(19) Deutsches Patent- und Markenamt

(10) **DE 20 2016 107 078 U1** 2017.07.20

(12) # Gebrauchsmusterschrift

(21) Aktenzeichen: **20 2016 107 078.3**
(22) Anmeldetag: **16.12.2016**
(47) Eintragungstag: **12.06.2017**
(45) Bekanntmachungstag im Patentblatt: **20.07.2017**

(51) Int Cl.: ***G06F 21/45*** (2013.01)
G06F 21/31 (2013.01)

(30) Unionspriorität:
62/305,994 **09.03.2016** **US**
15/156,415 **17.05.2016** **US**

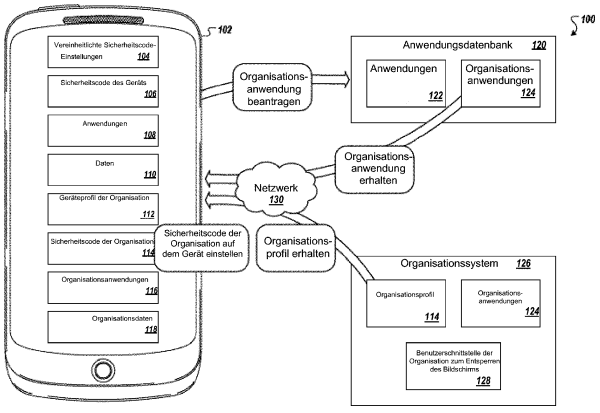
(73) Name und Wohnsitz des Inhabers:
GOOGLE INC., Mountain View, Calif., US

(74) Name und Wohnsitz des Vertreters:
Maikowski & Ninnemann Patentanwälte Partnerschaft mbB, 10707 Berlin, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Sicherheitscodes für Computergeräte**

(57) Hauptanspruch: Computergerät konfiguriert zum:
Identifizieren, dass ein Anwendungsprogramm, das auf dem Computergerät installiert ist, einem Profil für eine Organisationen zugeordnet ist;
Identifizieren, dass das Profil für die Organisation einen Sicherheitscode erfordert, um einen Zugriff auf das Anwendungsprogramm zu ermöglichen;
infolge der durchgeführten Identifikation, dass das Profil der Organisation den Sicherheitscode benötigt, um einen Zugriff auf das Anwendungsprogramm zu ermöglichen, Bereitstellen einer Benutzerschnittstelle, mithilfe der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät separate Sicherheitscodes verwenden sollte, um das Computergerät zu entsperren und einen Zugriff auf das Anwendungsprogramm bereitzustellen;
infolge des Bereitstellens der Benutzerschnittstelle Erhalten einer ersten Benutzereingabe, die spezifiziert, dass das Computergerät einen einzelnen Sicherheitscode verwenden muss, um sowohl das Computergerät zu entsperren als auch um einen Zugriff auf das Anwendungsprogramm bereitzustellen;
nachdem die erste Benutzereingabe spezifiziert hat, dass das Computergerät einen einzelnen Sicherheitscode verwenden muss und während das Computergerät gesperrt ist, Erhalten einer zweiten Benutzereingabe, die den einzelnen Sicherheitscode spezifiziert, um sowohl das Computergerät zu entsperren als auch um einen Zugriff auf das Anwendungsprogramm bereitzustellen und infolgedessen dazu führt, dass das Computergerät entsperrt wird; und
nachdem das Computergerät entsperrt worden ist, Erhalten einer Benutzereingabe, welche ein Benutzerschnittstellenelement auswählt, um das Anwendungsprogramm zu aktivieren und infolgedessen das Anwendungsprogramm aktiviert, ohne zu erfordern, dass ein Sicherheitscode über die Benutzereingabe bereitgestellt wird.



Beschreibung

TECHNISCHES GEBIET

[0001] Dieses Dokument betrifft im Allgemeinen die Verwendung von Sicherheitscodes in Bezug auf Computergeräte und Anwendungen.

HINTERGRUND

[0002] Ein Computergerät kann die Eingabe eines Sicherheitscodes erfordern, z. B. eines Passworts oder von Fingerabdruckdaten, um Zugriff auf die im Computergerät gespeicherten Daten bereitzustellen. Wenn das Computergerät gesperrt ist und die Benutzereingabe erhält, welche den Zugriff auf die Daten anfordert, stellt das Computergerät eine Benutzerschnittstelle bereit, welche die Benutzereingabe des Sicherheitscodes anfordert. Sobald das Computergerät die Benutzereingabe erhält, vergleicht das Computergerät die Benutzereingabe mit einem gespeicherten Sicherheitscode, um zu ermitteln, ob die Benutzereingabe mit dem gespeicherten Sicherheitscode übereinstimmt.

[0003] Das Computergerät kann das gespeicherte Passwort verschlüsseln, um einen unbefugten Zugriff auf den gespeicherten Sicherheitscode zu verhindern. Zum Beispiel kann das Computergerät einen Hash-Wert auf einen Sicherheitscode anwenden und den gehashten Sicherheitscode speichern. Wenn das Computergerät die Benutzereingabe durch die Benutzerschnittstelle erhält, wendet das Computergerät denselben Hash-Wert auf die Benutzereingabe an und vergleicht den gehashten Sicherheitscode, um zu ermitteln, ob ein Zugriff auf das Computergerät bereitgestellt werden soll.

ALLGEMEINE BESCHREIBUNG

[0004] Dieses Dokument beschreibt Techniken, Verfahren, Systeme und sonstige Mechanismen zum Auswählen der Zusammenführung von Passwörtern. Ausführungsformen sind durch die Gegenstände der unabhängigen Ansprüche gegeben. Die abhängigen Ansprüche definieren Merkmale weiterer beispielhafter Ausführungsformen. Weiterhin sind weitere Ausführungsformen nachstehend beschrieben:
In Ausführungsform 1 handelt es sich um ein Verfahren, welches Folgendes umfasst: das von dem Computergerät durchgeführte Identifizieren, dass ein auf dem Computergerät installiertes Anwendungsprogramm einem Profil für eine Organisationen zugeordnet ist; das mittels eines Computergeräts durchgeführte Identifizieren, dass das Profil für die Organisation einen Sicherheitscode erfordert, um einen Zugriff auf das Anwendungsprogramm zu ermöglichen; infolge der zuvor durchgeführten Identifikation, dass das Profil der Organisationen den Sicherheitscode benötigt, um einen Zugriff auf das Anwendungsprogramm zu ermöglichen, das von dem Computergerät durchgeführte Bereitstellen einer Benutzerschnittstelle, mithilfe der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät separate Sicherheitscodes verwenden sollte, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen; das von dem Computergerät und infolge des Bereitstellens der Benutzerschnittstelle durchgeführte Erhalten einer ersten Benutzereingabe, die spezifiziert, dass das Computergerät einen einzelnen Sicherheitscode verwenden muss, um sowohl das Computergerät zu entsperren als auch um einen Zugriff auf das Anwendungsprogramm bereitzustellen; nachdem die erste Benutzereingabe spezifiziert hat, dass das Computergerät einen einzelnen Sicherheitscode verwenden muss und während das Computergerät gesperrt ist, das von dem Computergerät durchgeführte Erhalten einer zweiten Benutzereingabe, die den einzelnen Sicherheitscode spezifiziert, um sowohl das Computergerät zu entsperren als auch um einen Zugriff auf das Anwendungsprogramm bereitzustellen und infolgedessen dazu führt, dass das Computergerät entsperrt wird; und nachdem das Computergerät entsperrt worden ist, das vom Computergerät durchgeführte Erhalten einer Benutzereingabe, welche ein Benutzerschnittstellenelement auswählt, um das Anwendungsprogramm zu aktivieren und infolgedessen das Anwendungsprogramm aktiviert, ohne zu erfordern, dass ein Sicherheitscode über die Benutzereingabe bereitgestellt wird.

[0005] In Ausführungsform 2 handelt es sich um das Verfahren aus Ausführungsform 1, welches Folgendes umfasst: das von dem Computergerät durchgeführte Identifizieren, dass eine Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren und um auf das Anwendungsprogramm zuzugreifen; während das Computergerät gesperrt ist und während die Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren und um auf das Anwendungsprogramm zuzugreifen, das von dem Computergerät durchgeführte Bereitstellen eines ersten Entsperrens der Benutzerschnittstelle; mittels des ersten Entsperrens der Benutzerschnittstelle das von dem Computergerät durchgeführte Erhalten einer dritten Benutzereingabe, welche einen Sicherheitscode für das Entsperren des Computergeräts spezifiziert und infolgedessen das Computergerät entsperrt; während das Computergerät entsperrt ist, das vom Computergerät durchgeführte Empfangen einer vierten Benutzereingabe, die das Benutzerschnittstellenelement zur Aktivierung des Anwendungsprogramms auswählt; infolge der vierten Benutzereingabe, welche eine Präsentation der Benutzerschnittstelle für das Anwendungsprogramm erfordert, das von dem Computergerät durchgeführte Bereitstellen

eines zweiten Entsperrens der Benutzerschnittstelle; das von dem Computergerät über das zweite Entsperren der Benutzerschnittstelle durchgeführte Erhalten einer fünften Benutzereingabe, die einen Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, und als Antwort auf das Erhalten der fünften Benutzereingabe, welche den Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, das mittels des Computergeräts durchgeführte Aktivieren des Anwendungsprogramms.

[0006] In Ausführungsform 3 handelt es sich um das Verfahren der Ausführungsformen 1 oder 2, wobei: das Erhalten der dritten Benutzereingabe, welche den Sicherheitscode für das Entsperren des Computergeräts das Erhalten der dritten Benutzereingabe umfasst, welche den Sicherheitscode für das Entsperren des Computergeräts spezifiziert, der die ersten Auflagen des Sicherheitscodes erfüllt, und das Erhalten der fünften Benutzereingabe, welche einen Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, umfasst das Erhalten der fünften Benutzereingabe, welche einen Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, der die zweiten Auflagen des Sicherheitscodes erfüllt, die im Profil für die Organisation spezifiziert sind, wobei die zweiten Auflagen des Sicherheitscodes sich von den ersten Auflagen des Sicherheitscodes unterscheiden.

[0007] In Ausführungsform 4 handelt es sich um das Verfahren der Ausführungsformen 1 bis 3, welche Folgendes umfassen: das von dem Computergerät durchgeführte Erhalten einer sechsten Benutzereingabe, welche einen neuen Organisationssicherheitscode spezifiziert; das von dem Computergerät und unter Verwendung der sechsten Benutzereingabe durchgeführte Ermitteln, ob der neue Organisationssicherheitscode die Auflagen des Sicherheitscodes erfüllt, die im Profil für die Organisation definiert werden; und das von dem Computergerät und als Antwort auf das Ermitteln, dass der neue Organisationssicherheitscode den Auflagen des Sicherheitscodes entspricht, die im Profil der Organisation definiert werden, durchgeführte Bereitstellen der Benutzerschnittstelle, mit der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät separate Sicherheitscodes verwenden sollte, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen.

[0008] In Ausführungsform 5 handelt es sich um die Ausführungsformen 1 bis 4, welche Folgendes umfassen: das von dem Computergerät als Antwort auf das Erhalten der fünften Benutzereingabe, welche den Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, durchgeführte Bereitstellen des Zugriffs auf das Anwendungsprogramm und alle Anwendungsprogramme, die dem Profil für die Organisation zugeordnet werden, einschließlich mindestens eines anderen Anwendungsprogramms, das dem Profil für die Organisation zugeordnet worden ist.

[0009] In Ausführungsform 6 handelt es sich um das Verfahren der Ausführungsformen 1 bis 5, welches Folgendes umfasst: während die Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen und als Antwort auf das Erhalten der dritten Benutzereingabe, welche den Sicherheitscode für das Entsperren des Computergeräts spezifiziert, das von dem Computergerät durchgeführte Ermitteln, dass das Computergerät separate Sicherheitscodes verwendet, um das Computergerät zu entsperren und um Zugriff auf das Anwendungsprogramm bereitzustellen; und bis zum Erhalt der Benutzereingabe, welche den Organisationssicherheitscode spezifiziert, das von dem Computergerät durchgeführte Verhindern des Zugriffs auf alle Anwendungsprogramme, die dem Profil für die Organisationen einschließlich des Anwendungsprogramms zugeordnet sind.

[0010] In Ausführungsform 7 handelt es sich um das Verfahren der Ausführungsformen 1 bis 6, wobei das vom Computergerät durchgeführte Bereitstellen der zweiten Benutzerschnittstelle zum Entsperren als Antwort auf die vierte Benutzereingabe, welche eine Präsentation der Benutzerschnittstelle für das Anwendungsprogramm erfordert, das vom Computergerät durchgeführte Bereitstellen der zweiten Benutzerschnittstelle zum Entsperren als Antwort auf die vierte Benutzereingabe, welche eine Präsentation der Benutzerschnittstelle für das Anwendungsprogramm umfasst, die sich von der ersten Benutzerschnittstelle zum Entsperren unterscheidet.

[0011] In Ausführungsform 8 handelt es sich um das Verfahren der Ausführungsformen 1 bis 7, wobei das vom Computergerät durchgeführte Bereitstellen der zweiten Benutzerschnittstelle zum Entsperren als Reaktion auf die vierte Benutzereingabe, welche eine Präsentation der Benutzerschnittstelle für das Anwendungsprogramm erfordert, die sich von der ersten Benutzerschnittstelle zum Entsperren unterscheidet, das Bereitstellen einer zweiten Benutzerschnittstelle mit einem Bild umfasst, das von der Organisation oder einem Administrator dieser spezifiziert ist.

[0012] In Ausführungsform 9 handelt es sich um das Verfahren der Ausführungsformen 1 bis 8, welches das Folgende umfasst: das von dem Computergerät durchgeführte Erhalten von Anweisungen, um den

Zugriff auf das Anwendungsprogramm und auf sonstige andere Anwendungsprogramme, die dem Profil der Organisation zugeordnet sind, zu verhindern, wobei die Anweisungen, als Reaktion auf eine zuvor definierte Menge erfolgloser Versuche einen Sicherheitscode für den Zugriff auf das Anwendungsprogramm einzugeben, oder als Reaktion auf eine Eingabe des Administrators, um einen Zugriff auf das Anwendungsprogramm zu verhindern, erhalten wird und das von dem Computergerät und als Reaktion auf das Erhalten der Anweisungen, um den Zugriff auf das Anwendungsprogramm und auf sonstige andere Anwendungsprogramme zu verhindern, die dem Profil der Organisation zugeordnet worden sind, durchgeführte Verhindern der Präsentation einer Benutzerschnittstelle für das Anwendungsprogramm.

[0013] In Ausführungsform 10 handelt es sich um ein Verfahren der Ausführungsformen 1 bis 9, welches das Folgende umfasst: das von dem Computergerät durchgeführte Erhalten einer dritten Benutzereingabe, welche einen Zugriff auf das Anwendungsprogramm anfordert, nachdem Anweisungen erhalten worden sind, welche einen Zugriff auf das Anwendungsprogramm oder sonstige Anwendungsprogramme verhindern, die dem Profil für die Organisation zugeordnet sind und das von dem Computergerät und als Reaktion auf die dritte Benutzereingabe, welche einen Zugriff auf das Anwendungsprogramm anfordert, durchgeführte Ermitteln, dass kein Zugriff auf das Anwendungsprogramm bereitgestellt werden soll.

[0014] In Ausführungsform 11 handelt es sich um das Verfahren der Ausführungsformen 1 bis 10, welches Folgendes umfasst: das von dem Computergerät durchgeführte Identifizieren, das eine Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren und um auf das Anwendungsprogramm zuzugreifen; während das Computergerät gesperrt ist und während die Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren und um auf das Anwendungsprogramm zuzugreifen, das von dem Computergerät durchgeführte Erhalten einer ersten E-Mail-Nachricht für ein erstes E-Mail-Konto, das nicht von der Organisation verwaltet wird; während das Computergerät gesperrt ist, das von dem Computergerät durchgeführte Bereitstellen von Informationen über die erste E-Mail-Nachricht in einer gesperrten Benutzerschnittstelle für das Computergerät; während das Computergerät gesperrt ist und über separate Sicherheitscodes verfügt, um das Computergerät zu entsperren und während ein Zugriff auf das Anwendungsprogramm bereitgestellt wird, das von dem Computergerät durchgeführte Empfangen einer zweiten E-Mail-Nachricht für ein zweites E-Mail-Konto, das von der Organisation verwaltet wird und während das Computergerät gesperrt ist und das Profil für die Organisation verwendet wird, das von Computergerät durchgeführte Ermitteln, dass keine Informationen über zweite E-Mail-Nachricht in der gesperrten Benutzerschnittstelle für das Computergerät bereitgestellt werden soll.

[0015] In Ausführungsform 12 handelt es sich um das Verfahren der Ausführungsformen 1 bis 11, welches Folgendes umfasst: das vom Computergerät durchgeführte Ermitteln, dass die Hardware des Computergeräts das Verwenden separater Sicherheitscodes für das Entsperren des Computergeräts und das Bereitstellen des Zugriffs auf das Anwendungsprogramm ermöglicht, wobei das Bereitstellen der Benutzerschnittstelle mit der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät die separaten Sicherheitscodes verwenden sollte, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm in Reaktion auf das Ermitteln bereitzustellen, dass die Hardware des Computergeräts das Verwenden separater Sicherheitscodes ermöglicht, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen.

[0016] In Ausführungsform 13 handelt es sich um das Verfahren der Ausführungsformen 1 bis 12, wobei das vom Computergerät durchgeführte Ermitteln, dass die Hardware des Computergeräts das Verwenden separater Sicherheitscodes ermöglicht, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen, das Ermitteln umfasst, dass das Computergerät das dateibasierte Verschlüsseln ermöglicht.

[0017] In Ausführungsform 14 handelt es sich um das Verfahren der Ausführungsformen 1 bis 13, welches das Folgende umfasst: das vom Computergerät als Reaktion auf das Erhalten der zweiten Benutzereingabe, welche den einzelnen Sicherheitscode spezifiziert, durchgeführte Ermitteln, dass die zweite Benutzereingabe den einzelnen Sicherheitscode spezifiziert und das vom Computergerät als Reaktion auf das Ermitteln, dass die zweite Benutzereingabe den einzelnen Sicherheitscode spezifiziert, durchgeführte Bereitstellen des Zugriffs auf das Anwendungsprogramm und eine zusätzliche Anwendung ohne dass ein zusätzlicher Sicherheitscode erfordert wird, wobei es sich bei dem zusätzlichen Programm um ein Programm handelt, das nicht dem Profil der Organisation zugeordnet worden ist, und auf das zugegriffen werden kann, wenn das Computergerät gesperrt ist.

[0018] Ausführungsform 15 ist auf ein oder mehrere computerlesbare Geräte ausgerichtet, die über darauf gespeicherte Anweisungen verfügen, die, wenn sie von einem oder mehreren Prozessoren ausgeführt werden, das Durchführen der Aktionen gemäß

den Verfahren jeglicher der Ausführungsformen 1 bis 14 veranlassen.

[0019] Besondere Ausführungsformen können in bestimmten Fällen einen oder mehrere der folgenden Vorteile zu erzielen. In einigen Implementierungen können die nachfolgend beschriebenen Systeme dem System ermöglichen, eine Benutzereingabe zu erhalten, die spezifiziert, ob ein einzelner Sicherheitscode oder mehrere Sicherheitscodes erforderlich sind, um auf verschiedene Anwendungsprogramme zuzugreifen, die verschiedenen Geräteprofilen zugeordnet werden können. Zum Beispiel kann ein System ein Organisationsprofil verwenden, um ein oder mehrere Anwendungsprogramme zu verwalten, und um zu ermitteln, ob das Organisationsprofil auf alle Anwendungsprogramme des Geräts (z. B. wenn das System über einen einzelnen vereinheitlichten Sicherheitscode verfügt) oder nur diejenigen, die sich spezifisch auf das Organisationsprofil beziehen (z. B. welcher Zugriff auf Daten für die Organisation ermöglicht, wenn das System über verschiedene Sicherheitscodes verfügt) angewendet werden soll.

[0020] Die Details einer oder mehrerer Implementierungen sind in den nachstehenden beiliegenden Zeichnungen und der Beschreibung dargelegt. Andere Merkmale, Objekte und Vorteile sind aus der Beschreibung und den Zeichnungen sowie aus den Patentansprüchen ersichtlich.

BESCHREIBUNG DER ZEICHNUNGEN

[0021] **Fig.** 1 ist ein Beispiel einer Umgebung, in der ein Computergerät eine Einstellung für einen vom Benutzer einstellbaren vereinheitlichten Sicherheitscode beinhaltet.

[0022] **Fig.** 2A–E stellen exemplarische Benutzerschnittstellen für das Erstellen eines vereinheitlichten Sicherheitscodes auf einem Computergerät dar.

[0023] **Fig.** 3 ist ein Beispiel einer Sicherheitseinstellung einer Benutzerschnittstelle für ein Computergerät.

[0024] **Fig.** 4 ist ein Beispiel eines Meldungsmenüs einer Benutzerschnittstelle.

[0025] **Fig.** 5 ist ein Flussdiagramm eines Verfahren für das Aktivieren einer Organisationsanwendung.

[0026] **Fig.** 6 ist ein Flussdiagramm für ein Verfahren für das Einstellen eines vereinheitlichten Sicherheitscodes.

[0027] **Fig.** 7 ist ein konzeptuelles Diagramm eines Systems, das zur Implementierung der in diesem Dokument beschriebenen Systeme und Verfahren angewendet werden kann.

[0028] **Fig.** 8 ist ein Blockdiagramm der Computergeräte, die zur Implementierung der in diesem Dokument beschriebenen Systeme und Verfahren benutzt werden können, entweder als ein Client oder als ein Server oder als eine Vielzahl von Servern.

[0029] Gleiche Bezugszeichen in den verschiedenen Zeichnungen zeigen gleiche Elemente an.

AUSFÜHRLICHE BESCHREIBUNG

[0030] Dieses Dokument beschreibt im Allgemeinen die Entscheidung, ob Sicherheitscodes vereinheitlicht werden sollen. Einige Computergeräte (z. B. Smartphones) erlauben es Benutzern einen Sicherheitscode zu spezifizieren, um das Gerät zu entsperren und um auf bestimmte Funktionen des Geräts zuzugreifen. Nachdem ein Computergerät zum Beispiel aufgrund eines Time-Outs oder aufgrund der Tatsache, dass ein Benutzer das Gerät ausgeschaltet hat, gesperrt wurde, muss ein Benutzer möglicherweise einen Sicherheitscode, wie etwa „59823“ spezifizieren, um auf den Hauptbildschirm des Computergeräts zuzugreifen und um eine Liste von Anwendungsprogrammen, die angewendet werden können, anzusehen.

[0031] Eines oder mehrere dieser Anwendungsprogramme können von oder im Namen des Arbeitgebers des Benutzers entwickelt werden, oder können konfiguriert worden sein, um auf die vom Arbeitgeber bereitgestellten Daten zuzugreifen. Beispiele derartiger Programme würden ein E-Mail-Programm umfassen, das konfiguriert ist, um auf ein E-Mail-Konto, das vom Arbeitgeber bereitgestellt worden ist, oder auf ein Anwendungsprogramm zuzugreifen, welches den Benutzer in die Lage versetzt, auf ein vom Arbeitgeber bereitgestelltes Prozessablaufsystem zuzugreifen. Das Computergerät kann ein oder mehrere dieser vom Arbeitgeber bereitgestellten Anwendungsprogramme einem Arbeitsprofil zuordnen und alle dem Arbeitsprofil zugeordneten Anwendungsprogramme müssen möglicherweise bestimmte Sicherheitskriterien erfüllen, die von einem Administrator des Arbeitgebers spezifiziert werden können. Zum Beispiel kann der Administrator spezifizieren, dass ein Benutzer einen Sicherheitscode einer bestimmten Länge eingeben muss, bevor der Benutzer in die Lage versetzt wird, auf jegliche der Anwendungsprogramme des Arbeitgebers zuzugreifen.

[0032] In einigen Beispielen können die vom Administrator spezifizierten Kriterien strenger als die Kriterien sein, die der Benutzer für seinen Sicherheitscode zum Entsperren des Geräts festgelegt hat, sein, zum Beispiel um auf den Hauptbildschirm des Computergeräts zuzugreifen. Zum Beispiel kann der Administrator spezifizieren, dass ein Benutzer einen Sicherheitscode, der mindestens acht Zeichen lang ist, einzugeben hat, um auf die Anwendungsprogramme

des Arbeitgebers zuzugreifen, während der Benutzer lediglich einen vier Zeichen langen Sicherheitscode eingeben muss, um sein eigenes Gerät zu entsperren. Einige Benutzer bevorzugen diese Herangehensweise, da sie auf diese Weise in der Lage sind, einen Sicherheitscode (möglicherweise einen eher einfachen) zu verwenden, um ihr Gerät zu entsperren und ab und an einen anderen Sicherheitscode eingeben müssen (möglicherweise einen viel komplexeren), sobald das Gerät entsperrt worden ist und wenn der Benutzer auf Arbeitsinhalte zugreifen möchte (z. B. um ein E-Mail-Programm zu aktivieren, das konfiguriert ist, um auf Arbeits-E-Mails zuzugreifen).

