

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7591343号
(P7591343)

(45)発行日 令和6年11月28日(2024.11.28)

(24)登録日 令和6年11月20日(2024.11.20)

(51)国際特許分類

F I

G 0 6 F 21/60 (2013.01)

G 0 6 F 21/60 3 2 0

G 0 6 Q 20/38 (2012.01)

G 0 6 F 21/60 3 6 0

G 0 6 Q 20/38 3 1 0

請求項の数 15 外国語出願 (全54頁)

(21)出願番号	特願2019-22277(P2019-22277)	(73)特許権者	503260918
(22)出願日	平成31年2月12日(2019.2.12)		アップル インコーポレイテッド
(62)分割の表示	特願2017-115083(P2017-115083)の分割		A p p l e I n c .
原出願日	平成29年6月12日(2017.6.12)		アメリカ合衆国 9 5 0 1 4 カリフォル ニア州 クパチーノ アップル パーク ウ エイ ワン
(65)公開番号	特開2019-106199(P2019-106199 A)		O n e A p p l e P a r k W a y ,
(43)公開日	令和1年6月27日(2019.6.27)		C u p e r t i n o , C a l i f o r
審査請求日	令和2年6月12日(2020.6.12)		n i a 9 5 0 1 4 , U . S . A .
審判番号	不服2023-12773(P2023-12773/J 1)	(74)代理人	100094569
審判請求日	令和5年7月31日(2023.7.31)		弁理士 田中 伸一郎
(31)優先権主張番号	62/349,003	(74)代理人	100103610
(32)優先日	平成28年6月12日(2016.6.12)		弁理士 ▲吉▼田 和彦
(33)優先権主張国・地域又は機関		(74)代理人	100067013
	最終頁に続く		弁理士 大塚 文昭
			最終頁に続く

(54)【発明の名称】 電子デバイスとサービスプロバイダの間のセキュリティ保護された取引の管理

(57)【特許請求の範囲】

【請求項1】

第1のサブシステムにて、
第2のサブシステムからのアイテムに対する注文に対応する注文データを、電子デバイスから受信することであって、前記注文データは資金提供資格データを含み、前記第2のサブシステムは前記第1のサブシステムから隔離されている、前記受信することと、
前記第2のサブシステムに前記注文データの少なくとも一部を送信することと、
前記送信された前記注文データの少なくとも一部に少なくとも部分的に基づいて前記第2のサブシステムから前記アイテムを受信することと、
前記電子デバイスのセキュアエレメント上で提供するために前記アイテムに対応するデータを前記電子デバイスに提供することと、
を含む方法。

【請求項2】

前記アイテムは、前記第2のサブシステムのサービスまたは製品へのアクセスを提供する、請求項1に記載の方法。

【請求項3】

前記第2のサブシステムに前記注文データの少なくとも一部を送信することは、
前記第2のサブシステムと前記第1のサブシステムとの間の共有秘密の少なくとも一部に基づいて前記注文データの少なくとも一部を暗号化することであって、前記共有秘密は、前記アイテムに対応する前記データとは異なる、ことと、

前記暗号化された前記注文データの少なくとも一部を送信することと、を含む、請求項 1 に記載の方法。

【請求項 4】

前記受信されたアイテムは暗号化され、

前記第 2 のサブシステムと前記第 1 のサブシステムとの間の前記共有秘密の少なくとも一部に基づいて前記受信されたアイテムを、前記第 1 のサブシステムにおいて、解読することを更に含む、請求項 3 に記載の方法。

【請求項 5】

前記注文に対応する注文状況データは、前記第 1 のサブシステムと前記第 2 のサブシステムの共有秘密を用いて前記第 1 のサブシステムによって検証される、請求項 1 に記載の方法。

10

【請求項 6】

非一時的なコンピュータ可読媒体に記憶されたコンピュータ可読命令であって、これが実行された場合、電子デバイスに、

当該電子デバイスにより第 1 のサブシステムに向けて、アイテムに対する注文に対応する注文データを送信させるようになっており、この場合、前記アイテムは第 2 のサブシステムからのものであり、かつ該第 2 のサブシステムは前記第 1 のサブシステムから区別されており、及び

前記電子デバイスに、

当該電子デバイスにより、前記第 2 のサブシステムによって前記電子デバイスから前記アイテムに対する前記注文が検証されたことの確認を前記第 2 のサブシステムから受信した前記第 1 のサブシステムに応答して、前記電子デバイス上の前記アイテムに対応するセキュリティドメインにおいて前記電子デバイスによって提供されるデータを前記第 1 のサブシステムから受信させるようにする、のに有効なコンピュータ可読命令、を備える非一時的なコンピュータ可読媒体。

20

【請求項 7】

前記第 1 のサブシステムは第 2 のサブシステムから隔離されている、請求項 6 に記載の非一時的なコンピュータ可読媒体。

【請求項 8】

前記データはアプレットを含み、前記アプレットは前記電子デバイスに提供された記憶された値に対応する、請求項 6 に記載の非一時的なコンピュータ可読媒体。

30

【請求項 9】

前記データはアプレットを含み、前記アプレットは前記電子デバイスに前記第 2 のサブシステムの製品へのアクセスを提供する、請求項 8 に記載の非一時的なコンピュータ可読媒体。

