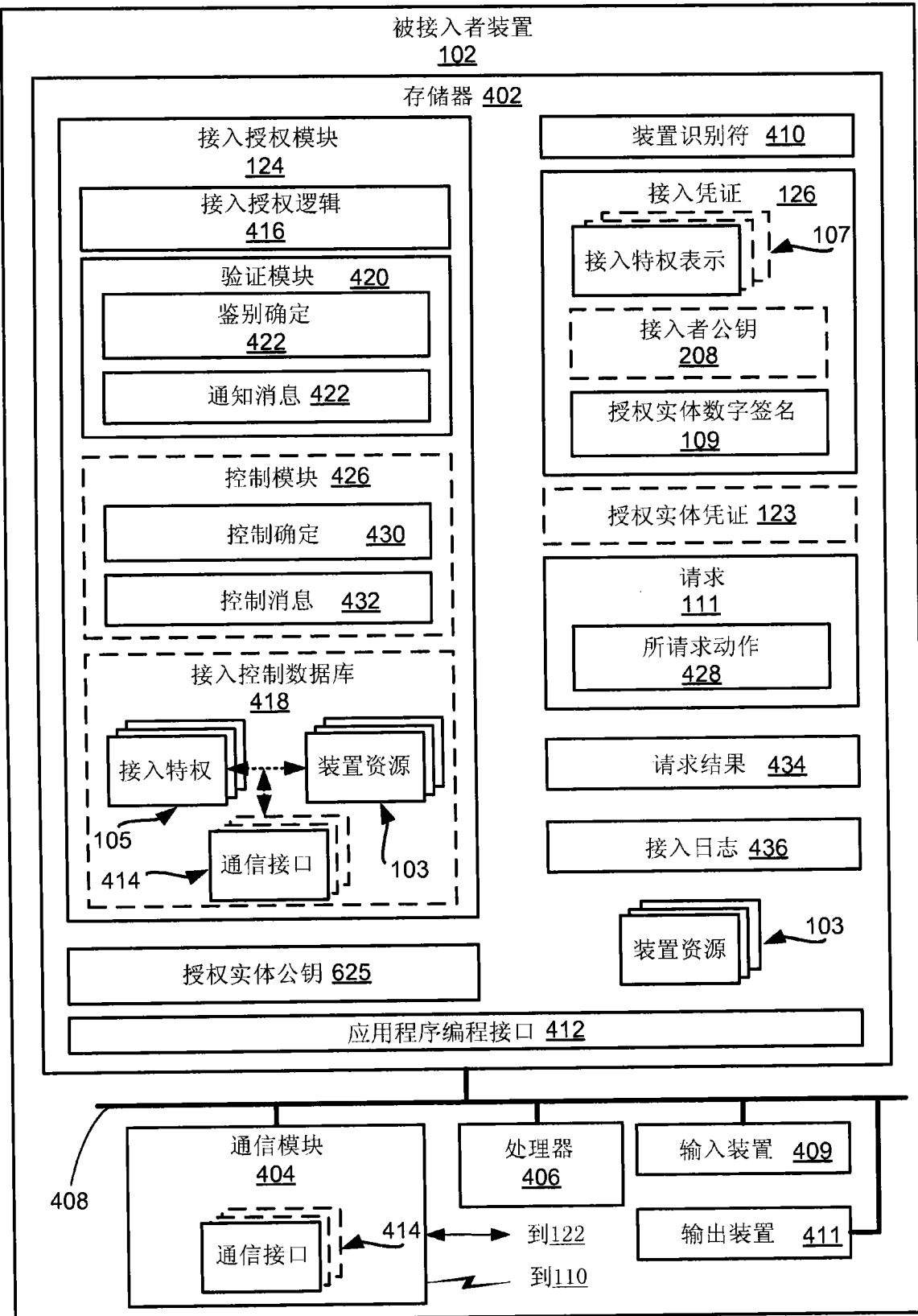


图 6