[0033] Das regelmäßige Eingeben von zwei Passwörtern kann von einigen Benutzern, die regelmäßig auf arbeitsbezogene Inhalte zugreifen, als schwerfällig empfunden werden. Als solches kann das Rechensystem eine Einstellung bereitstellen, welche Benutzer in die Lage versetzt, zu spezifizieren, ob sie wirklich zwei Sicherheitscodes bereitstellen möchten — einen um das Gerät zu entsperren und einen um auf arbeitsbezogene Inhalte zuzugreifen, sobald das Gerät einsperrt worden ist -oder nur ein Passwort eingeben möchten, um auf die gesamten Inhalte des Geräts zuzugreifen. Sobald die Einstellung „Ein Passwort“ ausgewählt worden ist, ist es möglicherweise erforderlich, dass dieses eine Passwort die vom Administrator spezifizierten Kriterien erfüllen muss, weswegen das Entsperren des Geräts möglicherweise die Eingabe eines komplexeren Passworts beinhalten kann.

[0034] Der Administrator des Arbeitgebers ist möglicherweise in der Lage, verschiedene Einstellungen für den Zugriff auf Anwendungen oder auf Daten, die mit dem Arbeitgeber in Verbindung stehen, zu spezifizieren. Der Administrator ist möglicherweise in der Lage, die Anforderungen für den Sicherheitscode zu spezifizieren. Hierzu gehört unter anderem auch nun das Festlegen der Länge des Sicherheitscodes, der Arten der zugelassenen Sicherheitscodes (z. B. nur numerische, alphanumerische fingerabdruckbezogene, musterbezogene Entsperrung, usw.). Er möglicherweise auch in der Lage, zu spezifizieren, wie oft der Sicherheitscode neu eingestellt werden kann (z. B. alle drei Monate) und ist möglicherweise auch in der Lage, die Anzahl der fehlgeschlagenen Versuche zu spezifizieren, bevor das Gerät Daten und/oder Anwendungen, die sich auf dem Gerät befinden und mit dem Arbeitgeber in Verbindung gebracht werden, löscht.

[0035] Für diese Instanzen, in denen Benutzer es vorziehen ein Passwort zu verwenden, um das Gerät zu entsperren und ein anderes, um auf arbeitsbezogene Daten zuzugreifen, kann der Benutzer des Geräts oder der Administrator Funktionen der Benutzerschnittstelle spezifizieren, um zwischen einem Bildschirm, in den der Sicherheitscode eingegeben wird, um das Gerät zu entsperren und einem anderen Bildschirm zu unterscheiden, in den der Sicherheitscode eingegeben wird, um auf arbeitsbezogene Inhalte zuzugreifen. Zum Beispiel kann der Administrator verschiedene Hintergründe (in Farbe, angezeigtes Bild, oder darauf präsentierter Text) auswählen, die auf jedem Bildschirm präsentiert werden.

[0036] In diesen Instanzen, in denen Benutzer lieber ein Passwort verwenden, um das Gerät zu entsperren und ein anderes Passwort verwenden, um auf die arbeitsbezogenen Inhalte zuzugreifen, kann der Administrator wieder spezifizieren, ob der Benutzer das arbeitsbezogene Passwort für jedes arbeitsbezogene Anwendungsprogramm, auf das der Benutzer zugreifen möchte, erneut eingeben muss, oder ob, sobald der Benutzer das arbeitsbezogene Passwort einmal eingegeben hat, der Benutzer das Passwort nicht mehr erneut eingeben muss, bis das Gerät gesperrt wird oder für eine im Voraus festgelegte Zeitdauer. In einigen Beispielen muss der Benutzer das arbeitsbezogene Passwort möglicherweise nur einmal für eine bestimmte Zeitdauer (z. B. einmal pro Stunde) eingeben, selbst wenn der Benutzer das Gerät gesperrt hat und den Sicherheitscode zum Entsperren des Geräts erneut eingeben muss. Zum Beispiel kann der Benutzer den Sicherheitscode eingeben, um das Gerät zu entsperren, versuchen ein erstes arbeitsbezogenes Anwendungsprogramm zu aktivieren (z. B. durch das Auswählen eines Symbols für das Anwendungsprogramm) und kann dazu aufgefordert werden, seinen arbeitsbezogenen Sicherheitscode einzugeben. Nach einer erfolgreichen Eingabe kann sich der Benutzer dazu entschließen, das Gerät zu sperren. Sollte der Benutzer sich dazu entscheiden, auf ein zweites arbeitsbezogenes Anwendungsprogramm zuzugreifen, muss der Benutzer sein Sicherheitscode möglicherweise eingeben, um das Gerät zu entsperren, kann aber gleichzeitig in der Lage sein, das zweite arbeitsbezogene Anwendungsprogramm zu aktivieren, ohne den arbeitsbezogenen Sicherheitscode erneut eingeben zu müssen, sofern der Benutzer die bestimmte im Voraus festgelegte Zeitdauer nicht überschritten hat, während der der arbeitsbezogene Sicherheitscode noch Gültigkeit hat.

[0037] Fig. 1 ist ein Beispiel einer Umgebung **100**, in der ein Computergerät **102**, eine Einstellung **104** für einen vom Benutzer einstellbaren vereinheitlichen Sicherheitscode beinhaltet, die spezifiziert, ob das Computergerät **102** über einen einzelnen Sicherheitscode verfügt, um das Computergerät **102** zu entsperren und um auf alle Anwendungen zuzugreifen, oder ob das Computergerät **102** über zwei Sicherheitscodes verfügt, wobei einer davon dazu dient, das Computergerät **102** zu entsperren und der andere einen Zugriff auf einige der auf dem Computergerät **102** installierten Anwendungen bereitstellt. Zum Beispiel kann das Computergerät **102** einen Sicherheits-

code **106** für Geräte beinhalten, der verwendet werden kann, um das Computergerät **102** zu entsperren, und der Zugriff auf eine oder mehrere Anwendungen **108** und Daten **110** auf dem Computergerät **102** bereitstellt.

[0038] Wenn das Computergerät **102**, aufgrund der Tatsache, dass der Benutzer eine Eingabe vornimmt, welche den Sicherheitscode **106** des Gerätes bereitstellt, von einem gesperrten Zustand in einen entsperrten Zustand übergeht, kann das Computergerät **102** einen Hauptbildschirm mit einer Liste von Anwendungen, einschließlich der Anwendungen **108** präsentieren. Nach Erhalt einer Benutzerauswahl hinsichtlich einer der Anwendungen **108**, stellt das Computergerät **102** einen Zugriff auf einige der Daten **110** bereit, die der ausgewählten Anwendungen entsprechen. Wenn das Computergerät **102** beispielsweise ermittelt, dass ein Symbol für einen Musik-Player ausgewählt worden ist, stellt das Computergerät **102** einen Zugriff auf die in den Daten **110** enthaltenen Songs bereit.

[0039] Eine der Anwendungen **108** kann eine Anwendungsdatenbank-Anwendung beinhalten, welche einen Zugriff auf eine sich an einem entfernt gelegenen Standort befindliche Anwendungsdatenbank **120** und auf Installationsdaten für Anwendungen bereitstellt. Das Computergerät **102** kann eine Benutzerschnittstelle für eine Anwendungsdatenbank-Anwendung in Reaktion auf die Benutzereingabe bereitstellen, welche eine Benutzerauswahl eines Symbols für die Anwendungsdatenbank-Anwendung spezifiziert. Die Benutzerschnittstelle kann Informationen über mehrere Anwendungen **122** präsentieren, die auf der Anwendungsdatenbank **120** zur Verfügung stehen, um es einem Benutzer zu ermöglichen, eine Anwendung auszuwählen, um weitere Informationen über die ausgewählte Anwendung anzusehen und um es dem Benutzer zu ermöglichen, das Computergerät **102** dazu zu veranlassen, die ausgewählte Anwendung aus der Anwendungsdatenbank **20** herunterzuladen und die ausgewählte Anwendung zu installieren.

[0040] Diese Anwendungsdatenbank-Anwendung kann Informationen für Anwendungen einer Organisation **124** beinhalten, die aus der Anwendungsdatenbank **120** zur Verfügung stehen, z. B. wenn es sich bei der Organisation um einen Arbeitgeber des Benutzers oder eine andere Entität handelt, der der zugeordnet ist, wie etwa eine Freiwilligenorganisation, für die der Benutzer arbeitet. Zum Beispiel kann die Anwendungsdatenbank-Anwendung eine Benutzereingabe erhalten, welche eine bestimmte Anwendung aus den Anwendungen **124** der Organisation spezifiziert, wie etwa eine Prozessablaufanwendung für die Organisation, und Informationen über die bestimmte Anwendung aus den Anwendungen **124** der Organisation auf einem Display des Computergeräts **102** präsentiert.

[0041] Als Antwort auf die vom Computergerät **102** erhaltenen Benutzereingabe und das Spezifizieren einer Anfrage die Prozessablaufanwendung zu installieren, fordert die Anwendungsdatenbank-Anwendung die Prozessablaufanwendung von der Anwendungsdatenbank **120** über ein Netzwerk **130** an. Das Computergerät **102** erhält über das Netzwerk **130** Installationsdaten für die Prozessablaufanwendung und installiert die Prozessablaufanwendung, zum Beispiel in einem Speicher des Computergeräts **102**.

[0042] Das Computergerät **102** erhält ein Geräteprofil **112** der Organisation für die Organisation, um die Installation der Prozessablaufanwendung zu ermöglichen oder um das Präsentieren des Inhalts unter Verwendung der Prozessablaufanwendung zu ermöglichen. Zum Beispiel fordert das Computergerät **102** das Geräteprofil der Organisation **112** von einem Organisationssystem **126** als Teil eines Installationsverfahrens für die Prozessablaufanwendung an. Das Computergerät **102** erhält das Geräteprofil der Organisation **112** über das Netzwerk **130** und installiert das Geräteprofil der Organisation **112** in einem Speicher des Computergeräts **102**.

[0043] Die Installation des Geräteprofils der Organisation **112** auf dem Computergerät **102** kann das Computergerät dazu veranlassen, eine Benutzerschnittstelle bereitzustellen, welche eine Benutzereingabe anfordert, welche einen Organisationssicherheitscode **114** für das Computergerät **102** spezifiziert. Das Computergerät **102** verwendet einen Organisationssicherheitscode **114**, um einen Zugriff auf eine oder mehrere Anwendungen der Organisation **116** einschließlich der Prozessablaufanwendung und Daten der Organisation **118** zuzugreifen.

[0044] Zum Beispiel kann das Computergerät **102** den Organisationssicherheitscode **114** verwenden, um Daten für die Anwendungen der Organisation **116** und Organisationsdaten **118** zu verschlüsseln, die beide auf dem Computergerät **102**, zum Beispiel in einem Speicher des Computergeräts **102**, gespeichert werden. Wenn das Computergerät **102** eine Anforderung erhält, auf eine der Anwendungen der Organisation **116** zuzugreifen, wie etwa der Prozessablauf-Anwendung, stellt das Computergerät **102** eine Benutzerschnittstelle bereit, die den Benutzer dazu auffordert, den Sicherheitscode **114** der Organisation einzugeben. Nach dem Erhalt des Sicherheitscodes der Organisation **114**, verwendet das Computergerät **102** den Organisationssicherheitscode **114** (oder einen anderen Code, der dem Geräteprofil der Organisation **112** zugeordnet ist), um die Anwendungen der Organisation **116** und die Daten der Organisation **118** zu entschlüsseln. Das Computergerät stellt

dann auch eine Benutzerschnittstelle für die Prozessablauf-Anwendung bereit, z. B. startet die Prozessablauf-Anwendung oder veranlasst das Präsentieren einer Benutzerschnittstelle für die Prozessablauf-Anwendung, wenn die Prozessablauf-Anwendung im Hintergrund ausgeführt wird.

[0045] Das Computergerät **102** beinhaltet verschiedene Benutzerschnittstellen für den Erhalt des Sicherheitscodes des Geräts **106**, z. B. der verwendet wird, um das Computergerät zu entsperren und für den Erhalt des Sicherheitscodes der Organisation **114**. Zum Beispiel kann das Computergerät **102** eine Benutzerschnittstelle der Organisationen **128** zum Entsperren mit dem Geräteprofil der Organisation **112** erhalten, z. B. als Teil des Geräteprofils der Organisation **112** oder separat. Wenn das Computergerät **102** gesperrt ist und die Eingabe eines Sicherheitscodes für das Gerät **106** erfordert, präsentiert das Computergerät **102** eine erste Benutzerschnittstelle, die spezifisch für den Sicherheitscode des Geräts **106** ist, z. B. damit ein Benutzer ermitteln kann, welcher Sicherheitscode in die erste Benutzerschnittstelle einzugeben ist. Wenn das Computergerät **102** den Sicherheitscode **114** der Organisation anfordert, um auf eine der Anwendungen der Organisation **116** zuzugreifen, präsentiert das Computergerät **102** die Benutzerschnittstelle der Organisation zum Entsperren **128**, z. B. damit der Benutzer festlegen kann, dass der Organisationssicherheitscode **114** statt dem Sicherheitscode des Geräts **106** eingegeben werden soll.

[0046] Nach der Installation des Geräteprofils der Organisation **112** oder zu jedem anderen geeigneten Zeitpunkt kann das Computergerät **102** ein Menü für das Einstellen eines vereinheitlichten Sicherheitscodes **104** präsentieren, wie etwa eine Benutzerschnittstelle für Sicherheitseinstellungen **200a**, die in **Fig.** 2A dargestellt wird. Wie vorstehend erörtert, versetzt diese Einstellung einen Benutzer in die Lage, zu spezifizieren, ob das Gerät ein einzelnes Passwort für sowohl die Anwendungen der Organisation als auch das Entsperren des Geräts verwendet werden soll, oder ob zwei verschiedene Passwörter für diese Funktionen anzuwenden sind. Beispiele der anderen entsprechenden Zeiten, zu denen das Menü für die vereinheitlichten Sicherheitscode-Einstellungen **104** präsentiert werden sollen, beinhalten die Installation einer der Anwendungen der Organisation **116**, das Starten einer neu installierten Anwendung der Organisation **116**, wenn der Organisationssicherheitscode **114** geändert wird, wenn die Auflagen für den Organisationssicherheitscode **114** geändert werden, auf periodische Weise (z. B. alle paar Monate) oder eine Kombination dieser zwei oder mehrerer dieser. In einigen Implementierungen erstellt das Computergerät **102** einen vereinheitlichten Sicherheitscode für das Entsperren des Computergeräts, z. B. für den Zugriff auf die Anwendungen **108**, und die Anwendungen der Organisation **116**, nach der Installation des Geräteprofils der Organisation **112** und ermöglicht danach das Erstellen separater Sicherheitscodes.

[0047] Fig. 2A–E stellen exemplarische Benutzerschnittstellen für das Erstellen eines vereinheitlichten Sicherheitscodes auf einem Computergerät dar. Zum Beispiel beinhaltet die Benutzerschnittstelle für Sicherheitseinstellungen **200a**, die in **Fig.** 2A dargestellt ist, Informationen über die Anforderungen an den Sicherheitscode, die im Geräteprofil der Organisation **112** definiert werden, wie etwa eine Sperreinstellung des Arbeitsprofils **202**, die eine Sicherheitscodeart spezifiziert, welche vom Computergerät **102** das Bereitstellen eines Zugriffs auf die Anwendungen der Organisation **116**, wie etwa eine PIN-Nummer oder ein Passwort, anfordert. Zum Beispiel stellt das Computergerät **102** die Sperreinstellungen des Arbeitsprofils **202** auf Basis der Sicherheitscodeart ein, die im Geräteprofil der Organisation **112** spezifiziert ist.

[0048] Eine Fingerabdruckeinstellung **204** gibt an, ob das Computergerät **102** nach dem Erhalt der biometrischen Daten, welche mit einem Fingerabdruckprofil, der auf dem Computergerät **102** gespeichert wird, übereinstimmen, einen Zugriff auf die Anwendungen der Organisationen **116** bereitstellen kann. Die Fingerabdruckeinstellung **204** kann angeben, wie viele Fingerabdruckprofile auf dem Computergerät **102** gespeichert werden.

[0049] Eine Verschlüsselungseinstellung **208** gibt an, ob die Anwendungen der Organisation **116** und die Daten der Organisation **118** verschlüsselt sind. In einigen Beispielen spezifiziert die Verschlüsselungseinstellung **208**, ob alle Daten auf dem Computergerät **102** verschlüsselt sind.

[0050] Die Benutzerschnittstelle für Sicherheitseinstellungen **200a** beinhaltet eine Einstellung für vereinheitlichte Sicherheitscodes **206**, die angibt, ob das Computergerät **102** einen einzelnen Sicherheitscode oder mehrere Sicherheitscodes für den Zugriff auf sämtliche Inhalte, die auf dem Computergerät **102** gespeichert werden, verwendet. Wenn die vereinheitlichte Sicherheitscode-Einstellung **206** ausgeschaltet ist, speichert das Computergerät **102** Daten für sowohl den Sicherheitscode des Geräts **106** für das Entsperren des Computergeräts **102** als auch den Organisationssicherheitscode **114**, der für den Zugriff auf die Anwendungen der Organisation **116** verwendet wird, auf einem Speicher.

[0051] Wenn das Computergerät **102** eine Benutzereingabe erhält, die eine Auswahl der Einstellung des vereinheitlichten Sicherheitscodes **206** von aktiviert zu deaktiviert angibt, präsentiert das Computergerät **102** die in **Fig.** 2B dargestellte Benutzerschnittstelle **210** „Dieselbe Sperre verwenden?“. Die Benut-

zerschnittstelle „Dieselbe Sperre verwenden“? **210** kann Informationen über das Verwenden des Sicherheitscodes der Organisation **114** beinhalten, um das Computergerät **102** (z. B. über das Verwenden eines vereinheitlichten Sicherheitscodes) zu entsperren, wie etwa einen Hinweis darauf, dass das Geräteprofil der Organisation **112** auf alle Anwendungen des Computergeräts und nicht nur auf die Anwendungen der Organisation **116** angewendet werden können. Die Benutzerschnittstelle „Dieselbe Sperre verwenden?“ **210** kann angeben, dass der Sicherheitscode des Geräts **106** nicht länger verwendet werden wird, wenn ein vereinheitlichter Sicherheitscode definiert wird, um der vereinheitlichte Sicherheitscode zu sein.

[0052] Die Sperr-Benutzerschnittstelle „Dieselbe Sperre verwenden?“ **210** beinhaltet eine Option zum Abbruch des Menüs **212** und eine Option zum Aktivieren eines vereinheitlichten Sicherheitscodes **214**. Wenn das Computergerät **102** eine Benutzereingabe erhält, die eine Auswahl der Option zum Abbruch des Menüs **212** erhält, präsentiert das Computergerät die Benutzerschnittstelle für Sicherheitseinstellungen **200a**. Wenn das Computergerät **102** eine Benutzereingabe erhält, welche die Auswahl eines Aktivierens eines vereinheitlichten Sicherheitscodes **214** erhält, präsentiert das Computergerät **102** Benutzerschnittstellen, um den gegenwärtigen Sicherheitscode des Geräts **106** zu bestätigen und um den Organisationssicherheitscode **114** vor dem Einstellen des vereinheitlichten Sicherheitscodes zu bestätigen.

[0053] Wie zum Beispiel in **Fig.** 2C dargestellt, kann das Computergerät **102** ermitteln, dass der Sicherheitscode des Geräts **106** mittels eines Mustereintrags bereitgestellt wurde und daher eine Benutzerschnittstelle der Musterbestätigung **200c** präsentieren kann. Ein Hintergrund für die Benutzerschnittstelle der Musterbestätigung **200c** kann spezifisch für den Eintrag des Sicherheitscodes des Geräts **106** (z. B. unterschiedlich im Vergleich zum Hintergrund für die Benutzerschnittstelle der Bestätigung des arbeitsbezogenen Sicherheitscodes, der in **Fig.** 2D dargestellt wurde) sein. Nachdem das Computergerät **102** eine Benutzereingabe erhält, welche ein Muster in der Benutzerschnittstelle der Musterbestätigung **200c** definiert (z. B. indem der Benutzer einen Finger zwischen individuellen Benutzerschnittstellenelementen im Raster der Anzeige einer bestimmten Sequenz nachverfolgt), ermittelt das Computergerät **102**, ob das Benutzereingabemuster mit dem Sicherheitscode des Geräts **106** übereinstimmt. Falls das Benutzereingabemuster nicht mit dem Sicherheitscode **106** des Geräts übereinstimmt, kann das Computergerät **102** eine Fehlermeldung präsentieren, das Verfahren des Erstellens eines vereinheitlichten Sicherheitscodes beenden, oder beides durchführen.

[0054] Wenn das Computergerät **102** ermittelt, das das Benutzereingabemuster mit dem Sicherheitscode des Geräts **106** übereinstimmt, kann das Computergerät **102** eine in **Fig.** 2D dargestellte Benutzerschnittstelle zur Bestätigung des arbeitsbezogenen Sicherheitscodes **200d** präsentieren. Ein Hintergrund für die Benutzerschnittstelle zur Bestätigung des arbeitsbezogenen Sicherheitscodes **200d** kann spezifisch für die Benutzereingabe des Sicherheitscodes der Organisation **114** sein, um die Benutzerschnittstelle zur Bestätigung des arbeitsbezogenen Sicherheitscodes **200d** von der Benutzerschnittstelle der Musterbestätigung **200c** zu unterscheiden. Zum Beispiel kann das Computergerät **102** ermitteln, dass der Organisationssicherheitscode **114** eine PIN-Nummer ist und in der Benutzerschnittstelle zur Bestätigung des arbeitsbezogenen Sicherheitscodes **200d** die Eingabe einer PIN-Nummer anfordern, um mit dem Verfahren des Erstellens eines vereinheitlichten Sicherheitscodes fortzufahren. Die Benutzerschnittstelle kann auch einen unterschiedlichen Text beinhalten. Zum Beispiel kann die Benutzerschnittstelle zur Bestätigung des arbeitsbezogenen Sicherheitscode **200d** „Arbeitsprofilsperre“ angeben, und auf die „Arbeits-PIN-Nummer“ verweisen, während die Benutzerschnittstelle der Musterbestätigung **200c** auf eine „Bildschirmsperre“ und ein „Gerätemuster“ verweisen kann.

[0055] Das Computergerät **102** ermittelt, ob der Sicherheitscode, der in die Benutzerschnittstelle zur Bestätigung des arbeitsbezogenen Sicherheitscodes **200d** eingegeben wird, derselbe wie der Organisationssicherheitscode **114** ist. Als Antwort auf das Ermitteln, dass es sich bei den Sicherheitscodes um dieselben Sicherheitscodes handelt, präsentiert das Computergerät **102** die in **Fig.** 2E gezeigte Benutzerschnittstelle **200e** für Sicherheitseinstellungen **206e**, die angibt, dass das Computergerät **102** einen vereinheitlichten Sicherheitscode verwendet, um das Computergerät **102** zu entsperren, und um einen Zugriff auf die Anwendungen der Organisation **116** und die Daten der Organisation **118** bereitzustellen.

[0056] Das Computergerät **102** kann über verschiedene Sicherheitscode-Auflagen für den Sicherheitscode des Geräts **106** und den Organisationssicherheitscode **114** verfügen. Das Computergerät **102** kann zum Beispiel über eine Gerätepolitik verfügen, die angibt, dass der Sicherheitscode des Geräts **106** über ein Entsperrungsmuster, biometrische Daten (z. B. Fingerabdruckdaten oder Gesichtserkennungsdaten) oder einen alphanumerischen Sicherheitscode verfügt, der über mindestens vier Zeichen verfügt (z. B. ein Passwort oder eine PIN-Nummer). Das Geräteprofil der Organisation **112** kann angeben, dass es sich bei dem Organisationssicherheitscode **114** um biometrische Daten, eine sechsstellige PIN-Nummer oder ein achtstelliges Passwort mit sowohl mindes-

tens einem Buchstaben als auch mindestens einer Zahl, handelt.