【請求項 10】

前記注文に対応する注文状況データは前記第 1 のサブシステムと前記第 2 のサブシステムの共有秘密を用いて前記第 1 のサブシステムによって検証される、請求項 6 に記載の非一時的なコンピュータ可読媒体。

【請求項 11】

40

メモリと、

第 2 のサブシステムによって、注文に対応する第 1 のサブシステムからの注文データを受信することであって、前記注文は第 2 のサブシステムのアイテムのための電子デバイスからのものであり、かつ前記注文データは資金提供資格データを含むものである、前記受信することと、

前記第 2 のサブシステムによって、前記注文データの受信に応答して、前記資金提供資格データを第 3 のサブシステムに送信して前記注文を有効化することと、及び

前記第 3 のサブシステムにより前記注文が有効化されたという確認を前記第 3 のサブシステムから前記第 2 のサブシステムが受信したことに応答して、前記アイテムを、前記電子デバイスのセキュアエレメントにおいて提供するために、前記第 2 のサブシステムによ

50

って前記第1のサブシステムに送信することを含む、ように構成されている少なくとも1つのプロセッサを備えた第2のサブシステム。

【請求項12】

前記受信された注文データは前記第2のサブシステムと前記第1のサブシステムとの間の共有秘密の少なくとも一部に基づいて暗号化され、かつ前記少なくとも1つのプロセッサは、更に前記共有秘密の少なくとも一部に基づいた前記注文データを解読するように構成されている、請求項11に記載の第2のサブシステム。

【請求項13】

前記少なくとも1つのプロセッサは、更に、前記アイテムの前記第1のサブシステムへの送信の前に前記共有秘密の少なくとも一部に基づいて前記アイテムを暗号化するように構成されている、請求項12に記載の第2のサブシステム。

10

【請求項14】

前記共有秘密は前記注文データを受信する前に前記第1のサブシステムと前記第2のサブシステムの間で共有されたデータを含んでいる、請求項13に記載の第2のサブシステム。

【請求項15】

前記アイテムは、前記電子デバイスに、前記第2のサブシステムのサービスまたは製品へのアクセスを提供する、提供されたアプレットに対応している、請求項11に記載の第2のサブシステム。

【発明の詳細な説明】

20

【技術分野】

【0001】

(関連出願の相互参照)

本出願は、2016年6月12日に先に出願された米国仮特許出願第62／349,003号の利益を主張するものであり、参照によりその全体が本明細書に組み込まれる。

【0002】

本開示は、電子デバイスとサービスプロバイダの間のセキュリティ保護された取引を管理することに関する。

【背景技術】

【0003】

30

ポータブル電子デバイス（例えば、セルラー電話）には、商品又はサービスとの引き換えでサービスプロバイダと取引を行うために使用されうる資格データを記憶及び／又は生成するセキュアエレメントを設けることができる。しかし、このような取引のセキュリティ保護された認可及び管理は、非効果的又は非効率的であることが多い。

【発明の概要】

【0004】

本明細書では、電子デバイスとサービスプロバイダの間のセキュリティ保護された取引を管理するためのシステム、方法、及びコンピュータ可読媒体について説明する。

【0005】

例として、方法は、運用エンティティサブシステムにて、電子デバイスに記憶されるサービスプロバイダサブシステムの価値アイテムに対する注文を示すデバイス注文データを電子デバイスから受信することと、注文を示すデバイス注文データの少なくとも一部分を含む運用注文データをサービスプロバイダサブシステムに送信することと、サービスプロバイダサブシステムによる価値に対する注文の履行の状況を示す注文状況更新データをサービスプロバイダサブシステムから受信することと、運用エンティティ及びサービスプロバイダサブシステムの共有秘密を使用して、受信した注文状況更新データを検証することと、を含むことができる。

40

【0006】

別の例として、サービスプロバイダシステム及び電子デバイスと通信状態にある運用エンティティシステムは、少なくとも1つのプロセッサ構成要素と、少なくとも1つのメモ

50

リ構成要素と、少なくとも1つの通信構成要素とを備え、運用エンティティシステムは、電子デバイスからデバイス注文データを受信することであって、受信したデバイス注文データは、電子デバイスに記憶されるサービスプロバイダシステムの価値アイテムに対する注文を示す、デバイス注文データを受信し、受信したデバイス注文データに基づいて、サービスプロバイダシステムに運用注文データであって、運用注文データは価値アイテムに対する注文を示す、運用注文データを送信し、送信した運用注文データに基づいて、サービスプロバイダシステムからサービスプロバイダ履行データであって、サービスプロバイダ履行データは価値アイテムを含む、サービスプロバイダ履行データを受信し、受信したサービスプロバイダ履行データに基づいて、電子デバイスに運用履行データであって、運用履行データは価値アイテムを含む、運用履行データを送信するように構成されている。

10

【0007】

また別の例として、製品は、非一時的なコンピュータ可読媒体と、非一時的なコンピュータ可読媒体に記憶されたコンピュータ可読命令であって、実行されると、コンピュータに、ターゲット電子デバイスに記憶されるサービスプロバイダシステムの価値アイテムに対する注文を示すデバイス注文データをソース電子デバイスから受信させ、注文を示すデバイス注文データの少なくとも一部分を含む認可注文データをサービスプロバイダシステムに送信させ、送信した認可注文データに応じて、価値アイテムを含むサービスプロバイダ履行データをサービスプロバイダシステムから受信させ、受信したサービスプロバイダ履行データの少なくともアイテム価値をターゲット電子デバイスに送信させる、のに有効なコンピュータ可読命令を含むことができる。