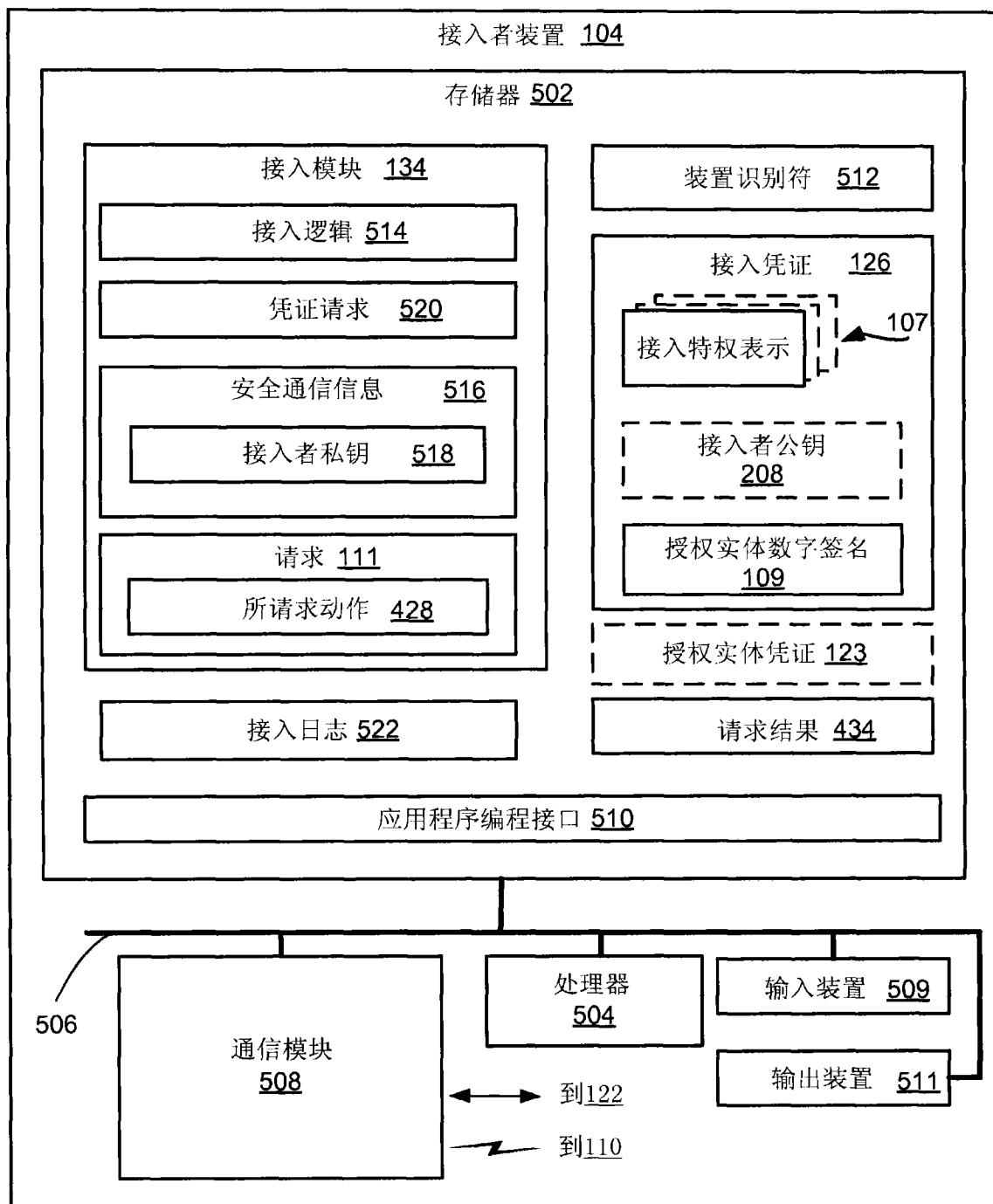


图 7