[0057] Während des Verfahrens zur Erstellung eines vereinheitlichten Sicherheitscodes, kann das Computergerät **102** bestätigen, dass der Organisationssicherheitscode **114** die Sicherheitscode-Auflagen, die Teil des Geräteprofils der Organisation **112** sind, erfüllt, z. B. sofern die Sicherheitscode-Einschränkungen seit der anfänglichen Einstellung des Sicherheitscodes der Organisation **114** für das Computergerät **102** inzwischen geändert worden sind. Wenn das Computergerät **102** ermittelt, dass der Organisationssicherheitscode **114** die Sicherheitscode-Auflagen, die Teil des Geräteprofils der Organisation **112** sind, nicht erfüllt, präsentiert das Computergerät **102** eine andere Benutzerschnittstelle, welche eine Benutzereingabe eines neuen Sicherheitscodes der Organisation anfordert, der die Auflagen des Sicherheitscodes erfüllt und den neuen Organisationssicherheitscode als einen vereinheitlichten Sicherheitscode verwendet.

[0058] Falls das Computergerät **102** eine Benutzereingabe erhält, welche die Auswahl der Einstellung eines vereinheitlichten Sicherheitscodes **206e** von einer aktivierten in eine deaktivierte Position angibt, präsentiert das Computergerät **102** eine Benutzerschnittstelle, welche die Bestätigung eines vereinheitlichten Sicherheitscodes anfordert, z. B. ähnlich wie die Benutzerschnittstelle zur Bestätigung des arbeitsbezogenen Sicherheitscodes **200d** aus **Fig.** 2D. Wenn das Computergerät **102** bestätigt, dass die Benutzereingabe für die Bestätigung mit dem vereinheitlichten Sicherheitscode übereinstimmt, verwendet das Computergerät **102** den vereinheitlichten Sicherheitscode als Organisationssicherheitscode **114** und präsentiert eine Benutzerschnittstelle, welche einen neuen Sicherheitscode des Geräts **106** anfordert.

[0059] **Fig.** 3 ist ein Beispiel einer Sicherheitseinstellung einer Benutzerschnittstelle **300** für ein Computergerät. Zum Beispiel kann die Benutzerschnittstelle für Sicherheitseinstellungen **200a** einen Abschnitt der Einstellungen der Benutzerschnittstelle für Sicherheitseinstellungen **300** beinhalten und ein Teil davon sein.

[0060] Die Benutzerschnittstelle für Sicherheitseinstellungen **300** beinhaltet Einstellungen und Informationen für sowohl die allgemeinen Sicherheitseinstellungen des Computergeräts **102** als auch die getrennten Sicherheitseinstellungen für das arbeits- oder organisationsbezogene Profil. Zum Beispiel beinhaltet die Benutzerschnittstelle für Sicherheitseinstellungen **300** eine Option zum Sperren des Bildschirmhintergrunds **302a**, die die Benutzereingabe in die Lage versetzt, ein bestimmtes Bild oder ein bestimmtes Muster zu spezifizieren, dass auf der Entsperrungsbenutzerschnittstelle angezeigt werden soll, z. B. eine Benutzerschnittstelle, auf der das Computergerät **102** eine Eingabe für den Sicherheitscode des Gerätes **106** erhält, wenn das Computergerät **102** entsperrt wird, eine ähnliche Benutzerschnittstelle, um den Sicherheitscode des Gerätes zu ändern, oder beides.

[0061] Eine Option zum Sichtbarmachen des Musters **304** versetzt die Benutzereingabe in die Lage, anzugeben, ob ein Muster, das auf einem gesperrten Bildschirm eingegeben wird, auf der Entsperrungsbenutzerschnittstelle angezeigt wird (z. B. indem der Benutzer einen Finger zwischen individuellen Benutzerschnittstellenelementen im Raster der Anzeige einer bestimmten Sequenz nachverfolgt). Wenn eine Option zum Sichtbarmachen des Musters **304** deaktiviert wird, präsentiert das Computergerät **102** das Muster auf der Entsperrungsbenutzerschnittstelle nicht. Wenn die Option zum Sichtbarmachen des Musters **304** aktiviert wird, präsentiert das Computergerät **102** auf der Entsperrungsbenutzerschnittstelle, das Muster, das von der Benutzereingabe auf der Entsperrungsbenutzerschnittstelle erstellt worden ist.

[0062] Eine Option zum Sperren des arbeitsbezogenen Bildschirmhintergrunds **302b** identifiziert ein bestimmtes Bild oder Muster, welches das Computergerät **102** anzeigt, wenn die Benutzereingabe des Sicherheitscodes der Organisation **114** angefordert wurde, wenn die Benutzereingabe zur Änderung des Sicherheitscodes der Organisation **114** angefordert wurde, oder wenn beides angefordert wird. Die Option zum Sperren des arbeitsbezogenen Bildschirmhintergrunds **302b** kann im Geräteprofil der Organisation **112** spezifiziert werden, z. B. durch den Administrator der Organisation. Die Option zum Sperren des arbeitsbezogenen Bildschirmhintergrunds **302b** kann ein Bild, ein Logo, oder eine Farbe für die Organisation identifizieren.

[0063] Das Computergerät **102** kann keine vom Benutzer durchgeführte Modifikation der Option zum Sperren des arbeitsbezogenen Bildschirmhintergrunds **302b** ermöglichen. Das Computergerät **102** ändert die Option zum Sperren des arbeitsbezogenen Bildschirmhintergrunds **302b** unter Verwendung von Daten vom Geräteprofil der Organisation **112** oder sonstigen Daten aus dem System der Organisation **126**. In einigen Implementierungen kann das Computergerät **102** die Benutzereingabe in die Lage versetzen, die Option zum Sperren des arbeitsbezogenen Bildschirmhintergrunds **302b** zu verändern, z. B. wenn das Geräteprofil der Organisation **112** angibt, dass ein Benutzer die Einstellung ändern kann.

[0064] Die Einstellung des vereinheitlichten Sicherheitscodes **206** in der Benutzerschnittstelle für Sicherheitseinstellungen **300** kann angeben, dass das Computergerät **102** nur einen einzelnen Hintergrund

für das Entsperren des Bildschirms präsentiert, wenn es anfordert, dass die Benutzereingabe einen Sicherheitscode definiert. Das Computergerät **102** kann das Sperren des arbeitsbezogenen Bildschirmhintergrunds **302b** als Hintergrund für alle Bildschirme mit der Sperrfunktion verwenden, wenn die Einstellungen des vereinheitlichten Sicherheitscodes **206** aktiviert sind. In einigen Beispielen kann das Computergerät **102** die Option zum Sperren des Bildschirmhintergrunds **302a** als Hintergrund für alle Bildschirme mit Sperrfunktion verwenden, um die Benutzereingabe in die Lage zu versetzen, den Hintergrund zu definieren.

[0065] Rückkehrend zu **Fig.** 1 kann das Geräteprofil der Organisation **112** Einstellungen für den Organisationssicherheitscode **114**, Sitzungen, während denen die Anwendungen der Organisation **116** und die Daten der Organisation **118** zur Verfügung stehen, oder beides beinhalten. Zum Beispiel kann das Geräteprofil der Organisation **112** eine Verschlüsselungseinstellung beinhalten, die angibt, wie die Anwendungen der Organisation **116**, die Daten der Organisation **118** oder beides in einem Speicher des Computergeräts **102** verschlüsselt und gespeichert werden.

[0066] Das Computergerät **102** kann eine Einstellung beinhalten, die angibt, dass das Computergerät **102** einen vereinheitlichten Sicherheitscode verwenden muss, wenn das Computergerät **102** über eine blockbasierte Verschlüsselung verfügt, z. B. da das Computergerät **102** nicht in der Lage ist, die Anwendungen **108** und die Daten **110** separat von den Anwendungen der Organisation **116** und den Daten der Organisation **118** zu verschlüsseln. Die Einstellungen können ergeben, dass das Computergerät **102** eine Benutzerschnittstelle für eine Benutzereingabe bereitstellt, die auswählt, ob ein vereinheitlichter Sicherheitscode oder separate Sicherheitscodes verwendet werden sollen, um das Computergerät **102** zu entsperren und auf die Anwendungen der Organisation **116** zuzugreifen, wenn das Computergerät **102** die dateibasierte Verschlüsselung unterstützt.

[0067] Wenn das Computergerät **102** das Geräteprofil der Organisation **112** erhält und ermittelt, dass das Geräteprofil der Organisation **112** eine höhere Anzahl an einschränkenden Sicherheitscode-Einstellungen enthält als diejenigen für den Sicherheitscode des Geräts **106**, kann das Computergerät **102** ermitteln, ob die Hardware des Computergeräts **102** nur einen vereinheitlichten Sicherheitscode oder sowohl einen vereinheitlichten Sicherheitscode als auch separate Sicherheitscodes unterstützt. Falls das Computergerät **102** ermittelt, dass nur ein vereinheitlichter Sicherheitscode unterstützt wird, z. B. und das Computergerät **102** verfügt über eine blog-basierte Verschlüsselung, wobei das Computergerät **102** eine Benutzerschnittstelle bereitstellt, welche die Benutzereingabe eines vereinheitlichten Passcodes für das Entsperren des Computergeräts **102** bereitstellt und Zugriff auf die Anwendungen **116** der Organisation bereitstellt.

[0068] Wenn das Computergerät **102** ermittelt, dass separate Sicherheitscodes unterstützt werden, z. B. und das Computergerät **102** über eine dateibasierte Verschlüsselung verfügt, kann das Computergerät **102** eine Benutzerschnittstelle bereitstellen, welche eine Benutzereingabe anfordert, die spezifiziert, ob das Computergerät **102** einen vereinheitlichten Sicherheitscode oder einen separaten Sicherheitscode verwenden sollte. Die Benutzerschnittstelle kann eine Menüoption beinhalten, die über ähnliche Eigenschaften wie die vereinheitlichte Sicherheitscode-Einstellung **206** aus **Fig.** 2A verfügt.

[0069] Das Computergerät **102** erhält eine Benutzereingabe, die spezifiziert, ob ein vereinheitlichter Sicherheitscode oder separate Sicherheitscodes verwendet werden sollen. Das Computergerät **102** kann eine zweite Benutzerschnittstelle bereitstellen, die die Benutzereingabe des vereinheitlichten Sicherheitscodes anfordert, falls ein vereinheitlichter Sicherheitscode in der ersten Benutzerschnittstelle ausgewählt worden ist, oder des Sicherheitscodes der Organisation **114** falls separate Sicherheitscodes in der ersten Benutzerschnittstelle ausgewählt worden sind. Das Computergerät **102** kann eine Einstellung im Geräteprofil der Organisation **112** verwenden, um zu ermitteln, wann eine Benutzerschnittstelle mit einer vereinheitlichten Sicherheitscode-Option bereitzustellen ist, wann eine Benutzerschnittstelle, die eine Benutzereingabe des Sicherheitscodes der Organisation anfordert, bereitzustellen ist, oder wann beide bereitzustellen sind, z. B. in derselben Benutzerschnittstelle oder separaten Benutzerschnittstellen.

[0070] Das Organisationssystem **126** kann eine Administratoreingabe erhalten, die mindestens einige der Einstellungen spezifiziert, die im Geräteprofil der Organisation **112** enthalten sind. Zum Beispiel kann das System der Organisation **126** eine Administrator-Benutzerschnittstelle, die an den Administrator präsentiert werden soll, bereitstellen. Der Administrator kann die Benutzerschnittstelle des Administrators verwenden, um einen Time-Out für den Organisationssicherheitscode **114**, eine Dauer, für die der Organisationssicherheitscode **114** gültig ist (z. B. nachdem ein Gerät eine Benutzereingabe anfordert, die einen neuen Organisationssicherheitscode spezifiziert) und die Anwendungen, auf die das Geräteprofil der Organisation **112** angewendet wird, (z. B. die Anwendungen auf die, die Einstellungen des Geräteprofils der Organisation **112** angewendet werden) zu spezifizieren.

[0071] Zum Beispiel kann das Organisationssystem **126** eine Eingabe des Administrators über die Benut-

zerschnittstelle des Administrators erhalten, die spezifiziert, dass die Einstellungen im Geräteprofil der Organisation **112**, die auf eine Prozessablauf-Anwendung angewendet werden, auf eine Mail-Anwendung und eine Kalender-Anwendung angewendet werden. Zum Beispiel gibt die Eingabe des Administrators an, dass die Prozessablauf-Anwendung, die Mail-Anwendung und die Kalender-Anwendung, Anwendungen der Organisation **124** sind, z. B. Anwendungen, die von der Organisation oder Anwendungen dritter Parteien entwickelt wurden, die verwendet werden, um auf Daten der Organisation zuzugreifen. Wenn das Computergerät **102** eine Anfrage erhält, um eine beliebige Anwendung der Organisation **124** zu aktivieren oder zu installieren, ermittelt das Computergerät **102**, ob die Anwendung, auf die die Anforderung angewendet wird, eine der Anwendungen der Organisation ist, und sofern dies der Fall ist, ermittelt sie die entsprechenden Einstellungen vom Geräteprofil der Organisation **112**, die auf die Anwendung angewendet werden. Diese vom Administrator spezifizierten Einstellungen, können angewendet werden und an alle oder zumindest an mehrere Geräte übermittelt werden, auf denen die Anwendungen der Organisation installiert werden.

[0072] In einem Beispiel kann das Computergerät **102** ermitteln, dass eine Mail-Anwendung Einstellungen für ein erstes E-Mail-Konto beinhaltet, und dass das erste E-Mail-Konto nicht dem Geräteprofil der Organisation **112** zugeordnet wird, da eine Domain für das erste E-Mail-Konto nicht dasselbe wie eine Domain ist, die von der Organisation gemanagt wird, z. B. das Computergerät **102** kann ermitteln, dass das erste E-Mail-Konto ein persönliches E-Mail-Konto ist. Wenn das Computergerät **102** eine Benutzereingabe für die Mail-Anwendung erhält, um ein zweites E-Mail-Konto zu erstellen, ermittelt das Computergerät **102**, dass das zweite E-Mail-Konto über eine Domain verfügt, die im Geräteprofil der Organisation **112** identifiziert wird, und ein E-Mail-Konto ist, dass von der Organisation verwaltet wird.

[0073] Das Computergerät **102** wendet Einstellungen vom Geräteprofil der Organisation **112** auf das zweite E-Mail-Konto an. Zum Beispiel verschlüsselt das Computergerät **102** Daten für das zweite E-Mail-Konto, das den Organisationssicherheitscode **114** verwendet und nur einen Zugriff auf Daten für das zweite E-Mail-Konto in Reaktion auf die Benutzereingabe des Sicherheitscodes der Organisation **114** erlaubt. In einigen Beispielen kann das Computergerät **102** zwei Benutzerschnittstellenelemente für die Mail-Anwendungen einem Menü beinhalten, z. B. auf einem Hauptbildschirm, ein erstes Benutzerschnittstellenelement für den Zugriff auf Daten für das erste E-Mail-Konto, und ein zweites Benutzerschnittstellenelement für Zugriff auf das zweite E-Mail-Konto. Das Computergerät **102** ermöglicht die Präsentation von Inhalten für das erste E-Mail-Konto in Reaktion auf die Benutzereingabe, die eine Auswahl des ersten Benutzerschnittstellenelements ohne die Eingabe des Sicherheitscodes der Organisation **114** spezifiziert und fordert die Eingabe des Sicherheitscodes der Organisation **114** nach dem Erhalt der Benutzereingabe, welche die Auswahl des zweiten Benutzerschnittstellenelements spezifiziert, z. B. unter der Annahme, dass eine Sitzung für den Zugriff auf die Anwendungen der Organisation **116** derzeit nicht aktiv sind.

[0074] Wenn das Computergerät **102** zum Beispiel eine Benutzereingabe erhält, die den Organisationssicherheitscode **114** spezifiziert, erstellt das Computergerät eine Sitzung für den Zugriff auf die Anwendungen der Organisation **116** und ermöglicht den Zugriff auf jegliche der Anwendungen der Organisation **116** und auf die Daten der Organisation **118** bis die Sitzung beendet worden ist. Die Dauer der Sitzung wird von einem Time-Out spezifiziert, der im Geräteprofil der Organisation **112** identifiziert wird. In einigen Beispielen kann das Computergerät **102** die Sitzung erweitern, während sämtliche beliebige Anwendungen der Anwendungen der Organisation **116** aktiv sind, z. B. auf einem Display präsentiert, beginnen einen Zeitmesser für die Sitzung, wenn keine der Anwendungen der Organisation **116** aktiv sind, z. B. keine der Anwendungen der Organisation über eine Benutzerschnittstelle verfügen, die auf dem Display präsentiert werden. Wenn das Computergerät **102** ermittelt, dass eine Dauer des Teilnehmers dasselbe ist wie ein Timeout, beendet das Computergerät **102** die Sitzung.

[0075] Das Computergerät **102** kann eine oder mehrere Einstellungen beinhalten, welche die Präsentation der Meldungen von den Organisationsanwendungen **116** steuern. Das Computergerät **102** kann die Einstellungen einer Benutzerschnittstelle des Meldungsmenüs **400**, die in **Fig.** 4 dargestellt wird, präsentieren. Die Benutzerschnittstelle des Meldungsmenüs **400** beinhaltet eine gesperrte Meldungseinstellung **402**, die spezifiziert, welche Art von Meldungen präsentiert werden sollen, wenn das Computergerät **102** gesperrt ist. Das Computergerät **102** verwendet gesperrte Meldungseinstellungen **402** für Meldungen von den Anwendungen **108**, die nicht dem Geräteprofil der Organisation **112** zugeordnet sind.

[0076] Die Benutzerschnittstelle des Meldungsmenüs **400** beinhaltet eine gesperrte Meldungseinstellung der Organisation **404a** ein, welche spezifiziert, ob die Meldungen von den Anwendungen der Organisation **116** präsentiert werden, wenn das Computergerät **102** gesperrt ist. Zum Beispiel wird die gesperrte Meldungseinstellung der Organisation **404a** eingestellt, um bei der Zeit T_0 „alle arbeitsbezogenen Meldungsinhalte darzustellen“. Wenn jegliche der Anwendungen der Organisation **116** eine Meldung er-

mitteln, z. B. wie etwa eine E-Mail-Meldung, erhält das Computergerät **102** Daten für die Meldung, welche die Präsentation der Meldung auf einem gesperrten Bildschirm unter Verwendung der Daten veranlasst.

[0077] Die Benutzerschnittstelle des Meldungsmenüs **400** erhält eine Auswahl der gesperrten Meldungseinstellung der Organisation **404a**–b und präsentiert zur Zeit T_1 ein Meldungsmenü **406**. Das Meldungsmenü **406** beinhaltet eine „keine arbeitsbezogenen Meldungen darstellen“ Option, eine „empfindliche arbeitsbezogene Meldungsinhalte verstecken“ Option und eine „sämtliche arbeitsbezogenen Meldungsinhalte darstellen“ Option. Wenn die „empfindliche arbeitsbezogene Meldungsinhalte verstecken“ Option eingestellt ist, verhindert das Computergerät **102** das Präsentieren empfindlicher arbeitsbezogener Inhalte auf einem gesperrten Bildschirm. Zum Beispiel kann das Geräteprofil der Organisation **112** angeben, dass empfindliche arbeitsbezogene Inhalte Kontaktnamen und E-Mail-Hauptteile beinhalten. Wenn das Computergerät **102** eine Meldung von einer Mail-Anwendung für eine E-Mail der Organisation erhält und die „empfindliche arbeitsbezogene Meldungsinhalte verstecken“ eingestellt ist, kann das Computergerät **102** unter Verwendung der Daten vom Geräteprofil der Organisation **112** einen Betreff der E-Mail, eine Meldung, dass die Arbeitssitzung der E-Mail erhalten worden ist oder eine Meldung, dass eine Nachricht erhalten worden ist, präsentieren, z. B. ohne das Identifizieren der Anwendung der Organisation, welche die Nachricht ermittelt hat.

[0078] Die Benutzerschnittstelle des Meldungsmenüs **400** erhält eine Benutzereingabe, welche die Auswahl der „keine arbeitsbezogenen Meldungen darstellen“ Option spezifiziert und präsentiert zur Zeit T_2 eine aktualisierte gesperrte Meldungseinstellung der Organisation **404b**, die angibt, dass das Computergerät **102** keine Meldungen für jegliche der Anwendungen der Organisation **116** anzeigen soll, während das Computergerät **102** gesperrt ist. In einigen Implementierungen kann das Computergerät **102** eine Meldung bereitstellen, z. B. hörbar, dass das Computergerät **102** über eine Meldung ohne einen sichtbaren Hinweis jeglicher Art auf Einzelheiten für die Meldung. Das Computergerät **102** kann eine Benutzereingabe für das Entsperren des Computergeräts **102** erhalten und Informationen über die Meldungen der Organisation bereitstellen, sobald das Computergerät **102** entsperrt ist.

[0079] In einigen Implementierungen kann gesperrte Meldungseinstellung der Organisation **404a**–b von einem Administrator spezifiziert werden. Zum Beispiel kann das Geräteprofil der Organisation **112** Daten beinhalten, die angeben, dass die gesperrte Meldungseinstellung der Organisation **404b** auf „keine arbeitsbezogene Meldungen darstellen“ eingestellt sein sollte und nicht in Reaktion auf die Benutzereingabe geändert werden kann

[0080] Rückkehrend zu **Fig.** 1 kann das Geräteprofil der Organisation **112** zusätzliche Einstellungen für das Computergerät beinhalten, die von einem Administrator spezifiziert werden, z. B. zum Beispiel der Organisation. Zum Beispiel kann das Geräteprofil der Organisation **112** angeben, welche Arten von Sicherheitscodes für den Organisationssicherheitscode verwendet werden können (z. B. nur numerisch, alphanumerisch, geometrisch, Musterentsperrung, usw.) eine Mindestlänge für einen Sicherheitscode (z. B. ob numerisch, alphanumerisch oder Musterentsperrung) eine Anzahl fehlgeschlagener Versuche bevor das Computergerät **102** den Zugriff auf die Anwendungen der Organisation **116** und die Daten der Organisation **118** verhindert (z. B. bevor die Daten für die Anwendungen der Organisation **116** und die Daten der Organisation **118** von allen Speichern des Computergeräts **102** entfernt werden) oder eine Kombination dieser zwei oder mehrerer dieser durchführen.

[0081] Das Geräteprofil der Organisation **112** kann die Entsperrungsbenutzerschnittstelle der Organisation **128** als Hintergrund für eine Entsperrungsbenutzerschnittstelle identifizieren, welche eine Benutzereingabe des Sicherheitscodes der Organisation **114** anfordert. Die Entsperrungsbenutzerschnittstelle der Organisation **128** kann ein Bild sein, z. B. ein Logo für eine Organisation, eine Farbe für die Organisation, z. B. blau, oder kann einen Namen der Organisation beinhalten, z. B. zur Präsentation in die Entsperrungsbenutzerschnittstelle, wie etwa an der Spitze der Benutzerschnittstelle oder kann eine Kombination der zwei oder mehrerer dieser sein. Das Computergerät **102** kann die Entsperrungsbenutzerschnittstelle der Organisation **128** verwenden, wenn eine Benutzereingabe angefordert wird, um den Organisationssicherheitscode **114** zu ändern. Das System der Organisation **126** kann eine Eingabe des Administrators erhalten, welche eine oder mehrere Einstellungen im Geräteprofil der Organisation **112** spezifiziert, bevor das Geräteprofil der Organisation **112** dem Computergerät bereitgestellt wird.

[0082] In einigen Beispielen kann das Computergerät **102** das Geräteprofil der Organisation **112** vom System der Organisation **126** erhalten und ermitteln, welche Anwendungen der Organisation dem Computergerät **102** unter Verwendung des Geräteprofils der Organisation **112** zur Verfügung stehen. Das Computergerät **102** kann ein Geräteprofil der Organisation **112** während der Einstellung einer der Anwendungen der Organisation **116** auf dem Computergerät erhalten, wie etwa ein E-Mail-Konto in einer E-Mail-Anwendung in Reaktion auf eine Anfrage für das Geräteprofil der Organisation **112** oder das Verwenden anderer angemessener Verfahren.

[0083] Das Computergerät **102** kann eine oder mehrere der Anwendungen der Organisation **116** von der Anwendungsdatenbank **120** erhalten, z. B. unter Verwendung der Anwendungsdatenbank der Anwendung, vom System der Organisation **126** von einem anderen Computer, der Anwendungen der Organisation **124** beinhaltet oder einer Kombination dieser oder mehrerer dieser. Zum Beispiel kann das Computergerät **102** Daten erhalten, um ein E-Mail-Konto auf dem Computergerät **102** vom System der Organisation **126** zu erhalten, z. B. wenn das Computergerät **102** eine vorinstallierte E-Mail-Anwendung für das E-Mail-Konto verwendet. Das Computergerät **102** kann eine Kalenderanwendung von der Anwendungsdatenbank **120** und eine Prozessablauf-Anwendung von einem Server, der von einer Organisation verwaltet wird, erhalten.