20

【0008】

本概要は、本明細書にて説明する主題の一部の態様の基本的な理解をもたらすように、一部の例示的な実施形態を提示するためのみに提供されるものである。したがって、本概要にて説明する特徴は例にすぎないことが理解されよう。本明細書にて説明する主題の範囲又は趣旨を、いかなる方法でも狭めるように解釈されてはならない。特に断らない限り、一例の文脈にて説明する特徴を、他の1つ以上の例の文脈にて説明する特徴と組み合わせてもよく、共に使用してもよい。本明細書にて説明する主題の他の特徴、態様及び利点は、以下の詳細な説明、図及び請求項から明らかになるであろう。

【0009】

以下の議論では、同じ参照文字が全体を通して同じ要素を参照している、以下の図面を参照する。

30

【図面の簡単な説明】

【0010】

【図1】セキュリティ保護された取引を管理するための例示的なシステムの概略図である。

【図1A】図1の例示的なシステムのより詳細な概略図である。

【図2】図1及び図1Aのシステムの例示的な電子デバイスのより詳細な概略図である。

【図3】図1～図2の例示的な電子デバイスの正面図である。

【図3A】セキュリティ保護された取引を管理するための処理を例示する、図1～図3のうちの1つ以上の少なくとも1つの電子デバイスにおけるグラフィックユーザインターフェース画面の正面図である。

40

【図3B】セキュリティ保護された取引を管理するための処理を例示する、図1～図3のうちの1つ以上の少なくとも1つの電子デバイスにおけるグラフィックユーザインターフェース画面の正面図である。

【図3C】セキュリティ保護された取引を管理するための処理を例示する、図1～図3のうちの1つ以上の少なくとも1つの電子デバイスにおけるグラフィックユーザインターフェース画面の正面図である。

【図3D】セキュリティ保護された取引を管理するための処理を例示する、図1～図3のうちの1つ以上の少なくとも1つの電子デバイスにおけるグラフィックユーザインターフェース画面の正面図である。

【図3E】セキュリティ保護された取引を管理するための処理を例示する、図1～図3の

50

うちの1つ以上の少なくとも1つの電子デバイスにおけるグラフィックユーザインターフェース画面の正面図である。

【図4】図1及び図1Aのシステムの例示的な運用エンティティサブシステムのより詳細な概略図である。

【図5】セキュリティ保護された取引を管理するための例示的な処理のフローチャートである。

【図6】セキュリティ保護された取引を管理するための例示的な処理のフローチャートである。

【発明を実施するための形態】

【0011】

図1及び図1Aは、電子デバイス100とサービスプロバイダサブシステム200の間のセキュリティ保護された取引を管理しうる運用エンティティサブシステム400を介して電子デバイス100のセキュアエレメント上に提供される1つ以上の取引資格（例えば、決済資格及び／又はサービス資格）を、サービスプロバイダ（「SP」）サブシステム200と共有しうるシステム1を示しており、図2及び図3は、システム1の電子デバイス100の具体的な実施形態に関する更なる詳細を示しており、図3A～図3Eは、そのようなセキュリティ保護された取引中のシステム1の電子デバイス100のグラフィックユーザインターフェースを表しうる例示的な画面190a～190eを示しており、図4は、システム1の運用エンティティサブシステム400の具体的な実施形態に関する更なる詳細を示しており、図5及び図6は、セキュリティ保護された取引を管理するための例示的な処理のフローチャートである。

【0012】

図1は、運用エンティティサブシステム400にて電子デバイス100とサービスプロバイダサブシステム200の間のセキュリティ保護された取引を管理することを可能にしうる例示的なシステム1の概略図である。電子デバイス100は、サービスプロバイダサブシステム200から電子デバイス100への新たなサービスプロバイダ価値の移転に資金提供するための、サービスプロバイダサブシステム200との取引において使用するためのデバイス注文（又は購入）データを生成することができ、電子デバイス100のユーザの便益のための、サービスプロバイダサブシステムの具体的なサービスプロバイダ製品（例えば、好適な任意の商品又はサービス）にアクセスするために（例えば、具体的なサービスプロバイダイベント、又は具体的なサービスプロバイダデータ若しくは物理的な商品へのアクセスを可能にするために）、デバイス100によりサービスプロバイダ価値を後で使用することができる。このようなデバイス注文データは、好適な任意の取引資格データ（例えば、サービスプロバイダ資格又は金融機関資格又は取引に資金提供するための好適な任意の価値ソースを提供又は識別するように機能しうる他の好適な任意の取引資格）を含むことができ、取引資格データは、電子デバイス100のセキュアエレメント上に記憶された好適な任意の取引資格又は資金提供資格により提供されてもよく、それらに基づいてもよく、サービスプロバイダサブシステム200との取引に資金提供するように機能することができる。しかし、電子デバイス100は、このようなデバイス注文データをサービスプロバイダサブシステム200に通信するのではなく、電子デバイス100及び／又はサービスプロバイダサブシステム200の信頼されたサービスマネージャでありうる運用（又は商業又は認可）エンティティサブシステム400に通信することができる。例えば、デバイス注文は、デバイス100のセキュアエレメント上の資金提供資格を使用して生成することができ、デバイス100の同一のセキュアエレメント上への新たなサービスプロバイダ価値の追加に資金提供することができ、運用エンティティサブシステム400は、サービスプロバイダサブシステム200と電子デバイス100の間の全ての通信の導管の役割を果たすことにより取引全体の中心的役割を担うことができ、それにより、運用エンティティサブシステム400及び他のサブシステム／デバイスの1つ以上にとって利用可能な1つ以上の共有秘密を使用することにより、デリケートな資格データをサブシステムの間で安全に通信することを運用エンティティサブシステム400に可能にする