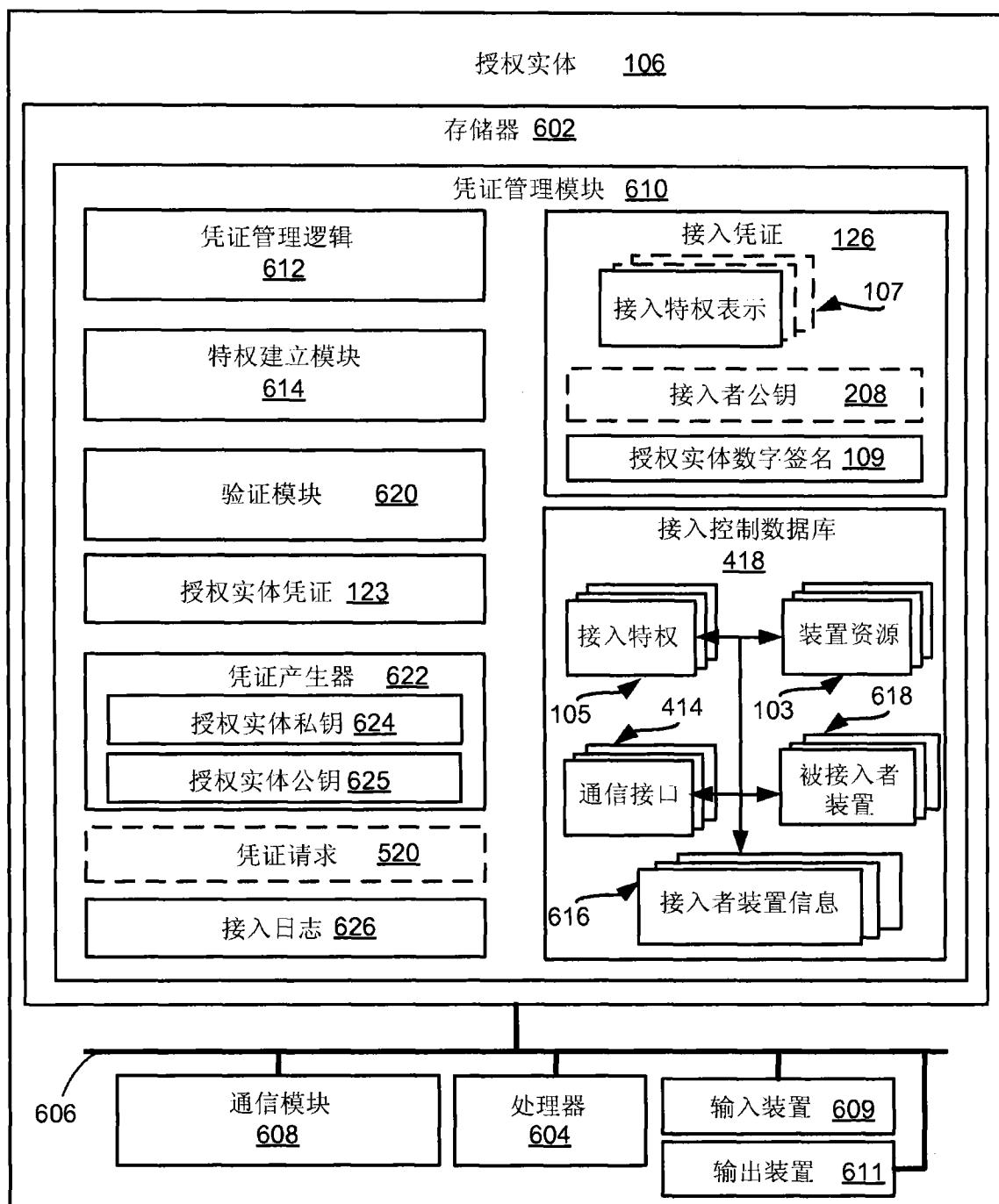


图 8