[0084] In einigen Implementierungen kann das Geräteprofil der Organisation **112** eine Einstellung beinhalten, die spezifiziert, dass wenn das Computergerät **102** über separate Sicherheitscodes verfügt und biometrische Daten erhält, um das Computergerät **102** zu entsperren, kann das Computergerät **102** unter der Annahme, dass das Computergerät **102** die biometrischen Daten validiert, um sicherzustellen, dass die biometrischen Daten mit den gespeicherten biometrischen Daten für den Organisationssicherheitscode **114** übereinstimmen, einen Zugriff auf die Anwendungen der Organisation **116** bereitstellen. Zum Beispiel kann das Computergerät **102** eine Entsperrungsbenutzerschnittstelle präsentieren, und als Antwort biometrische Daten erhalten. Das Computergerät **102** verwendet die biometrischen Daten, um zu bestätigen, dass die biometrischen Daten mit den biometrischen Daten für den Sicherheitscode des Geräts **106** und den biometrischen Daten für den Organisationssicherheitscode **114** übereinstimmen. Wenn das Computergerät **102** ermittelt, dass die erhaltenen biometrischen Daten mit den biometrischen Daten für sowohl den Sicherheitscode des Geräts **106** als auch den Organisationssicherheitscode **114** übereinstimmen, stellt das Computergerät **102** einen Zugriff auf die Anwendungen der Organisation **116** bereit, z. B. beginnt eine Sitzung, in der der Griff auf die Anwendungen der Organisation **116** erlaubt sind.

[0085] Wenn das Computergerät **102** ermittelt, dass die erhaltenen biometrischen Daten nur mit biometrischen Daten für den Sicherheitscode des Geräts **106** übereinstimmen, wird das Computergerät **102** entsperrt, und stellt keinen Zugriff auf die Anwendungen der Organisation **116** bereit, z. B. das Computergerät **102** stellt eine Benutzerschnittstelle für die Benutzereingabe des Sicherheitscodes der Organisation **114** vor dem Aktivieren jeglicher Anwendungen der Organisation **116** bereit. Wenn das Computergerät **102** ermittelt, dass die erhaltenen biometrischen Daten nicht mit jeglichen gespeicherten biometrischen Daten übereinstimmen, kann das Computergerät **102** eine Benutzerschnittstelle bereitstellen, die eine erneute Eingabe eines Sicherheitscodes anfordert.

[0086] In einigen Beispielen kann das Computergerät **102** die Eingabe des Sicherheitscodes der Organisation **114** von einem Bildschirm mit Sperrfunktion aus ermöglichen. Zum Beispiel kann das Computergerät **102** zwei unterschiedliche Entsperrungsbenutzerschnittstelle beinhalten, wobei jede, wie bereits vorstehend erörtert, mit einem unterschiedlichen Hintergrund identifiziert werden. Das Computergerät **102** kann eine erste Entsperrungsbenutzerschnittstelle für Benutzereingaben präsentieren, welche den Sicherheitscode des Geräts **106** in Reaktion auf eine erste Benutzereingabe auf einem Bildschirm mit Sperrfunktion des Computergeräts **102** zu spezifizieren, z. B. ein Wischen von der linken Seite des Bildschirms mit Sperrfunktion zur rechten Seite des Bildschirms mit Sperrfunktion. Das Computergerät **102** kann eine zweite Entsperrungsbenutzerschnittstelle für eine Benutzereingabe präsentieren, welche den Organisationssicherheitscode **114** in Reaktion auf eine zweite und unterschiedliche Benutzereingabe auf den Bildschirm mit Sperrfunktion spezifiziert, z. B. ein Wischen von der rechten Seite des Bildschirms mit Sperrfunktion zur linken Seite des Bildschirms mit Sperrfunktion.

[0087] Wenn das Computergerät **102** eine Benutzereingabe erhält, welche den Organisationssicherheitscode **114** in der zweiten Benutzerschnittstelle spezifiziert während das Computergerät **102** gesperrt ist, stellt das Computergerät **102** einen Zugriff auf die Anwendungen der Organisation **116** und die Daten der Organisation **118** und nicht die Anwendungen **108** oder die Daten **110** bereit. Wenn das Computergerät **102** eine Aufforderung erhält, eine der Anwendungen **108** oder den Zugriff auf die Daten **110** zu aktivieren, stellt das Computergerät **102** eine Benutzerschnittstelle für eine Benutzereingabe des Sicherheitscodes des Geräts **106** bereit.

[0088] Wenn das Computergerät **102** in einigen Beispielen Meldungen für die Anwendungen der Organisation **116** auf einem Bildschirm mit Sperrfunktion präsentiert und als Antwort eine Benutzereingabe erhält, welche eine Meldung für eine der Anwendungen der Organisation **116** auswählt, stellt das Computergerät **102** eine Benutzerschnittstelle mit einer Entsperrfunktion bereit, welche eine Benutzereingabe erhält, die einen Organisationssicherheitscode **114** spezifiziert. Das Computergerät **102** bestätigt, dass die Benutzereingabe, die von der Entsperrungsbenutzerschnittstelle erhalten wird, mit dem Organisationssicherheitscode **114** übereinstimmt, und einen Zugriff auf Daten für die Meldung für die eine der Anwendungen der Organisation **116** bereitstellt.

[0089] Alternativ kann das Computergerät **102** eine Entsperrungsbenutzerschnittstelle bereitstellen, welche eine Benutzereingabe anfordert, die den Sicherheitscode des Geräts **106** in Reaktion auf den Erhalt der Benutzereingabe spezifiziert, welche die Meldung für eine der Anwendungen der Organisation auswählt. Wenn das Computergerät **102** bestätigt, dass der Sicherheitscode des Geräts **106** in die Entsperrungsbenutzerschnittstelle eingegeben worden ist, stellt das Computergerät **102** einen Sicherheitscode für die Benutzerschnittstelle bereit, die eine zweite Benutzereingabe anfordert, welche den Organisationssicherheitscode **114** spezifiziert. Das Computergerät **102** bestätigt, dass die zweite Benutzereingabe, die von einer Benutzerschnittstelle für den Sicherheitscode erhalten worden ist, mit dem Organisationssicherheitscode **114** übereinstimmt und einen Zugriff auf die Daten für die Meldung für die eine der Anwendungen der Organisation **116** bereitstellt.

[0090] Wenn das Computergerät **102** über separate Sicherheitscodes verfügt, z. B. wenn die Einstellung vereinheitlichter Sicherheitscodes **104** deaktiviert ist, wendet das Computergerät **102** keine Einstellungen vom Geräteprofil der Organisation **112** auf die Anwendungen **108** oder die Daten **110** an. Zum Beispiel versetzt das Computergerät **102** die Organisation oder einen Administrator der Organisation nicht in die Lage, jegliche Anwendungen oder Daten zu steuern, die nicht dem Geräteprofil der Organisation **112** zugewiesen worden sind und versetzt lediglich die Organisation oder einen Administrator der Organisation in die Lage, die Anwendungen der Organisation **116**, die auf dem Computergerät **102** installiert sind und die Daten der Organisation **118**, die auf dem Computergerät **102** gespeichert sind, zu steuern.

[0091] Wenn das Computergerät **102** über einen vereinheitlichten Sicherheitscode verfügt, kann das Computergerät **102** in einigen Implementierungen über einen Organisationssicherheitscode **114** und über keinen Sicherheitscode des Geräts **106** verfügen, z. B. kann der Sicherheitscode des Geräts **106** deaktiviert sein. Zum Beispiel kann das Computergerät **102** keinen Sicherheitscode anfordern, um das Computergerät **102** zu entsperren, während der Organisationssicherheitscode **114** angefordert wird, um auf Anwendungen der Organisation **116** zuzugreifen.

[0092] Das Computergerät **102** kann PCs, mobile Kommunikationsgeräte und andere Geräte beinhalten, die Daten über das Netz **130** senden und empfangen können. Das Netzwerk **130**, wie etwa ein lokales Netzwerk (LAN), ein Weitverkehrsnetz (WAN), das Internet, oder eine Kombination davon, stellen eine Verbindung zwischen dem Computergerät **102**, der Anwendungsdatenbank **120** und dem Organisationssystem **126** her.

[0093] **Fig.** 5 ist ein Flussdiagramm eines Verfahrens **500** für das Aktivieren einer Organisationsanwendung. Zum Beispiel kann Verfahren **500** vom Computergerät **102** aus der Umgebung **100** verwendet werden.

[0094] Während das Computergerät gesperrt ist, stellt ein Computergerät eine erste Entsperrungsbenutzerschnittstelle (**502**) bereit. Zum Beispiel fordert eine erste Entsperrungsbenutzerschnittstelle eine Benutzereingabe eines Sicherheitscodes des Geräts an, um das Computergerät zu entsperren. Eine erste Entsperrungsbenutzerschnittstelle kann einen ersten Hintergrund beinhalten, z. B. der nicht organisationsspezifisch ist.

[0095] Das Computergerät erhält eine erste Benutzereingabe, welche einen Sicherheitscode für das Entsperren des Computergeräts (**504**) spezifiziert. Das Computergerät vergleicht die erste Benutzereingabe mit Daten für den Sicherheitscode des Geräts, um zu ermitteln, ob die erste Benutzereingabe einen zugelassenen Sicherheitscode des Geräts darstellt, z. B. zugelassenes Passwort oder biometrische Daten.

[0096] Das Computergerät wird entsperrt (**506**). Nachdem ermittelt worden ist, dass die erste Benutzereingabe ein zugelassener Sicherheitscode des Geräts ist, wird das Computergerät entsperrt, und stellt einen Zugriff auf eine oder mehrere Anwendungen des Geräts bereit, welche nicht von einem Geräteprofil der Organisation einer Organisation verwaltet werden.

[0097] Das Computergerät erhält eine zweite Benutzereingabe, welche ein Benutzerschnittstellenelement auswählt, um ein Anwendungsprogramm zu aktivieren, das auf dem Computergerät installiert ist, und einem Profil für eine Organisation zugeordnet worden ist (**508**). Zum Beispiel erhält das Computergerät eine zweite Benutzereingabe, die ein Symbol, das auf einem Hauptbildschirm des Computergeräts präsentiert wird, identifiziert. Das Computergerät ermittelt, dass das Symbol für ein Anwendungsprogramm gedacht ist, und dass es sich bei der zweiten Benutzereingabe um eine Anforderung, das Anwendungsprogramm zu aktivieren, handelt.

[0098] Das Computergerät stellt eine zweite Entsperrungsbenutzerschnittstelle bereit, wobei die zweite Entsperrungsbenutzerschnittstelle über eine unterschiedliche Benutzerschnittstelle als die erste Entsperrungsbenutzerschnittstelle (**510**) verfügt. Die zweite Entsperrungsbenutzerschnittstelle kann einen zweiten Hintergrund beinhalten, der spezifisch für die Organisation ist. Zum Beispiel kann die erste Entsperrungsbenutzerschnittstelle über eine allgemeine Hintergrundfarbe verfügen und die zweite Entsperrungsbenutzerschnittstelle kann über ein Bild

verfügen, z. B. Logo der Organisation. Der Hintergrund der zweiten Entsperrungsbenutzerschnittstelle ermöglicht die Erkennung der zweiten Entsperrungsbenutzerschnittstelle als eine Anforderung des Sicherheitscodes der Organisation auf dem Computergerät.

[0099] Das Computergerät erhält eine dritte Benutzereingabe, die einen Organisationssicherheitscode für das Zugreifen auf das Anwendungsprogramm (**512**) spezifiziert. Das Computergerät vergleicht die dritte Benutzereingabe mit dem Organisationssicherheitscode, um zu ermitteln, ob ein Zugriff auf das Anwendungsprogramm erlaubt werden soll, z. B. eine der Organisationsanwendungen, wie etwa eine Prozessablaufanwendung.

[0100] Das Computergerät aktiviert das Anwendungsprogramm (**514**). Als Antwort auf das Ermitteln, dass die dritte Benutzereingabe ein genehmigter Organisationssicherheitscode ist, aktiviert das Computergerät das Anwendungsprogramm. Das Computergerät kann das Prozessablauf-Programm starten, falls das Prozessablauf-Programm bereits läuft. Das Computergerät kann das Präsentieren einer Benutzerschnittstelle für das Prozessablauf-Programm veranlassen, z. B. wenn das Prozessablauf-Programm im Hintergrund läuft und nicht auf einem Display für das Computergerät präsentiert wird.

[0101] Das Computergerät erhält Anweisungen um einen Zugriff auf das Anwendungsprogramm und auf jeglichen anderen Anwendungsprogrammen zu verhindern, welche dem Profil für die Organisation (**516**) zugeordnet sind. Die Anweisungen können in Reaktion auf eine zuvor festgelegte Menge fehlgeschlagener Versuche, den Organisationssicherheitscode für den Zugriff auf das Anwendungsprogramm einzugeben oder in Reaktion auf die Eingabe des Administrators, mit dem Ziel den Zugriff auf das Anwendungsprogramm zu verhindern, erhalten werden. Zum Beispiel erhält das Computergerät Anweisungen von einem Computer, der von der Organisation verwaltet wird, um jeglichen Zugriff auf die Anwendungen der Organisation oder die Daten der Organisation zu verhindern, wenn der Computer die Eingabe des Administrators erhält, die angibt, dass der Zugriff auf die Anwendung verhindert werden sollte. Das Computergerät kann ermitteln, dass die Anweisungen angeben, dass Daten und Anwendungen für die Organisation vom Computergerät entfernt werden sollen.

[0102] Wenn das Computergerät über separate Sicherheitscodes verfügt, wendet das Computergerät die Anweisungen auf Anwendungen oder Daten an, die nicht einem Geräteprofil der Organisation zugehören. Zum Beispiel gelten die Anweisungen nicht für die Anwendungen **108** oder die Daten **110**, die vorstehend mit Bezugnahme auf **Fig.** 1 beschrieben werden.

[0103] Wenn das Computergerät über einen einzelnen vereinheitlichten Sicherheitscode verfügt, wendet das Computergerät die Anwendungen auf alle Anwendungen und Daten des Geräts an. Zum Beispiel erlaubt das Computergerät nicht das Entsperren des Computergeräts, denn das Computergerät stellt sich selbst zu Fabrikbedingungen wieder her, indem alle Anwendungen und Daten, die auf dem Gerät gespeichert werden nach der Installation eines Betriebssystems auf dem Computergerät, oder beide, entfernt werden.

[0104] Das Computergerät erhält eine vierte Benutzereingabe, welche einen Zugriff auf das Anwendungsprogramm (**518**) anfordert. Wenn das Computergerät beispielsweise keine Daten für die Anwendungen für die Organisation von einem Speicher des Computergeräts entfernt, kann das Computergerät eine Benutzereingabe erhalten, welche die Auswahl der Benutzerschnittstellenelemente spezifiziert, um das Anwendungsprogramm zu aktivieren, z. B. die auf einem Hauptbildschirm des Computergeräts präsentiert werden.

[0105] Das Computergerät ermittelt keinen Zugriff auf die Anwendungsprogramme in Reaktion auf das Erhalten der Anwendungen, um einen Zugriff auf das Anwendungsprogramm und auf alle anderen Anwendungsprogramme, die dem Profil für die Organisation zugeordnet worden sind, bereitzustellen. (**520**). Das Computergerät ermittelt, dass die Anweisungen erhalten worden sind, die angeben, dass der Zugriff auf das Anwendungsprogramm und sonstige Anwendungsprogramme für die Organisation nicht erlaubt werden sollten und aktiviert das Anwendungsprogramm nicht.

[0106] In einigen Implementierungen kann das Verfahren **500** zusätzliche Schritte, weniger Schritte, oder einige der Schritte beinhalten, die in mehrere Schritte unterteilt werden können. Zum Beispiel kann das Computergerät die Schritte **502** bis **514** oder Schritt **516** (allein) ohne das Durchführen der anderen Schritte des Verfahrens **500** durchführen. In einigen Implementierungen kann das Verfahren **500** einen oder mehrere Schritte vom Prozess **600**, der nachstehend detaillierter beschrieben wird, beinhalten.

[0107] **Fig.** 6 ist ein Flussdiagramm für ein Verfahren **600** für das Einstellen eines vereinheitlichten Sicherheitscodes. Zum Beispiel kann Verfahren **600** vom Computergerät **102** aus der Umgebung **100** verwendet werden.

[0108] Ein Computergerät identifiziert, dass ein Anwendungsprogramm, welches auf dem Computergerät installiert worden ist, einem Profil für eine Organisation (**602**) zugeordnet worden ist. Zum Beispiel kann ein Anwendungsprogramm eine neu installier-

te Anwendung oder eine Anwendung sein, die zuvor installiert worden ist. Das Computergerät kann ermitteln, dass das Anwendungsprogramm noch nicht ausgeführt worden ist, und identifizieren, dass das Anwendungsprogramm dem Profil für die Organisation in Reaktion auf eine Anfrage, die Anwendung auszuführen, zugeordnet worden ist.

[0109] Das Computergerät identifiziert, dass das Profil für die Organisation einen Sicherheitscode für den Zugriff auf das Anwendungsprogramm (**604**) erfordert. Zum Beispiel ermittelt das Computergerät, dass das Organisationsprofil spezifiziert, dass ein Sicherheitscode erforderlich ist, um auf einige Programme oder Daten für die Organisation zuzugreifen, wie etwa eine Prozessablauf-Anwendung der Organisation, und Daten, welche Projekte und Termine repräsentieren.

[0110] Das Computergerät stellt eine Benutzerschnittstelle bereit, mit der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät separate Sicherheitscodes für das Sperren des Computergeräts und den Zugriff auf das Anwendungsprogramm (**606**) bereitstellen sollte. Das Computergerät kann eine Benutzerschnittstelle in Reaktion auf das Identifizieren bereitstellen, dass das Profil für die Organisation einen Sicherheitscode für den Zugriff auf die Anwendung erfordert.

[0111] In einigen Beispielen präsentiert das Computergerät die Benutzerschnittstelle für Sicherheitseinstellungen bei **200a**, die vorstehend detaillierter beschrieben ist. Das Computergerät kann anfänglich einen vereinheitlichten Sicherheitscode erstellen, z. B. einen einzelnen Sicherheitscode, um das Computergerät zu entsperren und um auf die Anwendungen für die Organisation zuzugreifen, und dann eine Benutzerschnittstelle für den Erhalt der Benutzereingabe bereitstellen, welche spezifiziert, ob das Computergerät separate Sicherheitscodes für das Entsperren des Computergeräts und den Zugriff auf Anwendungen für die Organisation verwenden sollte.

[0112] In einigen Implementierungen kann das Computergerät ermitteln, ob das Computergerät mehrere Sicherheitscodes unterstützt. Zum Beispiel kann das Computergerät ermitteln, ob die Hardware des Computergeräts die dateibasierte Verschlüsselung oder die blockbasierte Verschlüsselung unterstützt. Als Antwort auf das Ermitteln, dass das Computergerät die dateibasierte Verschlüsselung unterstützt, z. B. dass ein Speicher des Computergeräts die dateibasierte Verschlüsselung unterstützt, stellt das Computergerät die Benutzerschnittstelle bereit. Als Antwort auf das Ermitteln, dass das Computergerät die blockbasierte Verschlüsselung unterstützt, ergreift das Computergerät keine weiteren Maßnahmen, z. B. und beendet das Durchführen der Schritte im Verfahren **600**.

[0113] Das Computergerät erhält eine erste Benutzereingabe, die spezifiziert, dass das Computergerät einen einzelnen Sicherheitscode verwenden soll, um sowohl das Computergerät zu entsperren als auch auf Anwendungsprogramme zuzugreifen (**608**). Zum Beispiel erhält das Computergerät eine erste Benutzereingabe über die Benutzerschnittstelle für Sicherheitseinstellungen **200a**. Das Computergerät kann eine oder mehrere zusätzliche Benutzerschnittstellen bereitstellen, welche das Auswählen des einzelnen Sicherheitscodes bestätigen, um sowohl das Computergerät zu entsperren als auch auf das Anwendungsprogramm zuzugreifen.

[0114] Während das Computergerät gesperrt ist erhält das Computergerät eine zweite Benutzereingabe, die den einzelnen Sicherheitscode spezifiziert, um sowohl das Computergerät zu entsperren als auch um auf das Anwendungsprogramm (**610**) zuzugreifen. Zum Beispiel stellt das Computergerät einen Bildschirm mit Sperrfunktion und eine Menüoption bereit, um eine Präsentation eines Bildschirms mit Sperrfunktion zu veranlassen. Das Computergerät erhält eine Benutzereingabe, welche die Auswahl der Menüoption spezifiziert und als Antwort eine Entsperrungsbenutzerschnittstelle bereitstellt, z. B. das Präsentieren der Entsperrungsbenutzerschnittstelle auf einem Display des Computergeräts. Das Computergerät erhält eine zweite Benutzerschnittstelle in Reaktion auf das Präsentieren der Entsperrungsbenutzerschnittstelle. Das Computergerät validiert die zweite Benutzereingabe, um zu bestätigen, dass die zweite Benutzereingabe ein gültiger Sicherheitscode für das Computergerät ist.

[0115] Das Computergerät wird entsperrt (**612**). Zum Beispiel wird das Computergerät in Reaktion auf das Erhalten und Validieren des einzelnen Sicherheitscodes entsperrt.

[0116] Das Computergerät erhält eine dritte Benutzereingabe, welche ein Benutzerschnittstellenelement auswählt, um das Anwendungsprogramm zu aktivieren (**614**). Zum Beispiel stellt das Computergerät nach dem Entsperren eine Benutzerschnittstelle für den Hauptbildschirm bereit, welche Symbole für Anwendungen beinhaltet, einschließlich der Prozessablauf-Anwendung, die auf dem Computergerät installiert sind. Das Computergerät erhält eine dritte Benutzereingabe, welche das Auswählen eines Symbols für die Prozessablauf-Anwendung spezifiziert.

[0117] Das Computergerät aktiviert das Anwendungsprogramm, ohne anzufordern, dass die Benutzereingabe einen Sicherheitscode bereitstellt (**616**). Zum Beispiel veranlasst das Computergerät das Anwendungsprogramm, wie z. B. die Prozessablauf-Anwendung, dazu, eine Benutzerschnittstelle für ein Anwendungsprogramm zu präsentieren, ohne eine Eingabe eines Sicherheitscodes der Organisation von

Seiten des Benutzers zwischen dem Erhalt der dritten Benutzereingabe zu erfordern, die das Benutzerschnittstellenelement für das Aktivieren des Anwendungsprogramms und das Anwendungsprogramm, das die Benutzerschnittstelle präsentiert, auswählt.

[0118] Die Reihenfolge der Schritte im vorstehend beschriebenen Prozess **600** ist veranschaulichender Natur und die Einstellung des einheitlichen Sicherheitscodes kann in unterschiedlicher Reihenfolge durchgeführt werden. Zum Beispiel kann das Computergerät identifizieren, dass das Profil für die Organisation einen Sicherheitscode für den Zugriff auf Anwendungsprogramme erfordert und die Benutzerschnittstelle bereitstellt, mit der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät separate Sicherheitscodes verwendet, bevor es identifiziert, dass das Ermittlungsprogramm installiert worden ist, z. B. vor der Installation des Anwendungsprogramms auf dem Computergerät.

[0119] In einigen Implementierungen kann das Verfahren **600** zusätzliche Schritte, oder weniger Schritte enthalten, oder einige der Schritte können in mehrere Schritte unterteilt werden. Zum Beispiel kann das Computergerät die Schritte **602** bis **608**, oder Schritte **604** bis **608** ohne das Durchführen der Schritte im Verfahren **600** durchführen.

[0120] Bezieht man sich nun auf **Fig.** 7 wird ein konzeptuelles Diagramm eines Systems veranschaulicht, das zur Implementierung der in diesem Dokument beschriebenen Systeme und Verfahren verwendet werden kann. Im System kann das mobile Computergerät **710** drahtlos mit einer Basisstation **740** kommunizieren, die für das mobile Computergerät einen drahtlosen Zugang zu zahlreichen gehosteten Diensten **760** über ein Netzwerk **750** anbieten.

[0121] In dieser Illustration wird das mobile Computergerät **710** als ein tragbares Mobiltelefon (z. B. ein Smartphone oder Anwendungstelefon) dargestellt, das ein Touchscreen-Anzeigegerät **712** zur Anzeige von Inhalten für einen Benutzer des mobilen Computergeräts **710** und zum Empfang von taktilen Benutzereingaben beinhaltet. Es können auch andere visuelle, akustische und taktile Ausgabekomponenten vorhanden sein (z. B. LED-Leuchten, ein Lautsprecher für tonale, sprachgenerierte oder aufgezeichnete Ausgaben oder Vibrationsmechanismen zur taktilen Ausgabe), wie auch verschiedene Eingabekomponenten (z. B. Tastatur **714**, physische Tasten, Trackballs, Beschleunigungsmesser, Gyroskope und Magnetometer).