10

20

30

40

50

ことができる。一部の実施形態では、運用エンティティサブシステム400は、デバイス100のセキュアエレメントに及び／又はセキュアエレメントから資格データを安全に通信する（例えば、サービスプロバイダ資格データ及び／又は金融機関資格データを暗号化通信する）ように機能しうる、システム1内の唯一のサブシステムとなることができ、それにより、運用エンティティサブシステム400は、サービスプロバイダサブシステムと電子デバイス100の間で通信される全ての注文取引データのためのゲートキーパの役割を果たしうようになっている。運用エンティティサブシステム400は、任意の注文の状況を確認に追跡するように、並びに／又はサービスプロバイダサブシステム200によりデバイス注文に資金提供する責任及び／若しくは新たなサービスプロバイダ価値を電子デバイス100上に提供する責任を管理するように機能することができる。電子デバイス100と運用エンティティサブシステム400の間における好適な任意のデータの通信を、好適な任意の通信設備95を介して可能にすることができ、通信設備には、好適な任意の通信プロトコル（単数又は複数）及び／又は好適な任意のネットワーク及び／又はクラウドアーキテクチャ（単数又は複数）を使用する、好適な任意の有線通信経路、無線通信経路、又は2つ以上の有線及び／若しくは無線通信経路の組合せを含むことができる。加えて又は代わりに、サービスプロバイダサブシステム200と運用エンティティサブシステム400の間における好適な任意のデータの通信を、好適な任意の通信設備95を介して可能にしてもよい。加えて又は代わりに、運用エンティティサブシステム400を介して行わなくてもよい電子デバイス100とサービスプロバイダサブシステム200の間における好適な任意のデータの通信を、好適な任意の通信設備95を介して可能にしてもよい。

【0013】

図1Aに示すように、システム1のより具体的な実施形態は、電子デバイス100（例えば、「ホスト」又は「ソース」電子デバイス）、電子デバイス100'（例えば、「クライアント」又は「ターゲット」又は「受領側」電子デバイス）、サービスプロバイダ（「SP」）サブシステム200、金融機関サブシステム350、及び運用エンティティサブシステム400を含むことができ、SPサブシステム200は、サービスプロバイダ認可（「SPA」）サブシステム202、第1のサービスプロバイダ発行者（「SPI」）サブシステム250、及び第2のSPIサブシステム290を含むことができる。その上、図1Aに示すように、システム1は、電子デバイス100とサービスプロバイダサブシステム200（例えば、第1のSPIサブシステム250）の間の通信を可能にする通信経路15と、電子デバイス100と運用エンティティサブシステム400の間の通信を可能にする通信経路25と、運用エンティティサブシステム400とサービスプロバイダサブシステム200（例えば、SPAサブシステム202）の間の通信を可能にする通信経路35と、運用エンティティサブシステム400と金融機関サブシステム350の間の通信を可能にする通信経路45と、サービスプロバイダサブシステム200（例えば、第1のSPIサブシステム250）と金融機関サブシステム350の間の通信を可能にする通信経路55と、電子デバイス100'と運用エンティティサブシステム400の間の通信を可能にする通信経路65と、SPサブシステム200のSPAサブシステム202と第1のSPIサブシステム250の間の通信を可能にする通信経路75と、SPサブシステム200のSPAサブシステム202と第2のSPIサブシステム290の間の通信を可能にする通信経路85とを含むことができる。経路15、25、35、45、55、65、75、及び85の1つ以上を、1つ以上の信頼されたサービスマネージャ（「TSM」）により少なくとも部分的に管理することができる。通信ネットワークを形成するように機能しうる、好適な任意の回路構成、デバイス、システム、又はそれら（例えば、1つ以上の通信タワー、電気通信サーバその他を含みうる有線及び／又は無線通信インフラストラクチャ）の組合せを使用して、好適な任意の有線又は無線通信プロトコルを使用する通信を提供することが可能である経路15、25、35、45、55、65、75、及び85の1つ以上を提供することができる。例えば、経路15、25、35、45、55、65、75、及び85の1つ以上は、Wi-Fi（例えば、802.11プロトコル）、Zig

10

20

30

40

50

Bee（例えば、802.15.4プロトコル）、WiDi（登録商標）、Ethernet、Bluetooth（登録商標）、BLE、高周波システム（例えば、900MHz、2.4GHz、及び5.6GHz通信システム）、赤外線、TCP/IP、SCTP、DHCP、HTTP、BitTorrent（登録商標）、FTP、RTP、RTSP、RTCP、RAOP、RDTP、UDP、SSH、WDS-bridging、無線及びセルラー電話並びに個人用電子メールデバイスにより使用されうる任意の通信プロトコル（例えば、GSM、GSM plus EDGE、CDMA、OFDMA、HSPA、マルチバンドなど）、低出力無線パーソナルエリアネットワーク（「6LoWPAN」）モジュールにより使用されうる任意の通信プロトコル、他の任意の通信プロトコル、又はこれらの任意の組合せをサポートすることができる。経路15、25、35、45、55、65、75、及び85の1つ以上を好適な任意の通信設備（例えば、図1の通信設備95）により可能にすることができる。