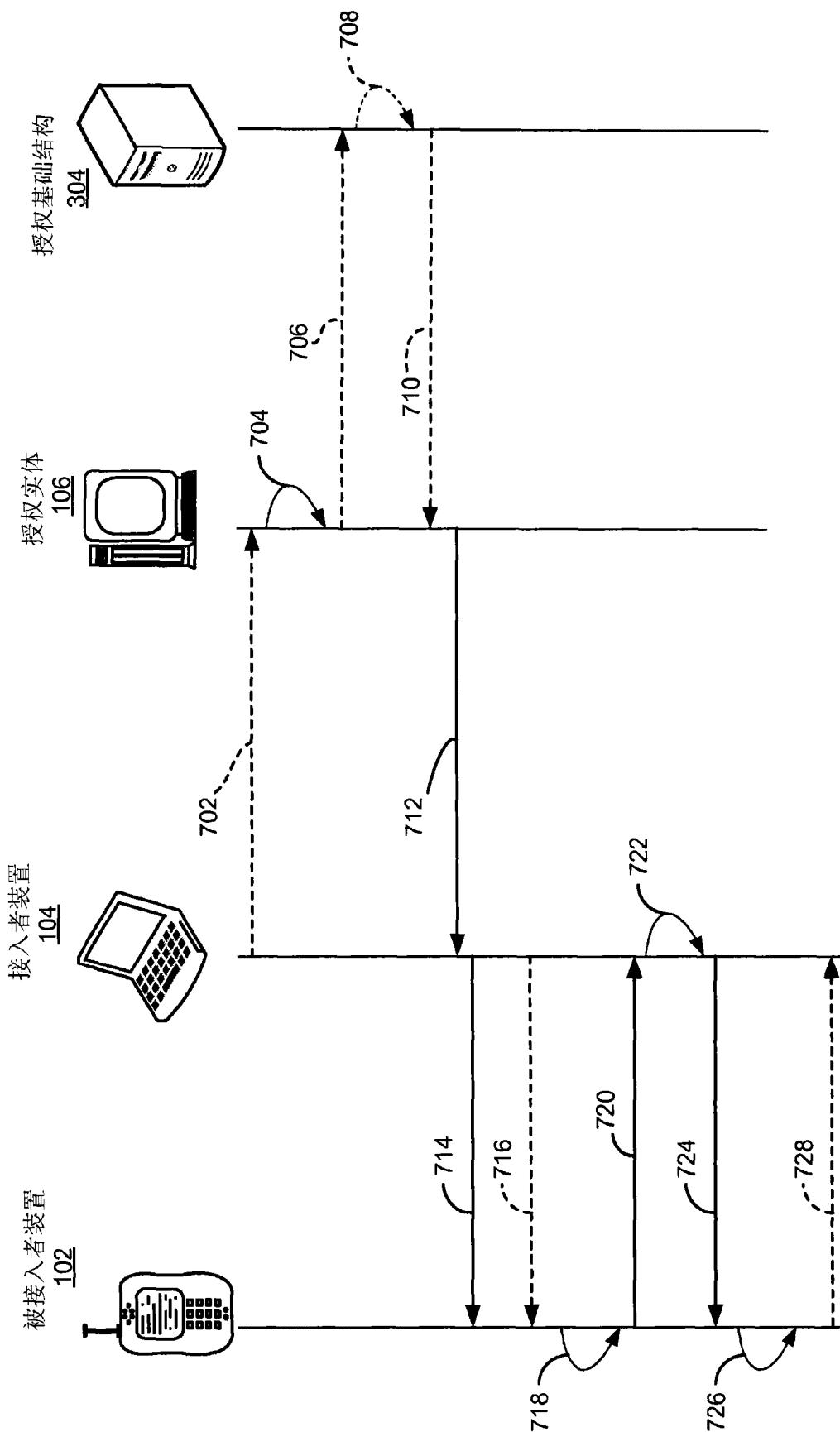


图 9