[0122] Exemplarische visuelle Ausgabemechanismen in der Form von Anzeigegerät **712** können die Form einer Anzeige mit widerstehenden oder kapazitiven taktilen Fähigkeiten annehmen. Das Anzeigegerät kann zum Anzeigen von Video, Grafiken, Bildern und Text, und zum Koordinieren von Toucheingaben des Benutzers an den Standorten mit der Position der angezeigten Information, so dass das Gerät **710** einen Benutzerkontakt an einer Position eines angezeigten Artikels mit dem Artikel verknüpfen kann. Das mobile Computergerät **710** kann auch alternative Formen annehmen, einschließlich einem Laptopcomputer, oder einem Tablet oder einem Schiefertafelcomputer, einem persönlichen digitalen Assistenten, einem eingelagerten System (z. B. ein Autonavigationssystem), einem persönlichen Desktopcomputer oder einer computerisierten Arbeitsstation sein.

[0123] Ein Beispielmechanismus zum Empfang von Benutzereingaben beinhaltet die Tastatur **714**, die eine volle Qwerty-Tastatur oder ein herkömmliches Keypad, das Tasten für die Zeichen „0–9“, „*“ und „#“ beinhaltet. Die Tastatur **714** erhält eine Eingabe, wenn ein Benutzer auf eine Taste der Tastatur drückt oder einen physikalischen Kontakt dazu herstellt. Die Benutzermanipulation eines Trackballs **716** oder die Interaktion mit einem Trackpad befähigen den Benutzer zur Eingabe von Richtungs- und Rotationsinformationen in das mobile Computergerät **710** (z. B. zum Verschieben eines Cursors auf dem Anzeigegerät **712**).

[0124] Das mobile Computergerät **710** kann in der Lage sein, die Stelle des physischen Kontakts mit dem Touchscreen-Anzeigegerät **712** zu bestimmen (z. B. eine Kontaktstelle mit dem Finger oder einem Stylus). Mit Nutzung des Touchscreen **712** können verschiedene „virtuelle“ Eingabemechanismen hervorgebracht werden, wo ein Benutzer mit einer grafischen Schaltfläche auf dem Touchscreen **712** durch Berühren der grafischen Schaltfläche interagiert. Ein Beispiel eines „virtuellen“ Eingabemechanismus ist eine „Softwaretastatur“, die auf dem Touchscreen angezeigt wird und ein Benutzer betätigt die Tasten durch Drücken der entsprechenden Bereiche auf dem Touchscreen **712**.

[0125] Das mobile Computergerät **710** kann mechanische oder berührungsempfindliche Schaltflächen **718a**–d beinhalten. Zusätzlich dazu kann das mobile Computergerät Schaltflächen zur Einstellung der Lautstärke des einen oder der mehreren Lautsprecher **720** und einen Knopf zum Ein- und Ausschalten des mobilen Computergeräts beinhalten. Ein Mikrofon **722** ermöglicht dem mobilen Computergerät **710** die Umwandlung hörbarer Klänge in ein elektrisches Signal, das digital codiert und in computerlesbarem Speicher abgelegt oder an ein anderes Computergerät übertragen werden kann. Das mobile Computergerät **710** kann auch einen digitalen Kompass, einen Beschleunigungsmesser, Annäherungssensoren und Lichtsensoren beinhalten.

[0126] Ein Betriebssystem kann eine Schnittstelle zwischen der Hardware des mobilen Computergeräts (z. B. die Eingabe-/Ausgabemechanismen und Prozessor ausführbare Anweisungen, die vom computerlesbaren Medium abgerufen werden) und der Software, bereitstellen. Exemplarische Betriebssysteme beinhalten ANDROID, CHROME, IOS, MAC OS X, WINDOWS 7, WINDOWS PHONE 7, SYMBIAN, BLACKBERRY, WEBOS, eine Vielzahl von UNIX Betriebssysteme; oder ein urheberrechtlich geschütztes Betriebssystem für computergestützte Geräte. Das Betriebssystem kann eine Plattform für die Ausführung von Anwendungsprogrammen bieten, die die Interaktion zwischen dem Computergerät und einem Benutzer erleichtern.

[0127] Das mobile Computergerät **710** kann eine grafische Benutzerschnittstelle auf dem Touchscreen **712** anzeigen. Eine grafische Benutzerschnittstelle ist eine Zusammenstellung eines oder mehrerer grafischen Oberflächenelemente und kann statisch (z. B. bleibt die Anzeige gleich über einen gewissen Zeitraum) oder dynamisch (z. B. beinhaltet die grafische Benutzerschnittstelle grafische Oberflächenelemente die ohne Benutzereingabe animiert werden) sein.

[0128] Ein grafisches Schnittstellenelement kann Text, Linien, Formen, Bilder oder Kombinationen davon sein. Zum Beispiel kann ein grafisches Oberflächenelement ein Icon sein, das mit dem dazugehörigen Text auf dem Desktop angezeigt wird. In manchen Beispielen kann ein grafisches Oberflächenelement mit einer Benutzereingabe ausgewählt werden. Ein Benutzer kann ein grafisches Schnittstellenelement durch Pressen eines Bereiches auf dem Touchscreen auswählen, der einer Anzeige auf dem grafischen Schnittstellenelement entspricht. In manchen Beispielen kann der Benutzer einen Trackball manipulieren, um ein einzelnes grafisches Oberflächenelement hervorzuheben. Die Benutzerauswahl eines grafischen Oberflächenelements kann eine vorgegebene Aktion durch das mobile Computergerät auslösen. In manchen Beispielen entsprechen auswahlfähige grafische Oberflächenelemente ferner oder alternativ eine Taste auf der Tastatur **704**. Die Betätigung der Taste durch den Benutzer kann eine vorgegebene Aktion auslösen.

[0129] In manchen Beispielen bietet das Betriebssystem eine graphische-„Desktop"-Benutzerschnittstelle, die beim Einschalten des mobilen Computergeräts **710**, nach dem Aktivieren des mobilen Computergeräts **710** aus einem Ruhezustand, nach dem „Entsperren" des mobilen Computergeräts **710** oder nach dem Erhalt der Benutzer-Auswahl der „Home"-Schaltfläche **718c** angezeigt wird. Die grafische Desktop-Benutzerschnittstelle kann verschiedene grafische Schnittstellenelemente anzeigen, deren Auswahl entsprechende Anwendungsprogramme aufruft. Ein aufgerufenes Anwendungsprogramm eine grafische Schnittstelle anzeigen, welche die grafische Desktop-Benutzerschnittstelle ersetzt, bis das Anwendungsprogramm beendet oder ausgeblendet wird.

[0130] Benutzereingaben können eine Abfolge von Operationen des mobilen Computergeräts **710** beeinflussen. Eine einmalige Benutzereingabe (z. B. ein einmaliges Tippen auf den Touchscreen, ein Wischen über den Touchscreen, das Berühren einer Schaltfläche oder eine gleichzeitige Kombination davon) kann beispielsweise eine Operation auslösen, welche eine Anzeige der Benutzerschnittstelle ändert. Ohne die Benutzereingabe ändert sich die Benutzerschnittstelle nicht zu einer bestimmten Zeit. Zum Beispiel kann eine Multitouch-Benutzereingabe im Touchscreen **712** auf eine Kartenanwendung zurückgreifen, um einen Standort „heranzuzoomen", obwohl die Kartenanwendung nach mehreren Sekunden eine Standardzoomeinstellung anzeigt.

[0131] Die grafische Desktop-Schnittstelle kann auch „Widgets" anzeigen. Ein Widget ist/sind ein oder mehrere grafische Oberflächenelement/e, die einem ausgeführten Anwendungsprogramm zugeordnet sind, die unter Kontrolle des laufenden Anwendungsprogramms im Desktop-Inhalt angezeigt werden. Ein Widget-Anwendungsprogramm kann starten, während das mobile Gerät sich einschaltet. Ferner braucht ein Widget nicht im Mittelpunkt des gesamten Displays zu stehen. Stattdessen kann ein Widget nur einen kleinen Teil des Desktops einnehmen, der in diesem Desktopteil Inhalte anzeigt und Touchscreen-Benutzereingaben empfängt.

[0132] Das mobile Computergerät **710** kann ein oder mehrere Ortungsverfahren beinhalten. Ein Ortungsverfahren kann eine Reihe von Hardware- und Softwareprodukten beinhalten, die dem Betriebssystem und Anwendungsprogrammen eine Schätzung der geografischen Position des Mobiltelefons bereitstellen. Ein Ortungsverfahren kann satellitengestützte Positionierungstechniken, Basisstation-Übertragungsantennenkennung, multiple Basisstation-Triangulation, Internet-Zugangspunkt-Standortbestimmungen (IP), inferenzielle Bezeichnung einer Benutzerposition ausgehend von Suchmaschinenanbfragen und vom Benutzer angegebene Standortbezeichnungen (z. B. durch „Einchecken" an einem Standort) anwenden.

[0133] Das mobile Computergerät **710** kann andere Anwendungen, Rechnerteilsysteme und Hardware beinhalten. Eine Bearbeitungseinheit für Anrufe kann eine Anzeige eines eintreffenden Telefonanrufs erhalten und einem Benutzer die Fähigkeit bereitstellen, den eintreffenden Anruf entgegenzunehmen. Ein Medienplayer kann einem Benutzer das Anhören von Musik oder das Abspielen von Filmen ermöglichen, die in einem lokalen Speicher des mobilen Compu-

tergeräts **710** aufgezeichnet sind. Das mobile Gerät **710** kann einen digitalen Kamerasensor, und entsprechende Bild- und Videoaufnahmen sowie Bearbeitungssoftware beinhalten. Ein Internetbrowser kann den Benutzer befähigen, Inhalte von einer Webseite anzuzeigen, indem er die Adresse der Webseite eingibt oder einen Link zu der Webseite anwählt.

[0134] Das mobile Computergerät **710** kann eine Antenne zur drahtlosen Kommunikation mit der Basisstation **740** beinhalten. Die Basisstation **740** kann eine von vielen Basisstationen in einer Reihe von Basisstationen sein (z. B. Mobiltelefon-Funknetz), die das mobile Computergerät **710** zur Aufrechterhaltung der Kommunikation mit einem Netz **750** befähigt, während das mobile Computergerät geografisch bewegt wird. Das Computergerät **710** kann alternativ oder zusätzlich mit dem Netz **750** über einen Wi-Fi-Router oder eine drahtgestützte Verbindung (z. B. Ethernet, USB oder FIREWIRE) kommunizieren. Das Computergerät **710** kann über BLUETOOTH-Protokolle auch drahtlos mit anderen Computergeräten kommunizieren oder ein drahtloses Ad-hoc-Netz nutzen.

[0135] Ein Dienstanbieter, der das Netzwerk mit Basisstationen betreibt, kann das mobile Computergerät **710** mit dem Netzwerk **750** verbinden, um eine Kommunikation zwischen dem mobilen Computergerät **710** und anderen Computersystemen zu ermöglichen, welche die Dienste **760** bereitstellen. Obgleich die Dienste **760** über verschiedene Netze angeboten werden können (z. B. das interne Netz des Serviceanbieters, das öffentliche Telefonnetz und das Internet), wird das Netz **750** als ein einzelnes Netz dargestellt. Der Dienstanbieter kann ein Serversystem **752** betreiben, das Informationspakete und Sprachdaten zwischen dem mobilen Computergerät **710** und den Rechnersystemen sendet, die mit den Diensten **760** verknüpft sind.

[0136] Das Netzwerk **750** kann das mobile Computergerät **710** mit dem öffentlich geschalteten Telefonnetzwerk (Public Switched Telephone Network PSTN) **762** verbinden, um Sprach- oder Fax-Kommunikation zwischen dem mobilen Computergerät **710** und einem anderen Computergerät zu etablieren. Zum Beispiel kann das Serviceanbieter-Serversystem **752** einen Hinweis vom PSTN **762** auf einen eingehenden Anruf für das mobile Computergerät **710** empfangen. Im Gegenzug kann das mobile Computergerät **710** eine Kommunikation an den Dienstleistungsanbieter Serversystem **752** senden, um einen Telefonanruf durch das Benutzen einer Telefonnummer zu initiieren, die mit einem Gerät verknüpft ist, das durch das PSTN **762** zugänglich ist.

[0137] Das Netz **750** kann das das mobile Computergerät **710** mit einem VoIP-Dienst **764** (Voice over Internet Protocol) verbinden, der Sprechverbindungen über ein IP-Netz leitet, im Gegensatz zum PSTN. Zum Beispiel kann ein Benutzer des mobilen Computergeräts **710** auf eine VoIP-zurückgreifen und einen Anruf vornehmen, der das Programm nutzt. Das Serviceanbieter-Serversystem **752** kann Sprachdaten des Anrufs an einen VoIP-Dienst weiterleiten, der den Anruf über das Internet an ein entsprechendes Computergeräts weiterleitet, das potenziell den PSTN für einen abschließenden Arm der Verbindung benutzt.

[0138] Ein Application Store **766** kann einem Benutzer des mobilen Computergeräts **710** die Fähigkeit zum Durchsuchen einer Liste von entfernt gespeicherten Anwendungsprogrammen geben, die der Benutzer über das Netz **750** herunterladen und auf dem mobilen Computergerät **710** installieren kann. Der Application Store **766** kann als Archiv für Anwendungen dienen, die von dritten Anwendungsentwicklern entwickelt wurden. Ein auf dem mobilen Computergerät **710** installiertes Anwendungsprogramm kann in der Lage sein, über das Netz **750** mit Serversystemen zu kommunizieren, die für das Anwendungsprogramm bestimmt sind. Zum Beispiel kann ein VoIP-Anwendungsprogramm aus dem Application Store **766** heruntergeladen werden, das den Benutzer befähigt, mit dem VoIP-Dienst **764** zu kommunizieren.

[0139] Das mobile Computergerät **710** kann über das Netz **750** auf Inhalte im Internet **768** zugreifen. Zum Beispiel kann ein Benutzer des mobilen Computergeräts **710** auf eine Webbrowseranwendung zurückgreifen, die Daten von entfernten Computergeräten anfordern, die an dafür vorgesehenen universellen Ressourcenstandorten zugänglich sind. In verschiedenen Beispielen sind manche der Dienste **760** über das Internet zugänglich.

[0140] Das mobile Computergerät kann mit einem persönlichen Computer **770** kommunizieren. Zum Beispiel kann der Personal Computer **770** der Heimcomputer für einen Benutzer des mobilen Computergeräts **710** sein. Demzufolge kann der Benutzer in die Lage versetzt werden Medien von seinem Personal Computer **770** zu streamen. Der Benutzer kann auch die Dateistruktur seines Personal Computers **770** ansehen und ausgewählte Dokumente zwischen den computergestützten Geräten übertragen.

[0141] Ein Spracherkennungsdienst **772** kann mit dem Mikrofon des mobilen Computergeräts **722** aufgezeichnete Sprachkommunikationsdaten empfangen und die Sprachkommunikation in entsprechende textuelle Daten umgewandelt. In manchen Beispielen wird der umgewandelte Text als Webanfrage an eine Suchmaschine gesendet und Suchergebnisse mit relevanten Antworten werden an das mobile Computergerät **710** zurückgesendet.

[0142] Das mobile Computergerät **710** kann mit einem sozialen Netzwerk **774** kommunizieren. Das soziale Netzwerk kann zahlreiche Mitglieder beinhalten, von denen einige mit der Bezeichnung als Bekanntschaften einverstanden sind. Anwendungsprogramme auf dem mobilen Computergerät **710** können auf das soziale Netzwerk **774** zugreifen, um Informationen über die Bekanntschaften des Benutzers des mobilen Computergeräts abzurufen. Zum Beispiel kann ein „Adressbuch"-Anwendungsprogramm Telefonnummern für die Bekanntschaften des Benutzers abrufen. In verschiedenen Beispielen können Inhalte an das mobile Computergerät **710** basierend auf sozialen Netzwerkentfernungen vom Benutzer an andere Mitglieder in einer sozialen Netzwerkgrafik von Mitgliedern und verbundenen Beziehungen geliefert werden. Zum Beispiel können Werbungs- und Zeitungsartikelinhalte für den Benutzer ausgehend von einer Interaktionsebene mit Inhalten von Mitgliedern ausgewählt werden, die dem Benutzer „nahe stehen" (z. B. Mitglieder, die „Freunde" oder „Freunde von Freunden" sind).

[0143] Das mobile Computergerät **710** kann über das Netz **750** auf eine Reihe von persönlichen Kontakten **776** zugreifen. Jeder Kontakt kann eine Person bezeichnen und Informationen über diese Person beinhalten (z. B. Telefonnummer, E-Mail-Adresse und Geburtsdatum). Weil die Reihe von Kontakten entfernt für das mobile Computergerät **710** bereitgestellt wird, kann der Benutzer über verschiedene Geräte auf die Kontakte **776**, wie auf einen gemeinsamen Kontaktsatz, zugreifen und diese pflegen.

[0144] Das mobile Computergerät **710** kann auf cloudbasierte Anwendungsprogramme **778** zugreifen. Cloud-Computing bietet Anwendungsprogramme (z. B. einen Textprozessor oder ein E-Mail-Programm), die vom mobilen Computergerät **710** entfernt bereitgestellt werden und das Gerät **710** kann mithilfe eines Webbrowsers oder eines speziellen Programms darauf zugreifen. Beispiel für cloudgestützte Anwendungsprogramme beinhalten den Texteditor-Dienst GOOGLE DOCS, den Webmail-Dienst GOOGLE GMAIL und den Bilddatei-Manager PICASA.

[0145] Der Kartendienst **780** kann Straßenkarten, Streckenplanungsinformationen und Satellitenbilder an das mobile Computergerät **710** bereitstellen. Ein Beispiel für einen Kartendienst ist GOOGLE MAPS. Der Kartendienst **780** kann auch Anfragen empfangen und standortspezifische Ergebnisse zurücksenden. Zum Beispiel kann das mobile Computergerät **710** einen geschätzten Standort des mobilen Computergeräts und eine vom Benutzer eingegebene Anfrage nach „Pizzerias" an den Kartendienst **780** senden. Der Kartendienst **780** kann einen Stadtplan mit übergelegten „Markern" auf der Karte zurücksenden, die geografische Standorte von nahegelegenen „Pizzerias" kennzeichnen.

[0146] Der Turn-by-Turn-Dienst **782** kann dem mobilen Computergerät **710** Turn-by-Turn-Richtungshinweise zu einem vom Benutzer vorgegebenen Ziel vorgeben. Zum Beispiel kann der Turn-by-Turn-Dienst **782** ein Streaming einer Straßenansicht eines geschätzten Standorts des Geräts **710**, zusammen mit Daten zur Ausgabe von akustischen Hinweisen und übergelegten Pfeilen, die den Benutzer des Geräts **710** zu seinem Ziel führen, bereitstellen.

[0147] Verschiedene Formen von Streaming-Medien **784** können vom mobilen Computergerät **710** angefordert werden. Zum Beispiel kann das Computergerät **710** einen Stream für eine vorab aufgezeichnete Videodatei, ein Live-TV-Programm oder ein Live-Radioprogramm anfordern. Zu Beispieldiensten, die Streaming-Daten bereitstellen, gehören YOUTUBE und PANDORA.

[0148] Ein Mikro-Bloggingdienst **786** kann einen vom Benutzer eingegebenen Post vom mobilen Computergerät **710** empfangen, der keine Empfänger für den Post angibt. Der Mikro-Bloggingdienst **786** kann den Post an andere Mitglieder des Mikro-Bloggingdienstes **786** verbreiten, die einer Anmeldung beim Benutzer zustimmen.

[0149] Eine Suchmaschine **788** kann vom Benutzer auf dem mobilen Computergerät **710** eingegebene textuelle oder verbale Anfragen empfangen, eine Reihe von internetzugänglichen Dokumenten bestimmen, die auf die Anfrage antworten, und Informationen zur Anzeige einer Suchergebnisliste der relevanten Dokumente für das Gerät **710** bereitstellen. In Beispielen, in denen eine verbale Anfrage empfangen wird, kann der Spracherkennungsdienst **772** die empfangenen Audiosignale in eine Textabfrage umwandeln, die zur Suchmaschine gesendet wird.

[0150] Diese und andere Dienstleistungen können in einem Serversystem **790** implementiert werden. Ein Serversystem kann eine Kombination aus Hardware und Software darstellen, die eine Dienstleitung oder eine Reihe von Dienstleistungen bereitstellt. Eine Reihe von physikalisch getrennten und vernetzten Computergeräten können beispielsweise als eine logische Serversystemeinheit zum Handhaben des notwendigen Verfahrens zusammenarbeiten, um Hunderte von Computergeräten eine Dienstleistung anzubieten. Ein Serversystem ist hier auch als ein Computergerät bezeichnet.

[0151] In verschiedenen Ausführungen werden Verfahren, die „in Reaktion auf" oder „als eine Konsequenz von" eines anderen Verfahrens (z. B. einer\ Bestimmung oder eine Identifizierung) ausgeführt sind, nicht ausgeführt, wenn das vorherige Ver-

fahren nicht erfolgreich war (z. B. wenn die Bestimmung nicht ausgeführt wurde). Verfahren, die „automatisch“ durchgeführt werden sind Verfahren, die ohne Eingriff (z. B. eingreifende Benutzereingabe) durchgeführt werden. Gegenstände, die in diesem Dokument unter Verwendung des Konjunktivs beschrieben sind, kann optionale Implementierungen beschreiben. In manchen Beispielen beinhaltet die „Übertragung“ von einem ersten Gerät auf ein zweites Gerät die Eingabe von Daten in ein Netz zum Empfang durch das zweite Gerät, aber nicht den Empfang der Daten durch das zweite Gerät. Umgekehrt kann der „Empfang“ von einem ersten Gerät den Empfang der Daten aus einem Netz beinhalten, aber nicht die Übertragung der Daten durch das erste Gerät.

[0152] Das „Bestimmen“ durch ein Computersystem kann beinhalten, dass das Computersystem ein anderes Gerät anfordert, um die Bestimmung durchzuführen und die Resultate an das Computersystem zu liefern. Außerdem kann das „Anzeigen“ oder das „Präsentieren“ durch ein Computersystem beinhalten, dass das Computersystem Daten sendet, um zu veranlassen, dass ein anderes Gerät die hingewiesenen Informationen anzeigt oder präsentiert.

[0153] **Fig.** 8 ist ein Blockdiagramm von Computergeräten **800**, **850** die zur Implementierung der in diesem Dokument beschriebenen Systeme und Verfahren angewendet werden können, entweder als Client oder Server oder als Vielzahl von Servern. Computergerät **800** soll verschiedene Formen von Digitalcomputern darstellen, zum Beispiel Laptops, Desktops, Workstations, Personal Digital Assistants, Server, Blade Server, Mainframes und andere geeignete Computer. Computergerät **850** soll verschiedene Formen mobiler Geräte, wie Personal Digital Assistants, Mobiltelefone, Smartphones und andere ähnliche Computergeräte, darstellen. Die hier gezeigten Komponenten, ihre Verbindungen und Beziehungen sowie ihre Funktionen sind rein exemplarisch gemeint und stellen keine Einschränkung der in diesem Dokument beschriebenen und/oder beanspruchten Implementierungen.

[0154] Das Computergerät **800** beinhaltet einen Prozessor **802**, einen Speicher **804**, ein Speichergerät **806**, eine Hochgeschwindigkeitsschnittstelle **808**, die verbunden ist mit Speicher **804** und Hochgeschwindigkeits-Erweiterungsports **810**, und eine Niedriggeschwindigkeitsschnittstelle **812** zum Anschluss an den Hochgeschwindigkeitsbus **814** und das Speichergerät **806**. Alle der Komponenten **802**, **804**, **806**, **808**, **810** und **812** sind mithilfe verschiedener Busse miteinander verbunden und können an einer gemeinsamen Hauptplatine oder auf andere Weise, wie geeignet, angebracht sein. Der Prozessor **802** kann Anweisungen für die Ausführung im Computergerät **800** verarbeiten, zum Beispiel Anweisungen, die im Speicher **804** oder Speichergerät **806** gespeichert sind, um grafische Informationen für eine grafische Benutzerschnittstelle auf einem externen Eingabe-/Ausgabegerät anzuzeigen, zum Beispiel Display **816**, das mit der High-Speed-Schnittstelle **808** gekoppelt ist. In anderen Implementierungen können mehrere Prozessoren und/oder mehrere Busse verwendet werden, wie angemessen, zusammen mit mehreren Speichern und Speichertypen. Außerdem können mehrere Computergeräte **800** verbunden sein, wobei jedes Gerät Teile der nötigen Operationen bereitstellt (z. B. als Serverbank, eine Gruppe von Blade Servern oder ein Multiprozessor-System).

[0155] Der Speicher **804** speichert Informationen im Computergerät **800**. In einer Implementierung ist der Speicher **804** ein flüchtiges Speichergerät oder flüchtige Speichergeräte. In einer anderen Implementierung ist der Speicher **804** ein nicht flüchtiges Speichergerät oder nicht flüchtige Speichergeräte. Der Speicher **804** kann auch eine andere Form von computerlesbarem Medium sein, zum Beispiel ein magnetischer oder optischer Datenträger.