【0014】

図1A及び／又は図2に示すように、例えば、電子デバイス100は、プロセッサ102、メモリ104、通信構成要素106、電源108、入力構成要素110、出力構成要素112、アンテナ116、及び近距離無線通信（「NFC」）構成要素120を含むことができる。電子デバイス100は、デバイス100の他の種々の構成要素に、同構成要素から又は同構成要素間でデータ及び／又は電力を移転する、1つ以上の有線又は無線通信リンク若しくは経路を提供しうるバス118を含むこともできる。電子デバイス100には、デバイス100の外部のゴミ及び他の劣化力から保護するために、デバイス100の構成要素のうちの1つ以上を少なくとも部分的に取り囲みうる筐体101を設けることもできる。一部の実施形態では、電子デバイス100の1つ以上の構成要素を組合せ又は省略してもよい。その上、電子デバイス100は、図1A及び／又は図2に示していない他の構成要素を含んでもよい。例えば、電子デバイス100は、他の好適な任意の構成要素、又は、図1A及び／又は図2に示す構成要素（例えば、アンテナ）のいくつかのインスタンスを含んでもよい。簡潔にするために、図2には、それぞれの構成要素を1つだけ示している。ユーザがデバイス100と対話若しくはインターフェースすることを可能にするために、1つ以上の入力構成要素110を設けることができ、並びに／又は、デバイス100のユーザに情報（例えば、グラフィック、聴覚、及び／又は触覚情報）を提示するために、1つ以上の出力構成要素112を設けることができる。本明細書では、1つ以上の入力構成要素及び1つ以上の出力構成要素を入力／出力（「I/O」）構成要素又はI/Oインターフェース114と総称する（例えば、入力構成要素110及び出力構成要素112をI/O構成要素又はI/Oインターフェース114と総称する）場合があることに留意されたい。例えば、入力構成要素110及び出力構成要素112は、表示画面のタッチにより入力情報を受け取り、同一の表示画面により視覚情報を出し示す、タッチスクリーンなどの単一のI/O構成要素114である場合がある。電子デバイス100のプロセッサ102は、電子デバイス100の1つ以上の構成要素の動作及びパフォーマンスを制御するように機能しうる任意の処理回路構成を含むことができる。例えば、プロセッサ102は、入力構成要素110から入力信号を受信し、及び／又は出力構成要素112を通じて出力信号を駆動することができる。図2に示すように、アプリケーション103及び／又はアプリケーション113などの1つ以上のアプリケーションを実行するためにプロセッサ102を使用することができる。一例として、アプリケーション103は、オペレーティングシステムアプリケーションとすることができ、アプリケーション113は、サードパーティアプリケーション又は他の好適な任意のオンラインリソース（例えば、サービスプロバイダサブシステム200のサービスプロバイダと関連付けられたアプリケーション）とすることができる。その上、プロセッサ102は、デバイス100を識別するために利用しうるデバイス識別情報119にアクセスすることができる。

【0015】

NFC構成要素120は、（例えば、単一チップ又は複数チップのセキュアマイクロコントローラとして）耐タンパー性プラットフォームを提供するように構成されうるセキュ

10

20

30

40

50

アエレメント１４５を含み、そうでなければ提供することができ、セキュアエレメントは、よく識別された信頼された権限者の集合（例えば、ＳＰサブシステム２００及び／又は運用エンティティサブシステム４００及び／又は金融機関サブシステム３５０及び／又はGlobal Platformなどの業界標準の権限者）により定められうる規則及びセキュリティ要件に従って、アプリケーション及びそれらの機密及び暗号データを安全にホスティングすることが可能である。サービスプロバイダ資格情報及び／又は金融機関資格情報などの好適な任意の取引資格情報を、デバイス１００（例えば、ＮＦＣ構成要素１２０）のセキュアエレメント１４５上のアプレットに記憶することができ、サービスプロバイダサブシステム２００及び／又は金融機関サブシステム３５０（例えば、銀行）などのリモートエンティティサブシステムとの取引の好適な任意のデバイス注文データにおいて使用するための取引資格データを提供するように構成することができる。例えば、取引資格データは、実際の価値ソースを提供することができ、及び／又はリモートエンティティサブシステムと関連付けられた、価値ソースとして使用しうるアカウントを識別するための十分な詳細を提供することができ、好適な任意のサービスプロバイダサービス（例えば、電子デバイス１００のユーザの便益のためにサービスプロバイダサブシステム２００に代えて提供されうる好適な任意の商品又はサービス）に関する電子デバイス１００とサービスプロバイダサブシステム２００の間の取引に少なくとも部分的に資金提供するために価値ソースを使用することができる。