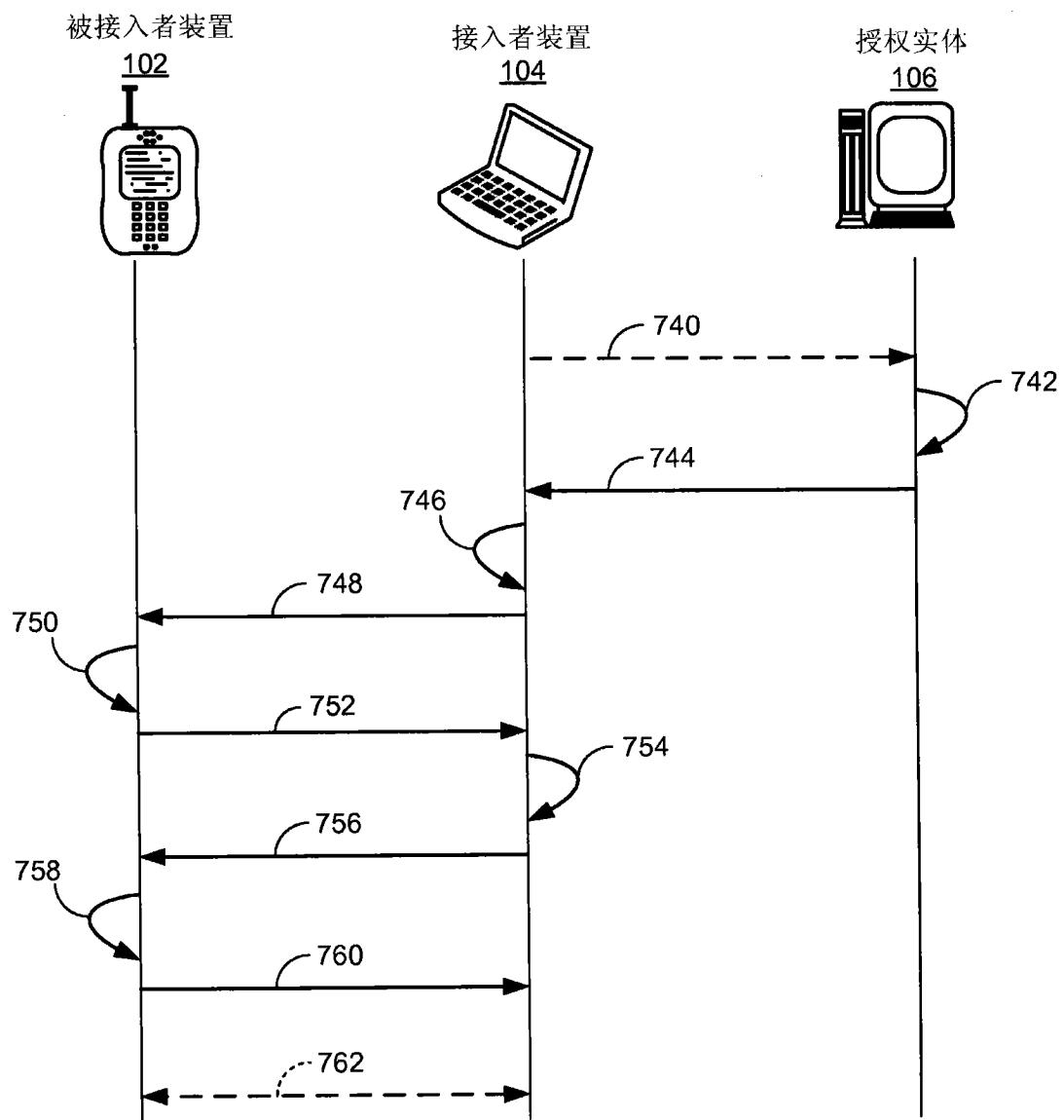


图 10