[0156] Das Speichergerät **806** kann Massenspeicher für das Computergerät **800** bereitstellen. In einer Ausführungsform kann das Speichergerät **806** ein computerlesbares Medium sein oder enthalten, zum Beispiel ein Diskettengerät, ein Festplattengerät, ein optisches Datenträgergerät oder ein Bandgerät, ein Flash-Speicher oder ein anderes ähnliches Solid-State-Speichergerät oder eine Reihe von Geräten, zum Beispiel Geräte in einem Storage Area Network oder anderen Konfigurationen. Ein Computerprogrammprodukt kann greifbar in einem Informationsträger ausgeführt sein. Das Computerprogrammprodukt kann auch Anweisungen enthalten, die, wenn sie ausgeführt werden, ein oder mehrere Verfahren durchführen, wie die oben beschriebenen. Der Informationsträger ist ein computer- oder maschinenlesbares Medium, wie der Speicher **804**, das Speichergerät **806** oder der Prozessorspeicher **802**.

[0157] Der Hochgeschwindigkeitscontroller **808** verwaltet bandbreitenintensive Operationen für das Computergerät **800**, während der Niedriggeschwindigkeitscontroller **812** weniger bandbreitenintensive Operationen verwaltet. Eine solche Zuordnung von Funktionen ist nur exemplarisch. In einer Implementierung ist die Hochgeschwindigkeitssteuerung **808** mit Speicher **804**, Anzeige **816** (z. B. über einen Grafikprozessor oder -beschleuniger) und mit den Hochgeschwindigkeits-Erweiterungsanschlüssen **810**, die verschiedene Erweiterungskarten (nicht gezeigt) akzeptieren können, verbunden. In der Implementierung ist die Niedergeschwindigkeitssteuerung **812** mit Speichervorrichtung **806** und Niedergeschwindigkeits-Erweiterungsanschlüssen **814** verbunden. Der langsame Erweiterungsanschluss, der verschiedene Kommunikationsanschlüsse (z. B. USB, B, Ethernet, Funkethernet) beinhalten kann, kann an ein oder

mehrere Eingabe-/Ausgabe-Geräte, wie eine Tastatur, ein Zeigegerät, einen Scanner oder ein Netzwerkgerät, wie einen Switch oder Router, z. B. durch einen Netzwerkadapter gekoppelt sein.

[0158] Das Computergerät **800** kann, wie in der Figur dargestellt, in einer Reihe verschiedener Formen implementiert sein. Es kann zum Beispiel als Standardserver **820** oder mehrmals in einer Gruppe solcher Server implementiert sein. Es kann auch als Teil eines Rackserversystems **824** implementiert sein. Außerdem kann es in einem Personal Computer, wie Laptop-Computer **822**, implementiert sein. Alternativ können Komponenten von Computergerät **800** mit anderen Komponenten in einem mobilen Gerät kombiniert sein (nicht dargestellt), z. B. Gerät **850**. Jedes solcher Geräte kann eines oder mehrere Computergeräte **800**, **850** enthalten, und ein gesamtes System kann aus mehreren Computergeräten **800**, **850** bestehen, die miteinander kommunizieren.

[0159] Das Computergerät **850** beinhaltet unter anderen Komponenten einen Prozessor **852**, einen Speicher **864**, eine Eingabe-/Ausgabevorrichtung, wie ein Display **854**, eine Verbindungsschnittstelle **866**, und einen Transceiver **868**. Das Gerät **850** kann auch mit einem Speichergerät ausgestattet sein, zum Beispiel einem Microdrive oder anderem Gerät, um zusätzlichen Speicher bereitzustellen. Alle der Komponenten **850**, **852**, **864**, **854**, **866** und **868** sind mithilfe verschiedener Busse miteinander verbunden und mehrere der Komponenten können an einer gemeinsamen Hauptplatine oder auf andere Weise, wie geeignet, angebracht sein.

[0160] Der Prozessor **852** kann Anweisungen im Computergerät **850** ausführen, einschließlich im Speicher **864** gespeicherte Anweisungen. Der Prozessor kann als ein Chipsatz von Chips implementiert werden, die separate und mehrere analoge und digitale Prozessoren beinhalten. Zusätzlich dazu kann der Prozessor mit einer beliebigen Anzahl von Architekturen implementiert werden. Der Prozessor kann beispielsweise ein CISC-Prozessor (Complex Instruction Set Computers), ein RISC-Prozessor (Reduced Instruction Set Computer) oder ein MISC-Prozessor (Minimal Instruction Set Computer) sein. Der Prozessor kann zum Beispiel für die Koordination der anderen Komponenten des Geräts **850** sorgen, zum Beispiel die Kontrolle von Benutzerschnittstellen, Anwendungen, die vom Gerät **850** ausgeführt werden, und die drahtlose Kommunikation durch Gerät **850**.

[0161] Der Prozessor **852** kann mit einem Benutzer über die Steueroberfläche **858** und die mit einem Display **854** gekoppelte Displayschnittstelle **856** kommunizieren. Das Display **854** kann zum Beispiel ein TFT (Thin-Film-Transistor Liquid Crystal Display)-Display oder ein OLED (Organic Light Emitting Diode)-Display oder eine andere geeignete Displaytechnologie sein. Die Displayschnittstelle **856** kann eine geeignete Schaltung enthalten, die das Display **854** dazu bringt, einem Benutzer grafische und andere Informationen zu präsentieren. Die Steuerschnittstelle **858** kann Befehle von einem Benutzer empfangen und sie für die Sendung an Prozessor **852** umwandeln. Zusätzlich kann eine externe Schnittstelle **862** in Verbindung mit dem Prozessor **852** bereitgestellt sein, um Nahbereichskommunikation von Vorrichtung **850** mit anderen Vorrichtungen zu ermöglichen. Die externe Schnittstelle **862** kann zum Beispiel in einigen Implementierungen eine kabelgebundene Kommunikation bereitstellen, oder in anderen Implementierungen eine drahtlose Kommunikation und es können auch mehrere Schnittstellen verwendet werden.

[0162] Der Speicher **864** speichert Informationen im Computergerät **850**. Der Speicher **864** kann als eines oder mehrere computerlesbare Medien, flüchtige Speichergeräte oder nicht flüchtige Speichergeräte implementiert werden. Erweiterungsspeicher **874** kann ebenfalls bereitgestellt und mit dem Gerät **850** über Erweiterungsschnittstelle **872** verbunden werden, die zum Beispiel eine SIMM(Single In Line Memory Module)-Kartenschnittstelle umfassen kann. Ein solcher Erweiterungsspeicher **874** kann zusätzlichen Speicherplatz für Gerät **850** bereitstellen oder er kann auch Anwendungen oder andere Informationen für Gerät **850** speichern. Insbesondere kann Erweiterungsspeicher **874** Anweisungen zum Ausführen oder Ergänzen der oben beschriebenen Prozesse enthalten und er kann außerdem sichere Informationen enthalten. Demnach kann Erweiterungsspeicher **874** beispielsweise als ein Sicherheitsmodul für Vorrichtung **850** bereitgestellt sein und kann mit Anweisungen programmiert sein, die eine sichere Benutzung von Vorrichtung **850** ermöglichen. Zusätzlich dazu können über die SIMM-Cards sichere Anwendungen bereitgestellt werden, zusammen mit zusätzlichen Informationen, wie das Ablegen von Identifizierungsinformationen auf der SIMM-Card auf eine Weise, die nicht gehackt werden kann.

[0163] Der Speicher kann zum Beispiel Flashspeicher und/oder NVRAM-Speicher beinhalten, wie unten besprochen. In einer Implementierung ist ein Computerprogrammprodukt greifbar in einem Informationsträger ausgeführt. Das Computerprogrammprodukt enthält Anweisungen, die, wenn sie ausgeführt werden, ein oder mehrere Verfahren durchführen, wie die oben beschriebenen. Der Informationsträger ist ein computer- oder maschinenlesbares Medium, wie der Speicher **864**, die Speichererweiterung **874** oder der Prozessorspeicher **852**, beispielsweise über den Transceiver **868** oder die externe Schnittstelle **862** empfangen werden kann.

[0164] Gerät **850** kann drahtlos über Kommunikationsschnittstelle **866** kommunizieren, die, wo nötig, eine digitale Signalverarbeitungsschaltung beinhal-

ten kann. Die Verbindungsschnittstelle **866** kann Verbindungen mit verschiedenen Kommunikationstypen oder -protokollen aufbauen, darunter GSM-Sprachanrufe, SMS, EMS, oder MMS-Messaging, CDMA, TDMA, PDC, WCDMA, CDMA2000 oder GPRS unter anderen. Eine solche Kommunikation kann zum Beispiel über Funkfrequenzempfänger **868** erfolgen. Zusätzlich kann eine Kurzstreckenkommunikation stattfinden, wie unter Verwendung eines Bluetooth-, WLAN- oder anderen solchen Sende-Empfängers (nicht gezeigt). Außerdem kann GPS(Global Positioning System)-Empfängermodul **870** zusätzliche mit der Navigation und dem Ort verbundene drahtlose Daten für Gerät **850** bereitstellen, die ggf. von Anwendungen verwendet werden können, die auf Gerät **850** ausgeführt werden.

[0165] Gerät **850** kann außerdem akustisch mithilfe von Audio-Codec **860** kommunizieren, der gesprochene Informationen von einem Benutzer empfangen und in nutzbare digitale Informationen umwandeln kann. Audio-Codec **860** kann ebenfalls akustische Töne für einen Benutzer erzeugen, zum Beispiel durch einen Lautsprecher zum Beispiel in einem Handgerät von Gerät **850**. Ein derartiger Ton kann einen Ton von Sprachfernsprechverbindungen beinhalten, kann aufgenommene Töne (z. B. Sprachnachrichten, Musikdateien, usw.) beinhalten und kann auch Töne, beinhalten, die von Anwendungen generiert werden, die auf Gerät **850** betrieben werden.

[0166] Das Computergerät **850** kann, wie in der Figur dargestellt, in einer Reihe verschiedener Formen implementiert sein. Es kann zum Beispiel als ein Mobiltelefon **880** implementiert werden. Es kann außerdem als Teil eines Smartphones **882**, Personal Digital Assistant oder eines anderen ähnlichen mobilen Geräts implementiert werden.

[0167] Das zusätzliche Computergerät **800** oder **850** kann USB-Speichermedien (Universal Serial Bus) beinhalten. Die USB-Speichermedien können Betriebssysteme und andere Anwendungen speichern. Die USB-Flashlaufwerke können Eingabe-/Ausgabekomponenten, wie z. B. einen kabellosen Transmitter oder USB-Anschluss enthalten, der in eine USB-Schnittstelle eines anderen Computers eingesteckt werden kann.

[0168] Verschiedene Implementierungen der hier beschriebenen Systeme und Techniken können in digitaler elektronischer Verschaltung, integrierter Verschaltung, in speziell konstruierten ASICs (anwendungsspezifische integrierte Schaltungen), in Computer-Hardware, Firmware, Software und/oder Kombinationen davon realisiert werden. Diese verschiedenen Implementierungen können eine Implementierung in einem oder mehreren Computerprogrammen beinhalten, die auf einem programmierbaren System ausführbar und/oder interpretierbar sind, das mindestens einen programmierbaren Prozessor beinhaltet, der ein spezieller oder für allgemeine Zwecke sein kann und der zum Empfangen von Daten und Anweisungen von und zum Übertragen von Daten und Anweisungen an ein Speichersystem, mindestens eine Eingabevorrichtung und mindestens eine Ausgabevorrichtung gekoppelt ist.

[0169] Diese Computerprogramme (auch bekannt als Programme, Software, Anwendungen oder Code) enthalten Maschinenbefehle für einen programmierbaren Prozessor und können in eine hochrangige verfahrens- und/oder objektorientierte Programmiersprache und/oder in eine Montage-/Maschinensprache umgesetzt werden. Wie hier verwendet, bezeichnen die Begriffe „maschinenlesbares Medium“, „computerlesbares Medium“ ein beliebiges Computerprogrammprodukt, eine beliebige Vorrichtung und/oder ein beliebiges Gerät (z. B. Magnetplatten, optische Platten, Speicher, programmierbare Logikbausteine (PLDs)), die verwendet werden, um einem programmierbaren Prozessor Maschinenanweisungen und/oder Daten bereitzustellen, einschließlich eines maschinenlesbaren Mediums, das Maschinenanweisungen als ein maschinenlesbares Signal empfängt. Der Begriff „maschinenlesbares Signal“ bezeichnet ein beliebiges Signal, das verwendet wird, um einem programmierbaren Prozessor Maschinenanweisungen und/oder Daten bereitzustellen.

[0170] Zur Interaktion mit einem Benutzer können die hier beschriebenen Techniken und Systeme auf einem Computer mit einem Bildschirm (z. B. einem CRT-(Cathode Ray Tube) oder LCD-(Liquid Crystal Display) Monitor) für die Anzeige von Informationen für den Benutzer und mit einer Tastatur und einem Zeigegerät (z. B. einer Maus oder einem Trackball), durch die der Benutzer Eingaben an den Computer weiterleiten kann, implementiert werden. Andere Arten von Geräten können auch verwendet werden, um eine Interaktion mit einem Benutzer bereitzustellen; zum Beispiel kann eine dem Benutzer bereitgestellte Rückmeldung irgendeine Form von Sinnesrückmeldung sein (z. B. visuelle Rückmeldung, auditive Rückmeldung oder Tastrückmeldung); und eine Eingabe vom Benutzer kann in einer beliebigen Form empfangen werden, einschließlich akustischer, Sprach- oder Tasteingaben.

[0171] Die hier beschriebenen Systeme und Techniken können in einem Computersystem implementiert werden, das eine Back-End-Komponente beinhaltet (z. B. als Datenserver) oder das eine Middleware-Komponente (z. B. einen Anwendungsserver) beinhaltet oder das eine Front-End-Komponente (z. B. einen Client-Computer, der eine grafische Benutzerschnittstelle oder einen Webbrowser aufweist, durch die ein Benutzer mit einer Implementierung der hier beschriebenen Systeme und Techniken in-

teragieren kann) oder eine beliebige Kombination solcher Back-End, Middleware- oder Front-End-Komponenten beinhaltet. Die Komponenten des Systems können durch eine beliebige Form oder ein beliebiges Medium von digitaler Datenkommunikation (z. B. ein Kommunikationsnetzwerk) miteinander verbunden sein. Beispiele von Kommunikationsnetzen beinhalten ein lokales Netz („LAN“), ein Weitverkehrsnetz („WAN“), Peer-to-Peer-Netze (mit Ad-hoc-Mitgliedern und ständigen Mitgliedern), Netzrechnerinfrastrukturen und das Internet.

[0172] Das Rechensystem kann Client und Server beinhalten. Ein Client und Server befinden sich im Allgemeinen ortsfern voneinander und interagieren typischerweise über ein Kommunikationsnetz. Die Beziehung zwischen Client und Server entsteht aufgrund von Computerprogrammen, die auf den jeweiligen Computern laufen und die eine Client-Server-Beziehung zueinander haben.

[0173] Obwohl vorstehend mehrere Implementierungen detailliert beschrieben wurden, sind andere Modifikationen möglich. Darüber hinaus können andere Systeme und Verfahren zur Ausführung der in diesem Dokument beschriebenen Systeme und Verfahren zur Anwendung kommen. Darüber hinaus erfordern die logischen Abläufe in den Abbildungen nicht die abgebildete Reihenfolge oder die sequenzielle Reihenfolge, um die gewünschten Resultate zu erzielen. Es können weitere Schritte zu den beschriebenen Abläufen hinzugefügt oder aus diesen weggelassen werden, und andere Komponenten können zu den beschriebenen Systemen hinzugefügt oder von diesen weggelassen werden. Dementsprechend liegen andere Implementierungen im Geltungsbereich der folgenden Ansprüche.

Schutzansprüche

1. Computergerät konfiguriert zum:
Identifizieren, dass ein Anwendungsprogramm, das auf dem Computergerät installiert ist, einem Profil für eine Organisationen zugeordnet ist;
Identifizieren, dass das Profil für die Organisation einen Sicherheitscode erfordert, um einen Zugriff auf das Anwendungsprogramm zu ermöglichen;
infolge der durchgeführten Identifikation, dass das Profil der Organisation den Sicherheitscode benötigt, um einen Zugriff auf das Anwendungsprogramm zu ermöglichen, Bereitstellen einer Benutzerschnittstelle, mithilfe der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät separate Sicherheitscodes verwenden sollte, um das Computergerät zu entsperren und einen Zugriff auf das Anwendungsprogramm bereitzustellen;
infolge des Bereitstellens der Benutzerschnittstelle Erhalten einer ersten Benutzereingabe, die spezifiziert, dass das Computergerät einen einzelnen Sicherheitscode verwenden muss, um sowohl das Computergerät zu entsperren als auch um einen Zugriff auf das Anwendungsprogramm bereitzustellen;
nachdem die erste Benutzereingabe spezifiziert hat, dass das Computergerät einen einzelnen Sicherheitscode verwenden muss und während das Computergerät gesperrt ist, Erhalten einer zweiten Benutzereingabe, die den einzelnen Sicherheitscode spezifiziert, um sowohl das Computergerät zu entsperren als auch um einen Zugriff auf das Anwendungsprogramm bereitzustellen und infolgedessen dazu führt, dass das Computergerät entsperrt wird; und
nachdem das Computergerät entsperrt worden ist, Erhalten einer Benutzereingabe, welche ein Benutzerschnittstellenelement auswählt, um das Anwendungsprogramm zu aktivieren und infolgedessen das Anwendungsprogramm aktiviert, ohne zu erfordern, dass ein Sicherheitscode über die Benutzereingabe bereitgestellt wird.

2. Computergerät nach Anspruch 1, ferner konfiguriert zum:
Identifizieren, dass eine Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren und auf das Anwendungsprogramm zuzugreifen;
während das Computergerät gesperrt ist und während die Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren und einen Zugriff auf das Anwendungsprogramm bereitzustellen, Bereitstellen einer ersten Entsperrungsbenutzerschnittstelle;
Erhalten einer dritten Benutzereingabe über die erste Entsperrungsbenutzerschnittstelle, die einen Entsperrungssicherheitscode für das Computergerät spezifiziert und infolgedessen das Computergerät entsperrt;
während das Computergerät entsperrt wird, Erhalten einer vierten Benutzereingabe, die das Benutzerschnittstellenelement auswählt, um das Anwendungsprogramm zu aktivieren;
als Reaktion auf die vierte Benutzereingabe, die eine Präsentation der Benutzerschnittstelle für das Anwendungsprogramm anfordert, Bereitstellen einer zweiten Entsperrungsbenutzerschnittstelle;
Erhalten einer fünften Benutzereingabe über die zweite Benutzerschnittstelle, die einen Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen; und
Aktivieren des Anwendungsprogramms als Reaktion auf das Erhalten der fünften Benutzereingabe, die den Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen.

3. Computergerät nach Anspruch 2, wobei:
Erhalten der dritten Benutzereingabe, welche den Entsperrungssicherheitscode für das Computergerät, das die dritte Benutzereingabe erhält, welche den Entsperrungssicherheitscode für das Computergerät

spezifiziert, der die ersten Auflagen des Sicherheitscodes erfüllt; und Erha
lten der fünften Benutzereingabe, welche einen Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, umfasst das Erhalten der fünften Benutzereingabe, welche einen Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, das die zweiten Auflagen des Sicherheitscodes erfüllt, die im Profil für die Organisation spezifiziert sind, wobei die zweiten Auflagen des Sicherheitscodes sich von den ersten Auflagen des Sicherheitscodes unterscheiden.

4. Computergerät nach Anspruch 2 oder 3, ferner konfiguriert zum:
Erhalten einer sechsten Benutzereingabe, welche einen neuen Organisationssicherheitscode spezifiziert; das Bereitstellen, unter Verwendung der sechsten Benutzereingabe, ob der neue Organisationssicherheitscode die Auflagen des Sicherheitscodes erfüllt, die im Profil für die Organisation definiert werden; und Bereitstellen, als Reaktion auf das Ermitteln, dass der neue Organisationssicherheitscode den Auflagen des Sicherheitscodes entspricht, die im Profil der Organisation definiert werden, der Benutzerschnittstelle, mit der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät separate Sicherheitscodes verwenden sollte, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen.

5. Computergerät nach den Ansprüchen 2 bis 4, ferner konfiguriert zum:
Bereitstellen, als Reaktion auf das Erhalten der fünften Benutzereingabe, welche den Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, des Zugriffs auf das Anwendungsprogramm und alle Anwendungsprogramme, die dem Profil für die Organisation zugeordnet werden, einschließlich mindestens eines anderen Anwendungsprogramms, das dem Profil für die Organisation zugeordnet worden ist.

6. Computergerät nach den Ansprüchen 2 bis 5, ferner konfiguriert zum:
Ermitteln, während die Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren, und um einen Zugriff auf das Anwendungsprogramm bereitzustellen und als Reaktion auf das Erhalten der dritten Benutzereingabe, welche den Entsperrungssicherheitscode für das Computergerät spezifiziert, dass das Computergerät separate Sicherheitscodes verwendet, um das Computergerät zu entsperren und um Zugriff auf das Anwendungsprogramm bereitzustellen; und
bis zum Erhalt der Benutzereingabe, welche den Organisationssicherheitscode spezifiziert, Verhindern des Zugriffs auf alle Anwendungsprogramme, die dem Profil für die Organisation einschließlich des Anwendungsprogramms zugeordnet sind.

7. Computergerät nach einem der Ansprüche 2 bis 6, wobei Bereitstellen der zweiten Entsperrungsbenutzerschnittstelle als Antwort auf die vierte Benutzereingabe, die eine Präsentation der Benutzerschnittstelle für das Anwendungsprogramm anfordert, Bereitstellen der zweiten Benutzerschnittstelle, die sich von der ersten Entsperrungsbenutzerschnittstelle unterscheidet, umfasst, welches, als Antwort auf die vierte Benutzereingabe, die eine Präsentation der Benutzerschnittstelle für das Anwendungsprogramm erfordert, durchgeführt wird.

8. Computergerät nach Anspruch 7, wobei Bereitstellen der zweiten Entsperrungsbenutzerschnittstelle, als Antwort auf die vierte Benutzereingabe, welche eine Präsentation der Benutzerschnittstelle für das Anwendungsprogramm anfordert, die sich von der Benutzerschnittstelle der ersten Entsperrungsbenutzerschnittstelle unterscheidet, Bereitstellen einer zweiten Benutzerschnittstelle mit einem sich darin befindlichen Bild umfasst, das von der Organisation oder einem Administrator dieser spezifiziert ist.

9. Computergerät nach irgendeinem der vorherigen Ansprüche, ferner konfiguriert zum:
Empfangen von Anweisungen, um den Zugriff auf das Anwendungsprogramm und auf sonstige andere Anwendungsprogramme, die dem Profil der Organisation zugeordnet sind, zu verhindern, wobei die Anweisungen, als Reaktion auf eine zuvor definierte Menge erfolgloser Versuche, einen Sicherheitscode für den Zugriff auf das Anwendungsprogramm einzugeben ist, oder als Reaktion auf eine Eingabe des Administrators, um einen Zugriff auf das Anwendungsprogramm zu verhindern, erhalten werden; und
Verhindern der Präsentation einer Benutzerschnittstelle für das Anwendungsprogramm als Reaktion auf das Erhalten der Anweisungen, um den Zugriff auf das Anwendungsprogramm und auf sonstige andere Anwendungsprogramme zu verhindern, die dem Profil der Organisation zugeordnet worden sind.

10. Computergerät nach Anspruch 9, ferner konfiguriert zum:
Erhalten einer weiteren Benutzereingabe, welche einen Zugriff auf das Anwendungsprogramm anfordert, nachdem Anweisungen erhalten worden sind, welche einen Zugriff auf das Anwendungsprogramm oder sonstige Anwendungsprogramme verhindern, die dem Profil für die Organisation zugeordnet sind; und
Ermitteln, als Reaktion auf die weitere Benutzereingabe, welche einen Zugriff auf das Anwendungsprogramm anfordert,, dass kein Zugriff auf das Anwendungsprogramm bereitgestellt werden soll.