【００１６】

サービスプロバイダサブシステム２００（例えば、デバイス１００のユーザが、デバイス１００上に記憶された１つ以上の取引資格を使用して、近接して位置するサービスプロバイダ端末２２０との取引を非接触近接ベース通信を介して行い、実店舗又は任意の物理的な位置に位置し、ＳＰサブシステム２００（例えば、ＳＰＩサブシステム２５０）のＳＰＩ端末２２０）との非接触近接ベース通信５（例えば、近距離無線通信）として、いくつかの取引資格データを通信するように、ＮＦＣ構成要素１２０を構成することができる。代わりに又は加えて、デバイス１００が、（例えば、通信経路１５、２５、及び３５の１つ以上を介して）好適な任意の有線又は無線プロトコルを使用して、好適な任意の取引資格データを他の１つ以上の電子デバイス又はサーバ又はサブシステム（例えば、好適な任意のオンライン通信によりＳＰサブシステム２００（例えば、ＳＰＩサブシステム２５０）のＳＰＩサーバ２１０など、システム１の１つ以上のサブシステム又は他の構成要素）と（例えば、オンラインベース通信として）通信することを可能にするように、通信構成要素１０６が設けられてもよい。デバイス１００のプロセッサ１０２は、デバイス１００の１つ以上の構成要素の動作及びパフォーマンスを制御するように機能し、任意の処理回路構成を含むことができる。例えば、１つ以上のアプリケーション（例えば、デバイス又は運用エンティティアプリケーション１０３及び／又はオンラインリソース又はサービスプロバイダ又は金融機関アプリケーション１１３）をデバイス１００上で実行するようにプロセッサ１０２を構成することができ、アプリケーションは、サービスプロバイダサブシステム２００との取引に資金提供するために、そうでなければ取引を行うために、データ（例えば、好適な任意のデバイス注文データの取引資格データ）をデバイス１００により通信し、方法を少なくとも部分的に命令することができる。その上、デバイス１００は、プロセッサ１０２又はデバイス１００の他の好適な任意の部分にとってアクセス可能であり、好適な任意のデバイス識別情報又はデバイス識別子（例えば、図２のデバイス識別子情報１１９）を含むことができる。デバイス１００を一意に識別して、サービスプロバイダサブシステム２００との取引を容易にするために、及び／又はデバイス１００との好適な任意のセキュリティ保護された通信を可能にするために、運用エンティティサブシステム４００及び／又はサービスプロバイダサブシステム２００などの、システム１の好適な任意のサブシステムにより好適な任意のデバイス識別情報を利用することができる。単なる一例として、デバイス識別情報は、電話番号若しくは電子メールアドレス、又はデバイス１００と関連付けられうる任意の一意的識別子とすることができる。

10

20

30

40

50

【0017】

NFC構成要素120は、電子デバイス100とサービスプロバイダサブシステム200のサービスプロバイダ端末（例えば、サービスプロバイダ決済端末220）の間の非接触近接ベースの取引又は通信を可能にする好適な任意の近接ベース通信メカニズムとすることができる。NFC構成要素120は、電子デバイス100と、このようなサービスプロバイダ端末の間の非接触近接ベース通信を可能にするための好適な任意のモジュールを含むことができる。図2に示すように、例えば、NFC構成要素120は、NFCデバイスモジュール130、NFCコントローラモジュール140、及び／又はNFCメモリモジュール150を含むことができる。NFCデバイスモジュール130は、NFCデータモジュール132、NFCアンテナ134、及びNFCブースタ136を含むことができる。NFC構成要素120により非接触近接ベース通信又はNFC通信の一部としてサービスプロバイダ端末に送信されうる好適な任意のデータを收容し、経路設定し、そうでなければ提供するように、NFCデータモジュール132を構成することができる。加えて又は代わりに、NFC構成要素120により非接触近接ベース通信の一部としてサービスプロバイダ端末から受信されうる好適な任意のデータを收容し、経路設定し、そうでなければ受信するように、NFCデータモジュール132を構成してもよい。NFCコントローラモジュール140は、少なくとも1つのNFCプロセッサモジュール142を含むことができる。NFCプロセッサモジュール142は、電子デバイス100とサービスプロバイダ端末の間でNFC通信を行うためにNFC構成要素120を有効化、アクティブ化、許可するように、及び／又はそうでなければ制御するように、NFCデバイスモジュール130と共に動作することができる。NFCコントローラモジュール140は、NFC構成要素120の機能を命令するのに役立ちうるNFC低出力モード又はウォレットアプリケーション143などの、1つ以上のアプリケーションを実行するために使用されうる、少なくとも1つのNFCプロセッサモジュール142を含むことができる。NFCメモリモジュール150は、電子デバイス100とサービスプロバイダサブシステム200の間のNFC通信を可能にするように、NFCデバイスモジュール130及び／又はNFCコントローラモジュール140と共に動作することができる。NFCメモリモジュール150は、耐タンパー性とすることができ、セキュアエレメント145の少なくとも一部分を提供することができる。例えば、このようなセキュアエレメントを、（例えば、単一チップ又は複数チップのセキュアマイクロコントローラとして）耐タンパー性プラットフォームを提供するように構成することができ、プラットフォームは、よく識別された信頼された権限者の集合（例えば、金融機関サブシステム及び／又はGlobal Platformなどの業界標準の権限者）により定められうる規則及びセキュリティ要件に従って、アプリケーション及びそれらの機密及び暗号データ（例えば、アプレット153及び鍵155）を安全にホスティングすることが可能である。