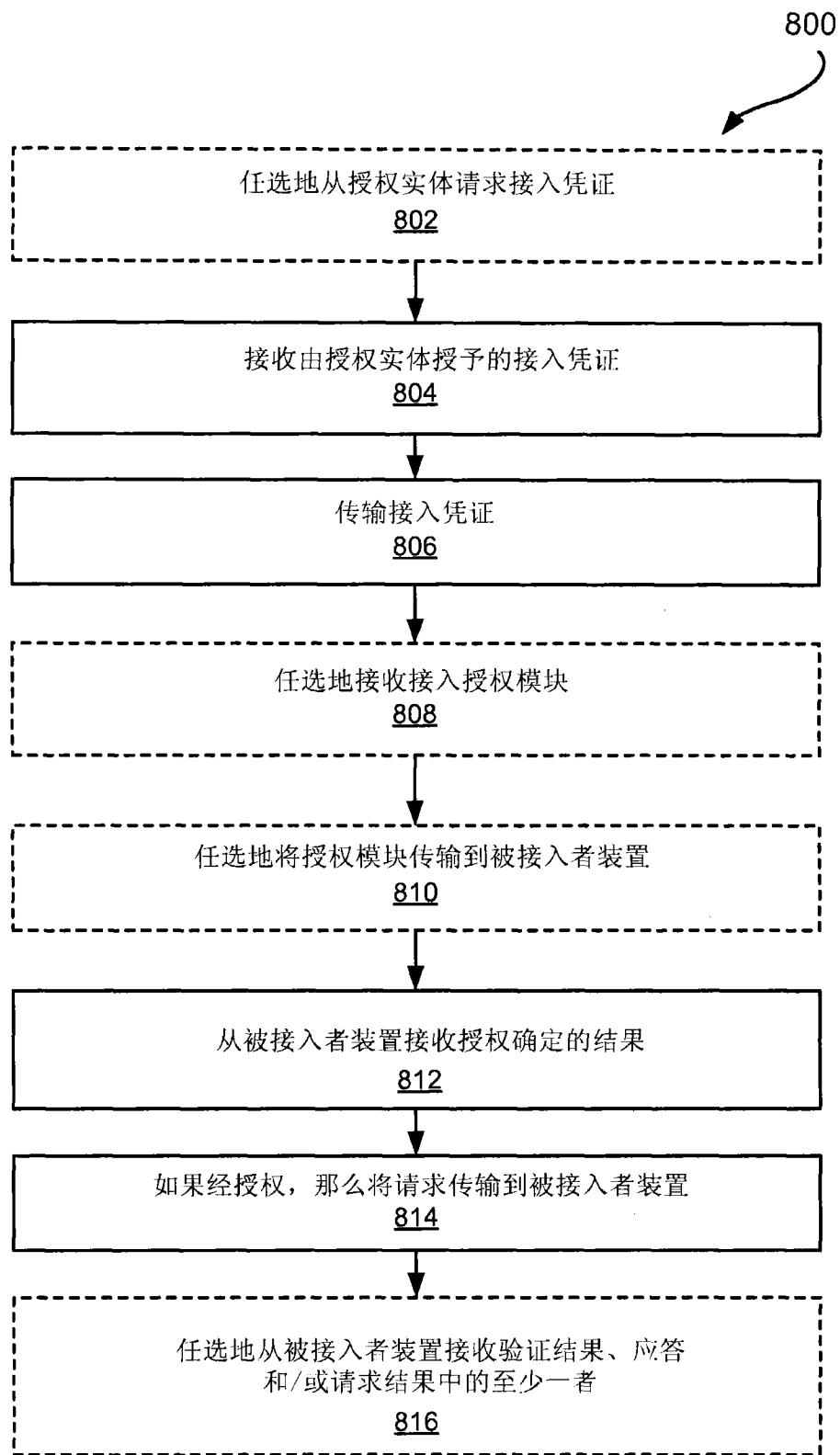


图 11