11. Computergerät nach Anspruch 1, ferner konfiguriert zum:
Identifizieren, dass eine Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren und um auf das Anwendungsprogramm zuzugreifen;
Erhalten einer ersten E-Mail-Nachricht für ein erstes E-Mail-Konto, das nicht von der Organisation verwaltet wird, während das Computergerät gesperrt ist und während die Einstellung des Computergeräts spezifiziert, dass das Computergerät separate Sicherheitscodes verwenden muss, um das Computergerät zu entsperren und um auf das Anwendungsprogramm zuzugreifen;
Bereitstellen von Informationen über die erste E-Mail-Nachricht in einer gesperrten Benutzerschnittstelle für das Computergerät, während das Computergerät gesperrt ist;
Empfangen einer zweiten E-Mail-Nachricht für ein zweites E-Mail-Konto, das von der Organisation verwaltet wird, während das Computergerät gesperrt ist und über separate Sicherheitscodes verfügt, um das Computergerät zu entsperren und während ein Zugriff auf das Anwendungsprogramm bereitgestellt wird; und
Ermitteln, dass keine Informationen über die zweite E-Mail-Nachricht in der gesperrten Benutzerschnittstelle für das Computergerät bereitgestellt werden sollen, während das Computergerät gesperrt ist und das Profil für die Organisation verwendet wird.

12. Computergerät nach irgendeinem der vorherigen Ansprüche, ferner konfiguriert zum:
Bestimmen, dass die Hardware des Computergeräts das Verwenden separater Sicherheitscodes für das Entsperren des Computergeräts und das Bereitstellen des Zugriffs auf das Anwendungsprogramm ermöglicht, wobei das Bereitstellen der Benutzerschnittstelle mit der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät separate Sicherheitscodes verwenden sollte, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm in Reaktion auf das Ermitteln bereitzustellen, dass die Hardware des Computergeräts das Verwenden separater Sicherheitscodes ermöglicht, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen.

13. Computergerät nach Anspruch 12, wobei das Bestimmen, dass die Hardware des Computergeräts das Verwenden separater Sicherheitscodes ermöglicht, um das Computergerät zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen, das Ermitteln umfasst, dass das Computergerät das dateibasierte Verschlüsseln ermöglicht.

14. Computergerät nach irgendeinem der vorherigen Ansprüche, ferner konfiguriert zum:
Ermitteln, als Reaktion auf das Erhalten der zweiten Benutzereingabe, welche den einzelnen Sicherheitscode spezifiziert, dass die zweite Benutzereingabe den einzelnen Sicherheitscode spezifiziert; und
Bereitstellen, des Zugriffs auf das Anwendungsprogramm und eine zusätzliche Anwendung ohne dass ein zusätzlicher Sicherheitscode erfordert wird, als Reaktion auf das Ermitteln, dass die zweite Benutzereingabe den einzelnen Sicherheitscode spezifiziert, wobei es sich bei dem zusätzlichen Programm um ein Programm handelt, das nicht dem Profil der Organisation zugeordnet worden ist, und auf das zugegriffen werden kann, wenn das Computergerät gesperrt ist.

15. System, umfassend:
ein oder mehrere computerlesbare Geräte, die über darauf gespeicherte Anweisungen verfügen, die wenn sie von einem oder mehreren Prozessoren ausgeführt werden, einen oder mehrere Prozessoren dazu veranlassen, Operationen auszuführen, die Folgendes umfassen:
Identifizieren, dass ein Anwendungsprogramm, das auf dem System installiert ist, einem Profil für eine Organisation zugeordnet ist;
Identifizieren, dass das Profil für die Organisation einen Sicherheitscode erfordert, um einen Zugriff auf das Anwendungsprogramm zuzulassen;
infolge des Identifizierens, dass das Profil für die Organisation den Sicherheitscode erfordert, um einen Zugriff auf das Anwendungsprogramm zuzulassen, das Bereitstellen einer Benutzerschnittstelle, mit der die Benutzereingabe in der Lage ist zu spezifizieren, ob das System separate Sicherheitscodes verwenden sollte, um das System zu entsperren und einen Zugriff auf das Anwendungsprogramm bereitzustellen;
infolge des Bereitstellens der Benutzerschnittstelle das Erhalten einer ersten Benutzereingabe, welche spezifiziert, dass das System einen einzelnen Sicherheitscode verwenden muss, um sowohl das System zu entsperren als auch einen Zugriff auf das Anwendungsprogramm bereitzustellen;
nachdem die erste Benutzereingabe spezifiziert hat, dass das System einen einzelnen Sicherheitscode verwenden sollte und während das System gesperrt ist, Empfangen einer zweiten Benutzereingabe, die den einzelnen Sicherheitscodes spezifiziert, um sowohl das System zu entsperren, als auch um einen Zugriff auf das Anwendungsprogramm bereitzustellen und infolgedessen das System zu entsperren;
nachdem das System gesperrt worden ist, Erhalten einer Benutzereingabe, die ein Benutzerschnittstellenelement auswählt, um das Anwendungsprogramm zu aktivieren, und infolgedessen das Aktivieren eines Anwendungsprogramms ohne anzufordern, dass die Benutzereingabe einen Sicherheitscode bereitstellt.

16. System nach Anspruch 15, wobei die Operationen Folgendes umfassen:

Identifizieren, dass eine Einstellung des Systems spezifiziert, dass das System separate Sicherheitscodes verwenden muss, um das System zu entsperren und auf das Anwendungsprogramm zuzugreifen;
während das System gesperrt ist und während die Einstellung des Systems spezifiziert, dass das System separate Sicherheitscodes verwenden muss, um das System zu entsperren und einen Zugriff auf das Anwendungsprogramm bereitzustellen, Bereitstellen einer ersten Entsperrungsbenutzerschnittstelle;
das von einer ersten Entsperrungsbenutzerschnittstelle durchgeführte Erhalten einer dritten Benutzereingabe, die einen Entsperrungssicherheitscode Entsperungssicherheitscode für das System spezifiziert und infolgedessen das System entsperrt;
während das System entsperrt wird, Erhalten einer vierten Benutzereingabe, die das Benutzerschnittstellenelement auswählt, um das Anwendungsprogramm zu aktivieren;
als Reaktion auf die vierte Benutzereingabe, die eine Präsentation der Benutzerschnittstelle für das Anwendungsprogramm anfordert, Bereitstellen einer zweiten Entsperrungsbenutzerschnittstelle;
durch die zweite Entsperrungsbenutzerschnittstelle, Erhalten einer fünften Benutzereingabe, welche einen Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen; und
Aktivieren des Anwendungsprogramms in Reaktion auf das Erhalten der fünften Benutzereingabe, die den Organisationssicherheitscode Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen.

17. System nach Anspruch 16, wobei:
Erhalten einer dritten Benutzereingabe, welche den Sicherheitscode für das Entsperren des Systems das Erhalten der dritten Benutzereingabe umfasst, welche den Sicherheitscode für das Entsperren des Systems spezifiziert, der die ersten Auflagen des Sicherheitscodes erfüllt; und
Erhalten der fünften Benutzereingabe, welche einen Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, umfasst das Erhalten der fünften Benutzereingabe, welche einen Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen, der die zweiten Auflagen des Sicherheitscodes erfüllt, die im Profil für die Organisation spezifiziert sind, wobei sich die zweiten Auflagen des Sicherheitscodes von den ersten Auflagen des Sicherheitscodes unterscheiden.

18. System nach Anspruch 16 oder 17, wobei die Operationen Folgendes umfassen:
Erhalten einer sechsten Benutzereingabe, welche einen neuen Organisationssicherheitscode spezifiziert;
Ermitteln unter Verwendung der sechsten Benutzereingabe, ob der neue Organisationssicherheitscode die Auflagen des Sicherheitscodes erfüllt, die im Profil für die Organisation definiert werden; und
Organisationssicherheitscode Bereitstellen der Benutzerschnittstelle, mit der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das System separate Sicherheitscodes verwenden sollte, um das System zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen als Reaktion auf das Ermitteln, dass der neue Organisationssicherheitscode den Auflagen des Sicherheitscodes entspricht, die im Profil der Organisation definiert werden.

19. System nach Anspruch 16, 17 oder 18, wobei die Operationen Folgendes umfassen:
Bereitstellen des Zugriffs auf das Anwendungsprogramm und alle Anwendungsprogramme, die dem Profil für die Organisation zugeordnet werden, einschließlich mindestens eines anderen Anwendungsprogramms, das dem Profil für die Organisation zugeordnet worden ist, als Reaktion auf das Erhalten der fünften Benutzereingabe, welche den Organisationssicherheitscode spezifiziert, der verwendet wird, um auf das Anwendungsprogramm zuzugreifen.

20. System nach einem der Ansprüche 16 bis 19, wobei die Operationen Folgendes umfassen:
Bestimmen, während der Einstellung des Systems, dass das System separate Sicherheitscodes verwenden muss, um das System zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen und als Reaktion auf das Erhalten der dritten Benutzereingabe, den Entsperungssicherheitscode für das System spezifiziert, das Ermitteln, dass das System separate Sicherheitscodes verwendet, um das System zu entsperren und um einen Zugriff auf das Anwendungsprogramm bereitzustellen; und
Verhindern, bis zum Erhalten der Benutzereingabe, die den Organisationssicherheitscode spezifiziert, des Zugriffs auf alle Anwendungsprogramme, die dem Profil für die Organisation, einschließlich des Anwendungsprogramms zugeordnet sind.

Es folgen 10 Seiten Zeichnungen

Anhängende Zeichnungen

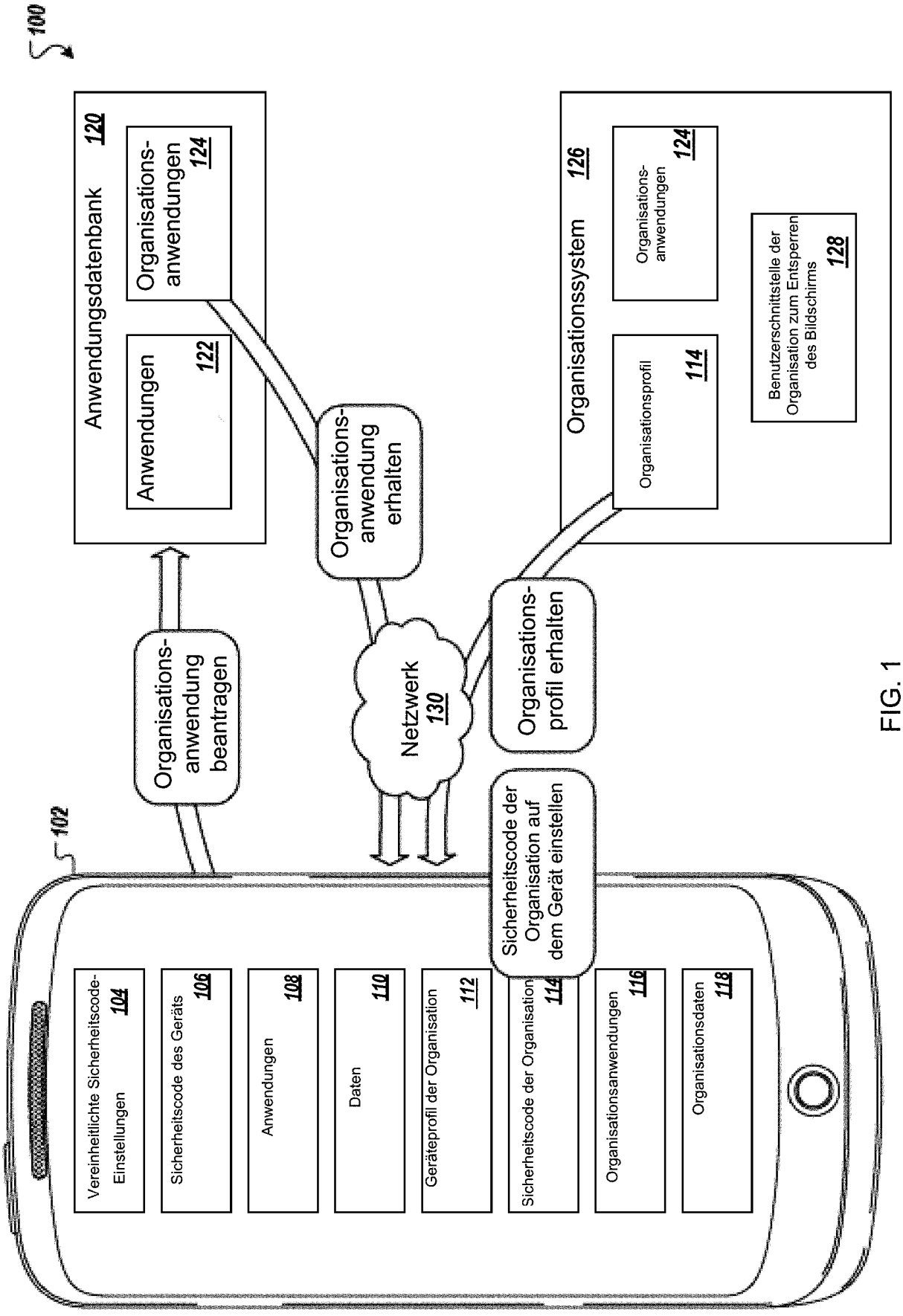


FIG. 1

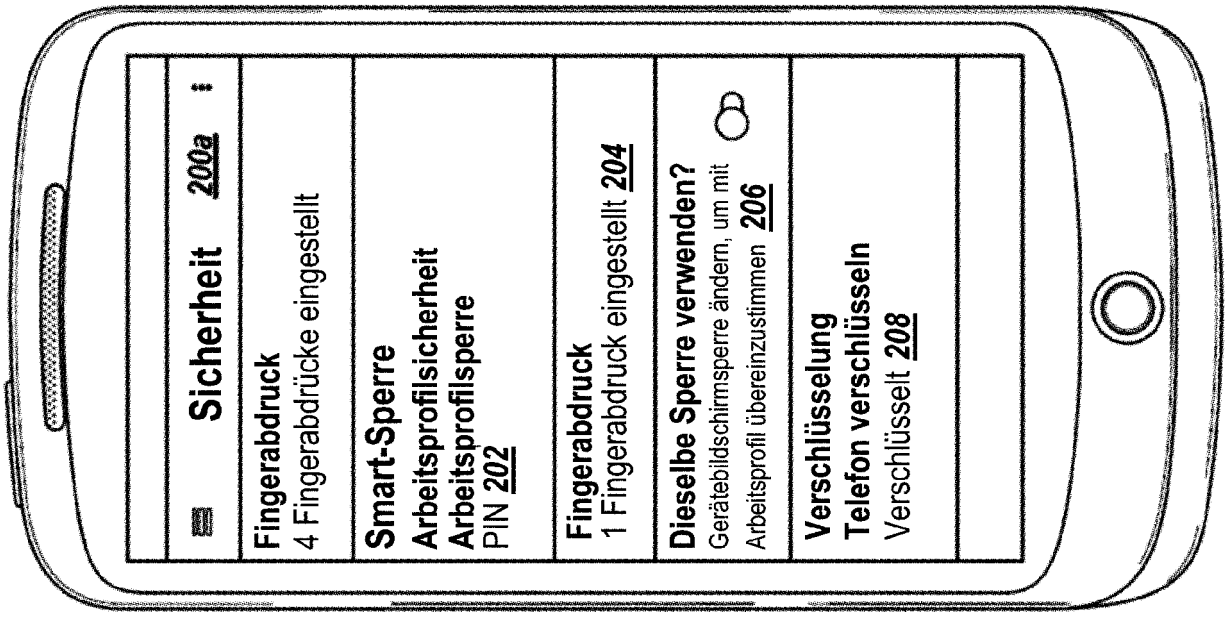

Sicherheit 200a
Fingerabdruck
4 Fingerabdrücke eingestellt
Smart-Sperre
Arbeitsprofilsicherheit
Arbeitsprofilsperre
PIN 202
Fingerabdruck
1 Fingerabdruck eingestellt 204
Dieselbe Sperre verwenden?
Gerätebildschirmsperre ändern, um mit Arbeitsprofil übereinzustimmen 206
Verschlüsselung
Telefon verschlüsseln
Verschlüsselt 208

FIG. 2A

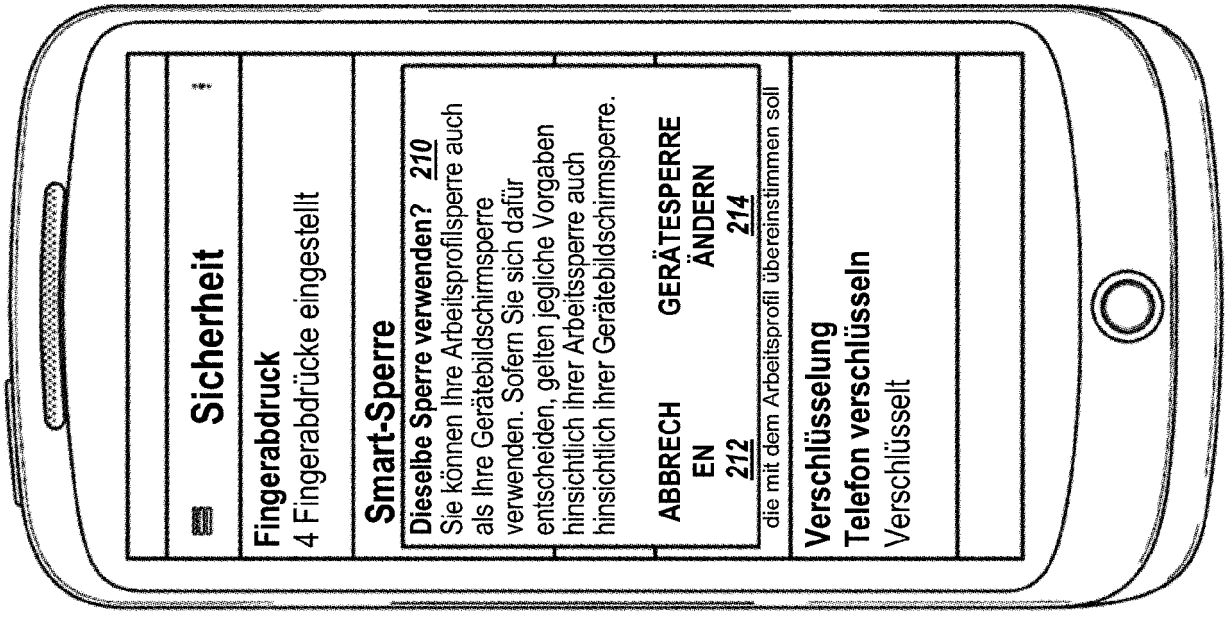

Sicherheit
Fingerabdruck
4 Fingerabdrücke eingestellt
Smart-Sperre
Dieselbe Sperre verwenden? 210
Sie können Ihre Arbeitsprofilsperre auch als Ihre Gerätebildschirmsperre verwenden. Sofern Sie sich dafür entscheiden, gelten jegliche Vorgaben hinsichtlich ihrer Arbeitssperre auch hinsichtlich ihrer Gerätebildschirmsperre.
ABBRECHEN 212
GERÄTESPERRE ÄNDERN 214
die mit dem Arbeitsprofil übereinstimmen soll
Verschlüsselung
Telefon verschlüsseln
Verschlüsselt

FIG. 2B

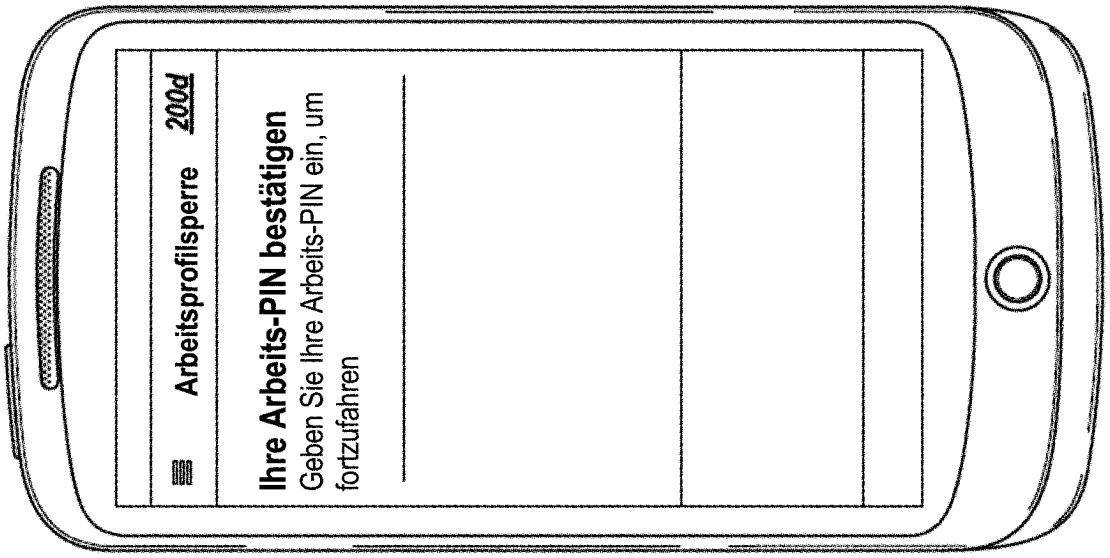

Arbeitsprofilsperre
200d
Ihre Arbeits-PIN bestätigen
Geben Sie Ihre Arbeits-PIN ein, um fortzufahren

FIG. 2D

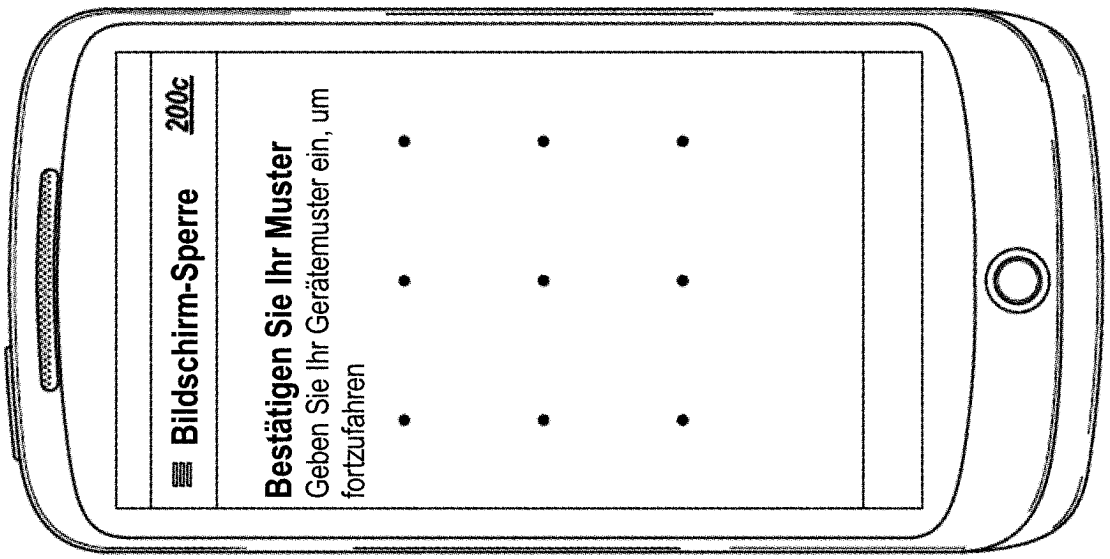

Bildschirm-Sperre
200c
Bestätigen Sie Ihr Muster
Geben Sie Ihr Gerätemuster ein, um fortzufahren

FIG. 2C

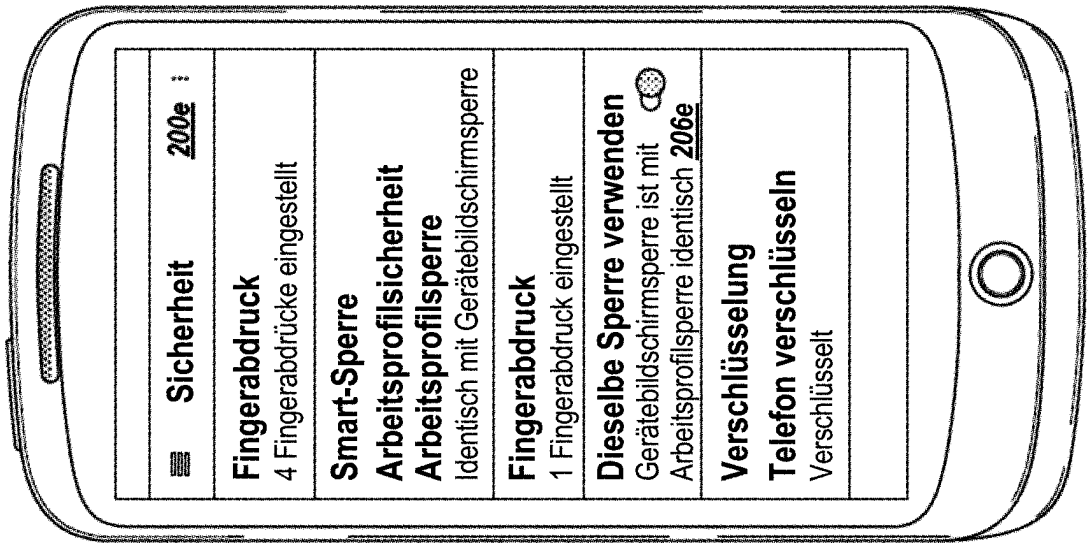

Sicherheit
200e
Fingerabdruck
4 Fingerabdrücke eingestellt
Smart-Sperre
Arbeitsprofilsicherheit
Arbeitsprofilsperre
Identisch mit Gerätebildschirmsperre
Fingerabdruck
1 Fingerabdruck eingestellt
Dieselbe Sperre verwenden
Gerätebildschirmsperre ist mit
Arbeitsprofilsperre identisch 206e
Verschlüsselung
Telefon verschlüsseln
Verschlüsselt