【0018】

図2に示すように、例えば、NFCメモリモジュール150は、NFC仕様標準（例えば、Global Platform）により定義され管理されうる、発行者セキュリティドメイン（「ISD」）152及び追加セキュリティドメイン（「SSD」）154（例えば、サービスプロバイダセキュリティドメイン（「SPSD」）、信頼されたサービスマネージャセキュリティドメイン（「TSMSSD」）など）のうちの1つ以上を含むことができる。例えば、ISD152は、NFCメモリモジュール150の一部分とすることができ、その一部分には、信頼されたサービスマネージャ（「TSM」）又は発行用リモートサブシステム（例えば、サービスプロバイダサブシステム200及び／又は金融機関サブシステム350及び／又は運用エンティティサブシステム400）が、資格コンテンツ管理及び／又はセキュリティドメイン管理のために、（例えば、通信構成要素106を介して）電子デバイス100上に1つ以上の資格（例えば、種々のクレジットカード、バンクカード、ギフトカード、価値記憶カード、金額追加可能なカード、アクセスカード、交通パス、サービスプロバイダ製品アクセスパス又は価値、デジタル通貨（例えば、ビットコイン及び関連する決済ネットワーク）などに関連付けられた資格）を形成し、そうで

10

20

30

40

50

なければ提供するために鍵及び／又は他の好適な情報を記憶することができる。資格は、ユーザ／消費者／デバイスに割り当てられ電子デバイス100上に安全に記憶されうる、クレジットカード決済番号（例えば、トークン又は他のものとして）例えば、デバイス主アカウント番号（「DPAN」）、DPAN有効期限、CVVなど）などの資格データ（例えば、資格情報）を含むことができる。示すように、NFCメモリモジュール150は、少なくとも3つのSSD154（例えば、少なくとも第1のSSD154a、第2のSSD154b、及び第3のSSD154c）を含むことができる。例えば、第1のSSD154a（例えば、サービスプロバイダ資格SSD154a）を、電子デバイス100に特定の特典又はアクセス権を提供しうる特定のサービスプロバイダ資格（例えば、サービスプロバイダサブシステム200により提供されうる特定のタイプの価値ソース資格）と関連付けることができ、第2のSSD154b（例えば、金融機関資格SSD154b）を、電子デバイス100に特定の特典又は決済権を提供しうる特定の金融機関資格（例えば、金融機関サブシステム350により提供される特定のクレジットカード資格又は他の好適な決済資格）と関連付けることができ、第3のSSD154c（例えば、運用SSD154c）を、別のSSD（例えば、第1のSSD154a及び／又は第2のSSD154b）の特定の資格へのデバイス100のアクセスを制御して、例えば、特定の特典又は決済権を電子デバイス100に提供しうる運用エンティティ（例えば、デバイス100の制御エンティティでありうる、運用エンティティサブシステム400の運用エンティティ）と関連付けることができる。異なるセキュアエレメント上又は同一のセキュアエレメント上に様々なSSDを設けることができる。例えば、デバイス100の第1のセキュアエレメント上にSSD154aを設けることができ、第1のセキュアエレメントとは異なりうるデバイス100の第2のセキュアエレメント上にSSD154bを設けることができる。SSD154は、少なくとも1つのアプレット153を含むことができ、及び／又はアプレットと（例えば、SSD154aがアプレット153aと、SSD154bがアプレット153bと、SSD154cがアプレット153cと）関連付けられることができる。例えば、SSD154のアプレット153は、（例えば、GlobalPlatform環境で）NFC構成要素120のセキュアエレメント上で実行しうるアプリケーションとすることができる。資格アプレット153は、資格情報を含むことができ、又は資格情報と関連付けられることができる（例えば、SSD154a及び／又はSSD154bの資格情報は、デバイス100とサービスプロバイダサブシステム200の間の取引に資金提供するための取引資格データを提供するように機能しうる）。各SSD154及び／又はアプレット153は、少なくとも1つの鍵155を含むことができ、及び／又は少なくとも1つの鍵と（例えば、アプレット153aが少なくとも1つの鍵155aと、アプレット153bが少なくとも1つの鍵155bと、アプレット153cが少なくとも1つの鍵155cと）関連付けられることができる。

【0019】

SSD154の鍵155は、暗号アルゴリズム又は暗号の機能的出力を決定しうる情報とすることができる。例えば、暗号化では、鍵は、平文から暗号文への具体的な変換を指定することができる、解読中はその逆とすることができる。デジタル署名方式及びメッセージ認証コードなどの他の暗号アルゴリズムにおいて鍵を使用することもできる。SSDの鍵は、好適な任意の共有秘密を別のエンティティに提供することができる（例えば、サービスプロバイダ資格SSD154aの鍵155aは、サービスプロバイダサブシステム200にとってアクセス可能とすることができる（例えば、サービスプロバイダ資格SSD154aの鍵155aは、SSD154aとSPサブシステム200の間におけるSSD154aの資格データのセキュリティ保護された通信を可能にするために、SPサブシステム200のSPI鍵155aと同一でもよく、又はSPI鍵と関連付けられてもよく（例えば、それらは、公開鍵／秘密鍵ペアでありうる））、金融機関資格SSD154bの鍵155bも、金融機関サブシステム350にとってアクセス可能とすることができる（例えば、金融機関資格SSD154bの鍵155bは、SSD154bと金融機関サブシステム350の間におけるSSD154bの資格データのセキュリティ保護された通信を可能に