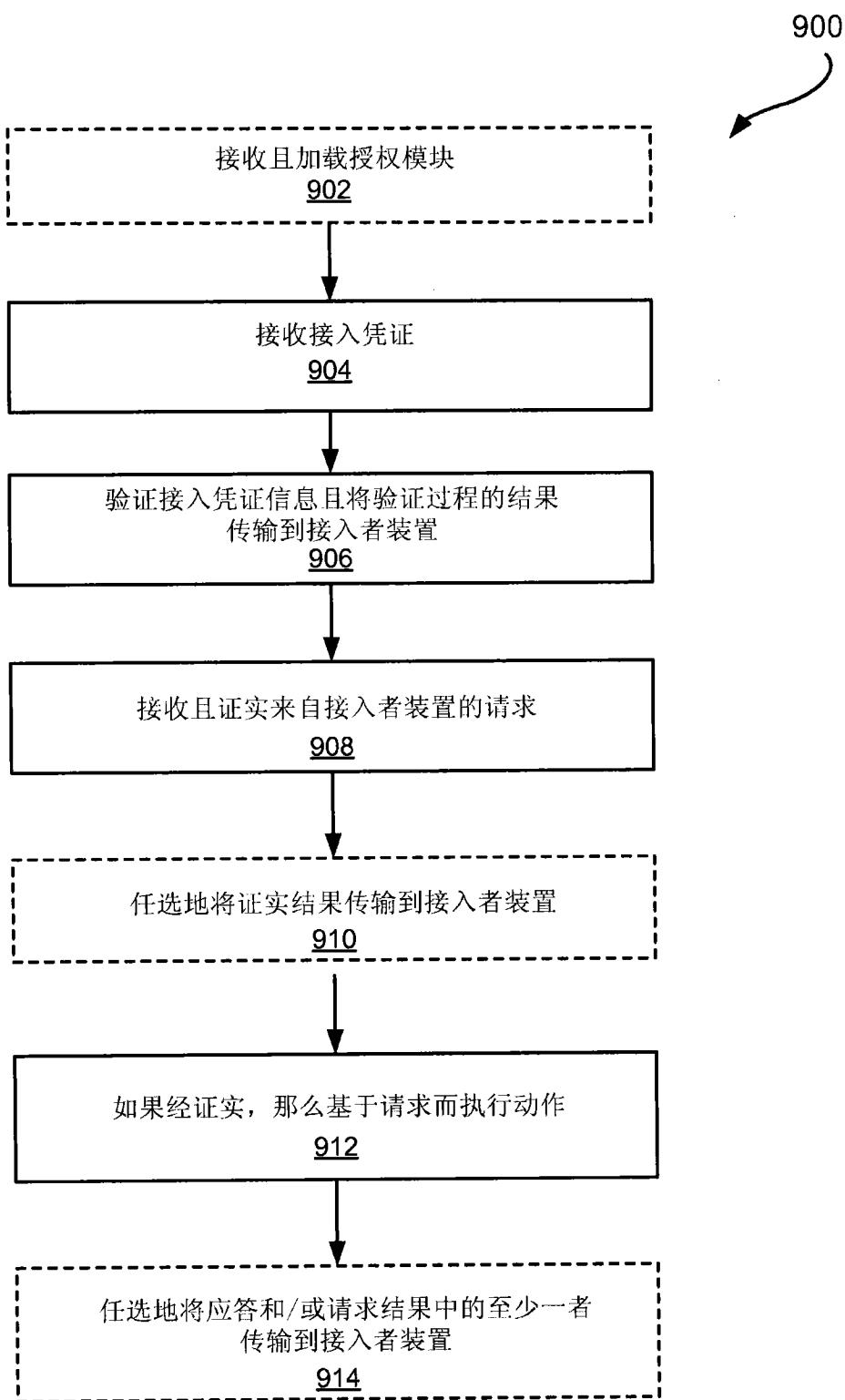


图 12