FIG. 2E


Sicherheit
300
Gerätesicherheit
Bildschirm-Sperre
Muster 302a
Sichtbarmachen des Musters 304
Automatische Sperre
30 Sekunden nach Übergang in den Ruhezustand, außer, wenn durch Smart-Sperre entsperrt gehalten
Einschaltknopf wird augenblicklich gesperrt
Außer, wenn durch Smart-Sperre entsperrt gehalten
Nachricht auf Bildschirm mit Sperrfunktion
Keine
Fingerabdruck
4 Fingerabdrücke eingestellt
Smart-Sperre
Arbeitsprofilsicherheit
Bildschirm-Sperre
Muster 302b
Option zum Sichtbarmachen des Musters
Fingerabdruck
1 Fingerabdruck eingestellt 204
Dieselbe Sperre verwenden?
Gerätebildschirmsperre ändern, um mit Arbeitsbildschirmsperre übereinzustimmen? 206
Verschlüsselung
Telefon verschlüsseln
Verschlüsselt 208

FIG. 3

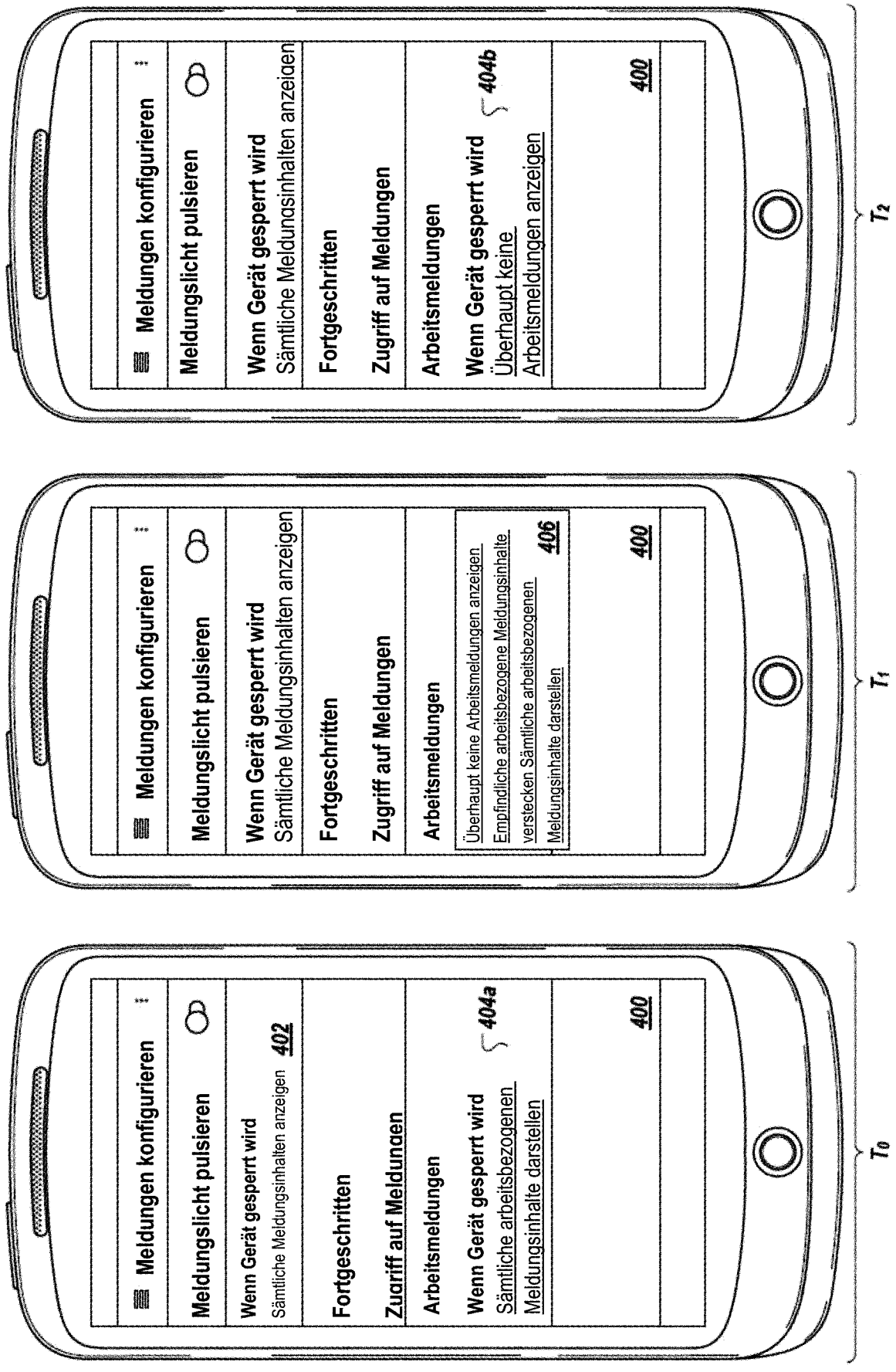

Meldungen konfigurieren
Meldungslicht pulsieren
Wenn Gerät gesperrt wird
Sämtliche Meldungsinhalten anzeigen 402
Fortgeschritten
Zugriff auf Meldungen
Arbeitsmeldungen
Wenn Gerät gesperrt wird
Sämtliche arbeitsbezogenen Meldungsinhalte darstellen 404a
400
T0
Meldungen konfigurieren
Meldungslicht pulsieren
Wenn Gerät gesperrt wird
Sämtliche Meldungsinhalten anzeigen
Fortgeschritten
Zugriff auf Meldungen
Arbeitsmeldungen
Überhaupt keine Empfindliche arbeitsbezogene Meldungsinhalte verstecken Sämtliche arbeitsbezogenen Meldungsinhalte darstellen 406
400
T1
Meldungen konfigurieren
Meldungslicht pulsieren
Wenn Gerät gesperrt wird
Sämtliche Meldungsinhalten anzeigen
Fortgeschritten
Zugriff auf Meldungen
Arbeitsmeldungen
Wenn Gerät gesperrt wird
Überhaupt keine Arbeitsmeldungen anzeigen 404b
400
T2

FIG. 4

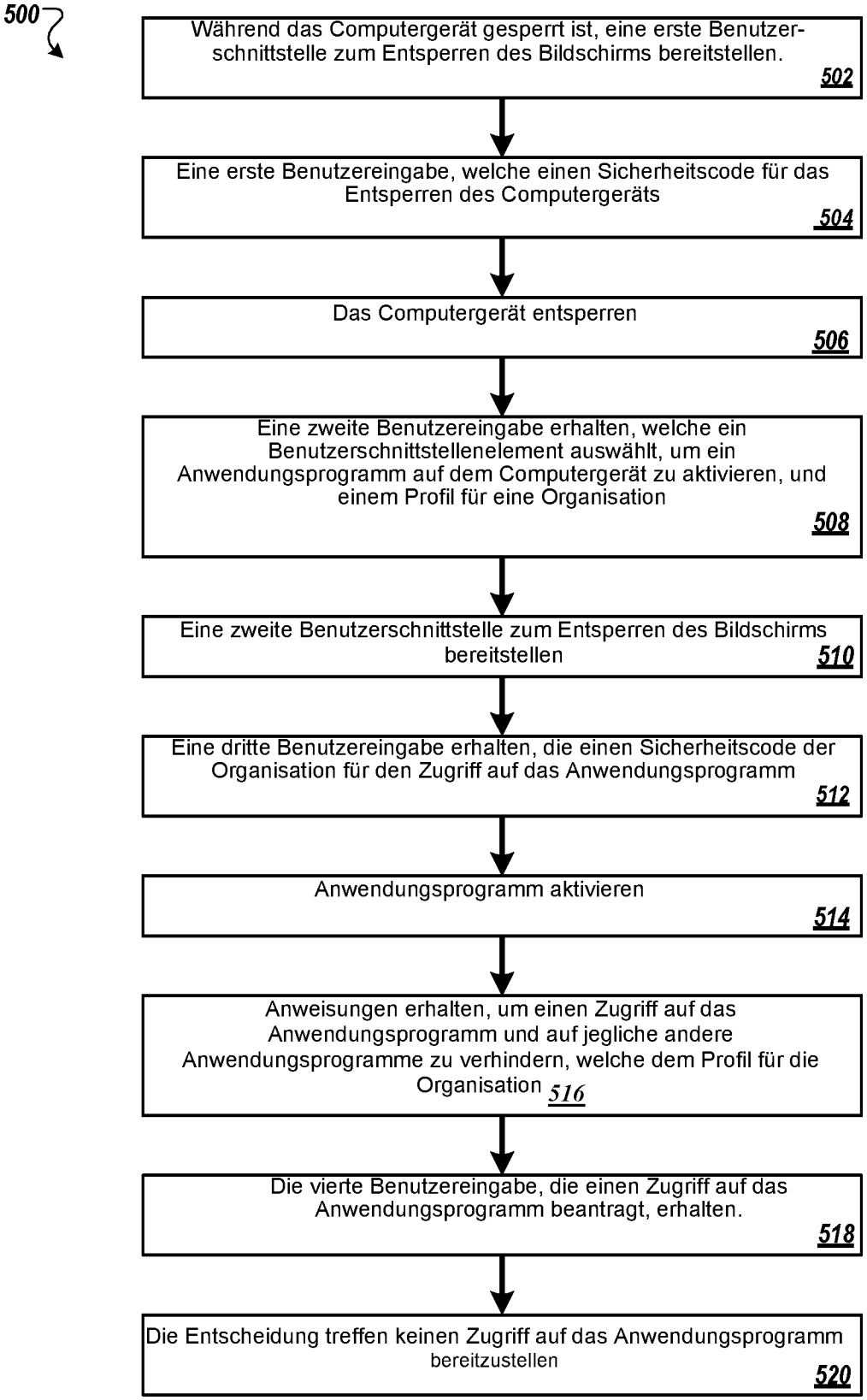

500
Während das Computergerät gesperrt ist, eine erste Benutzerschnittstelle zum Entsperren des Bildschirms bereitstellen. 502
Eine erste Benutzereingabe, welche einen Sicherheitscode für das Entsperren des Computergeräts 504
Das Computergerät entsperren 506
Eine zweite Benutzereingabe erhalten, welche ein Benutzerschnittstellenelement auswählt, um ein Anwendungsprogramm auf dem Computergerät zu aktivieren, und einem Profil für eine Organisation 508
Eine zweite Benutzerschnittstelle zum Entsperren des Bildschirms bereitstellen 510
Eine dritte Benutzereingabe erhalten, die einen Sicherheitscode der Organisation für den Zugriff auf das Anwendungsprogramm 512
Anwendungsprogramm aktivieren 514
Anweisungen erhalten, um einen Zugriff auf das Anwendungsprogramm und auf jegliche andere Anwendungsprogramme zu verhindern, welche dem Profil für die Organisation 516
Die vierte Benutzereingabe, die einen Zugriff auf das Anwendungsprogramm beantragt, erhalten. 518
Die Entscheidung treffen keinen Zugriff auf das Anwendungsprogramm bereitzustellen 520

FIG. 5

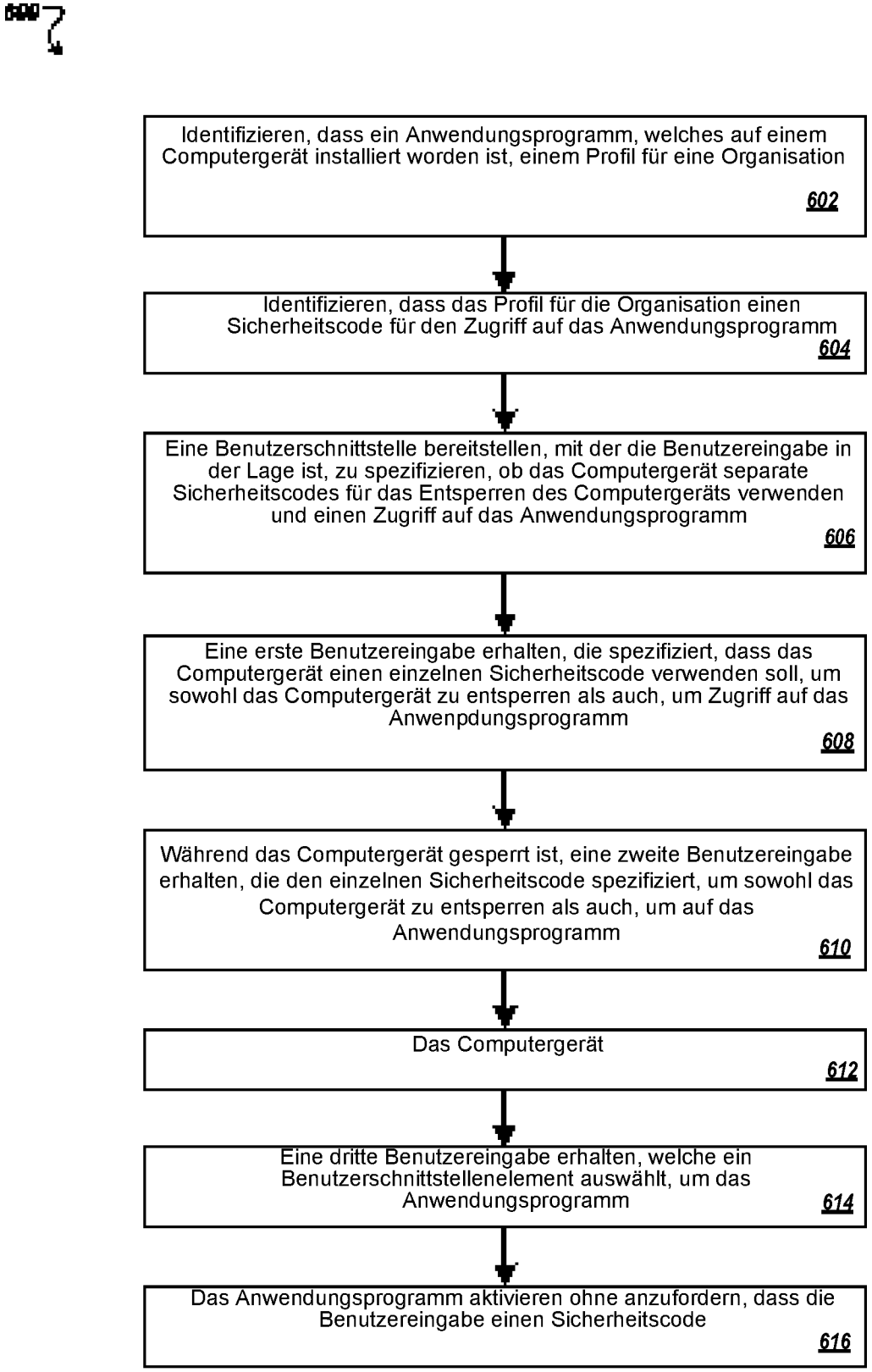

600
Identifizieren, dass ein Anwendungsprogramm, welches auf einem Computergerät installiert worden ist, einem Profil für eine Organisation
602
Identifizieren, dass das Profil für die Organisation einen Sicherheitscode für den Zugriff auf das Anwendungsprogramm
604
Eine Benutzerschnittstelle bereitstellen, mit der die Benutzereingabe in der Lage ist, zu spezifizieren, ob das Computergerät separate Sicherheitscodes für das Entsperren des Computergeräts verwenden und einen Zugriff auf das Anwendungsprogramm
606
Eine erste Benutzereingabe erhalten, die spezifiziert, dass das Computergerät einen einzelnen Sicherheitscode verwenden soll, um sowohl das Computergerät zu entsperren als auch, um Zugriff auf das Anwenpdungsprogramm
608
Während das Computergerät gesperrt ist, eine zweite Benutzereingabe erhalten, die den einzelnen Sicherheitscode spezifiziert, um sowohl das Computergerät zu entsperren als auch, um auf das Anwendungsprogramm
610
Das Computergerät
612
Eine dritte Benutzereingabe erhalten, welche ein Benutzerschnittstellenelement auswählt, um das Anwendungsprogramm
614
Das Anwendungsprogramm aktivieren ohne anzufordern, dass die Benutzereingabe einen Sicherheitscode
616

FIG. 6

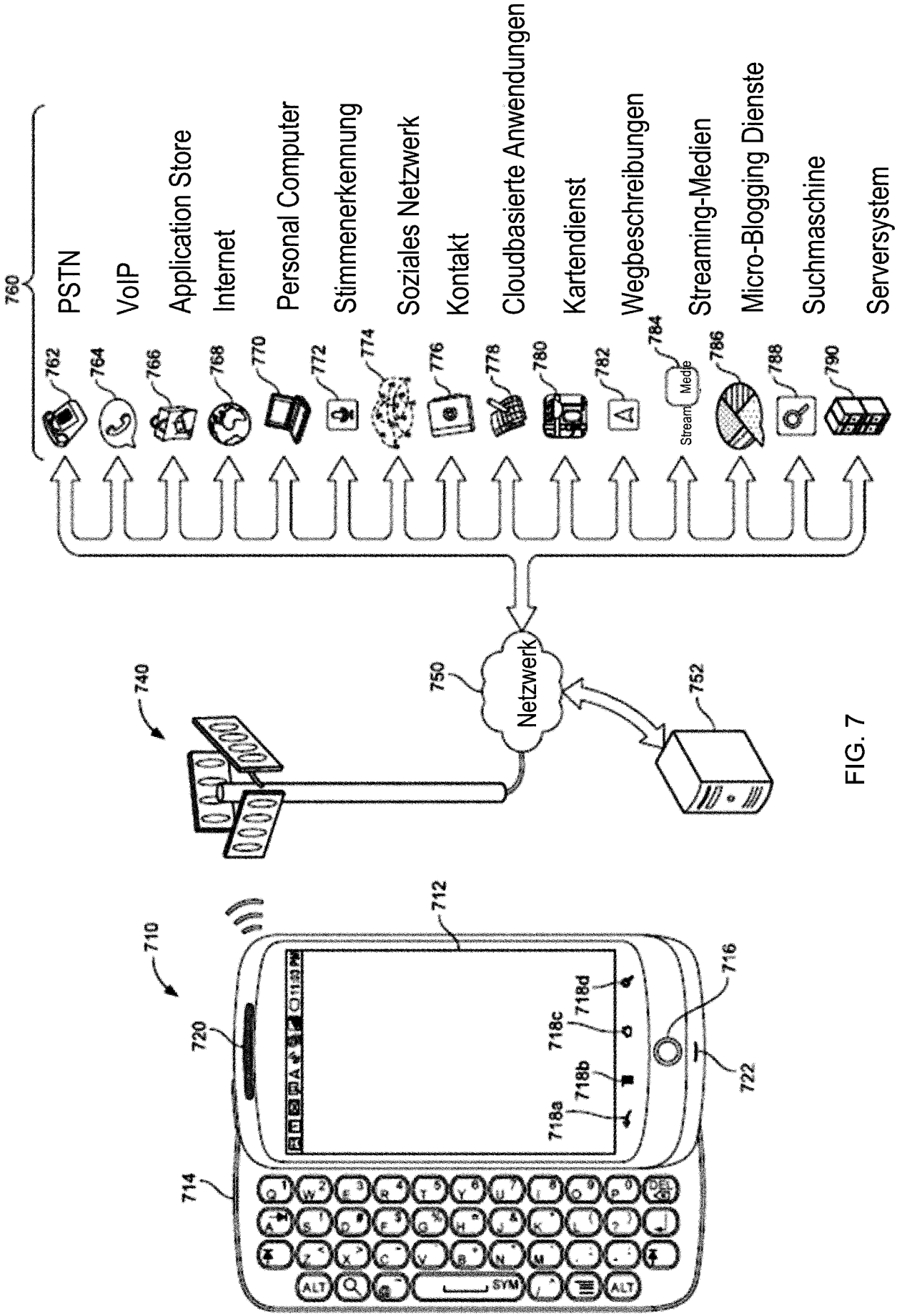

760
PSTN
VoIP
Application Store
Internet
Personal Computer
Stimmenerkennung
Soziales Netzwerk
Kontakt
Cloudbasierte Anwendungen
Kartendienst
Wegbeschreibungen
Streaming-Medien
Micro-Blogging Dienste
Suchmaschine
Serversystem
762
764
766
768
770
772
774
776
778
780
782
784
786
788
790
Stream
Medie
740
750
Netzwerk
752
710
712
714
716
718a
718b
718c
718d
720
722

FIG. 7

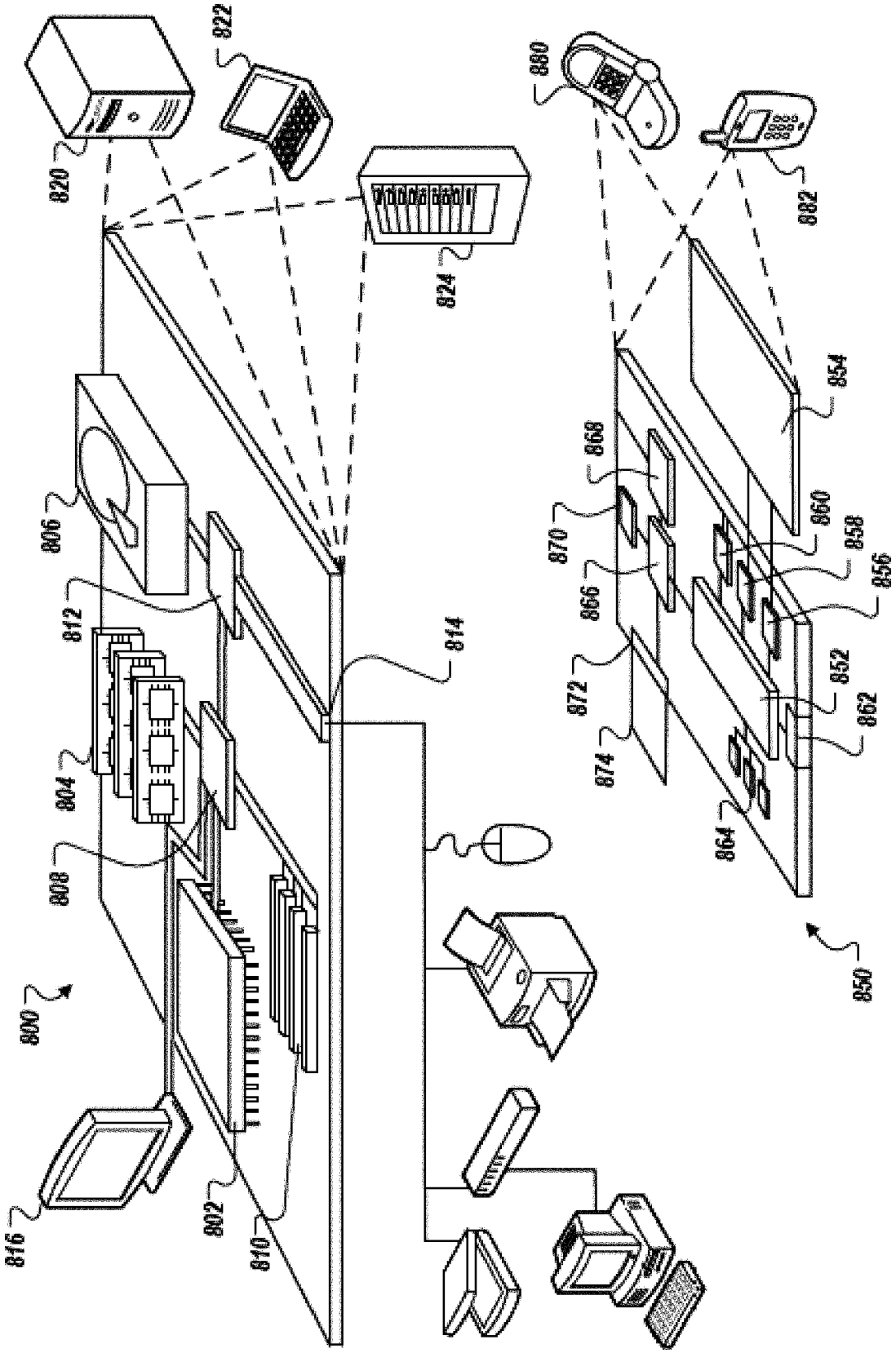

800
802
804
806
808
810
812
814
816
820
822
824
850
852
854
856
858
860
862
864
866
868
870
872
874
880
882

FIG. 8