10

20

30

40

50

するために、金融機関サブシステム 350 の鍵 155b と同一でもよく、又は鍵と関連付けられてもよく（例えば、それらは、公開鍵／秘密鍵ペアでありうる）、及び／又は運用資格 SSD 154c の鍵 155c も、運用エンティティサブシステム 400 にとってアクセス可能とすることができる（例えば、運用資格 SSD 154c の鍵 155c は、SSD 154c と運用エンティティサブシステム 400 の間における SSD 154c の資格データのセキュリティ保護された通信を可能にするために、運用エンティティサブシステム 400 の運用鍵 155c と同一でもよく、又は運用鍵と関連付けられてもよい（例えば、それらは、公開鍵／秘密鍵ペアでありうる））。デバイス 100 のセキュアエレメント 145 の SSD とリモートサブシステムの間のような共有秘密は、電子デバイス 100 のセキュアエレメントとリモートサブシステムの両方に対する好適な任意の共有秘密鍵（例えば、パスワード、パスフレーズ、ランダムに選ばれたバイトのアレ、1 つ以上の対称鍵、公開秘密鍵（例えば、非対称鍵）など）とすることができ、共有秘密は、機能的出力が共有秘密により少なくとも部分的に決定されうる好適な任意の暗号アルゴリズム又は暗号を使用することなどによって、好適な任意の暗号データ（例えば、暗号）又は他の好適な任意のデータを、（例えば、取引のための資金提供データを有効にするために）電子デバイス 100 及びリモートサブシステムにより独立して生成することを可能にするように機能することができ、そのような共有秘密をリモートサブシステムによりデバイス 100 上に提供することができる。（例えば、リモートサブシステムによりデバイス 100 上に資格を提供する間に）リモートサブシステムとデバイス 100 の間で共有秘密を事前に共有することができ、その場合、そのような共有秘密を事前共有鍵と呼ぶ場合があり、又は鍵共有プロトコル（例えば、ディフィーヘルマンなどの公開鍵暗号法、又はケルベロスなどの対称鍵暗号法）を使用して、具体的な金融取引に使用される前に共有秘密を形成することができる。共有秘密、及び機能的出力が共有秘密により少なくとも部分的に決定されうる好適な任意の暗号アルゴリズム若しくは暗号は、デバイス 100 のセキュアエレメントにとってアクセス可能とすることができる。鍵及びアプレットのそれぞれを、TSM 又は認可されたエージェントによりデバイス 100 のセキュアエレメント上にロードしてもよく、デバイス 100 上に初めて提供されるときにセキュアエレメント上に事前ロードしてもよい。一例として、資格 SSD 154b を具体的なクレジットカード資格と関連付けることができ、その資格 SSD 154b のアプレット 153b が、そのような使用のために有効化され、そうでなければアクティブ化又はロック解除されているときに、その具体的な資格をデバイス 100 のセキュアエレメント（例えば、NFC 構成要素 120）から取引のための取引資格データとしてのみ通信することができる。

【0020】

NFC 構成要素 120 の使用を可能にするために、資格のクレジットカード情報又はバンクアカウント情報などの機密資格情報を電子デバイス 100 から送信するときに特に有用でありうるセキュリティ特徴を提供することができる。このようなセキュリティ特徴は、アクセスが制限されうるセキュリティ保護された記憶領域を含むこともできる。セキュリティ保護された記憶領域にアクセスするために、例えば、個人識別番号（「PIN」）の入力又は生体認証センサとのユーザ対話によるユーザ認証の提供を必要とすることができる。例として、運用 SSD 154c は、他の SSD 154（例えば、資格 SSD 154a 又は資格 SSD 154b）をその資格情報を通信するために使用することを可能にする前に、このような認証が生じたかどうかを判定するために、アプレット 153c を活用することができる。いくつかの実施形態では、セキュリティ特徴の一部又は全てを NFC メモリモジュール 150 内に記憶することができる。いくつかの実施形態では、NFC メモリモジュール 150 は、電子デバイス 100 内に組み込まれたマイクロコントローラを含むことができる。単なる一例として、運用 SSD 154c のアプレット 153c を、（例えば、バイオメトリック入力構成要素などの 1 つ以上の入力構成要素 110 により）デバイス 100 のユーザの意向及びローカル認証を決定するように構成することができ、そのような決定に応じて、（例えば、資格 SSD 154a の資格により）取引を行うために別の具体的な SSD を有効化するように構成することができる。

10

20

30

40

50

【0021】

サービスプロバイダサブシステム200は、SPAサブシステム202、及び第1のサービスプロバイダ発行者（「SPI」）サブシステム250及び第2のSPIサブシステム290などの少なくとも1つのSPIサブシステムを含むことができる。SPサブシステム200のSPIサブシステムのそれぞれは、売買業者又はデバイス100のユーザの便益のための好適な任意のサービス又は商品を提供するように機能しうる他の好適なタイプのサービスプロバイダ（例えば、輸送プロバイダ、イベントプロバイダ、ホスピタリティプロバイダ、商品販売者など）とすることができる。例えば、一部の実施形態では、SPIサブシステムは、デバイス100のユーザにとっての価値となりうる好適な任意のSP製品（例えば、商品若しくはサービス又は位置若しくは他の好適な構成）へのアクセスを制御しうるSPエンティティにより制御されてもよく、又はSPエンティティの代わりに動作されてもよく、SPIサブシステムは、受領側電子デバイス（例えば、注文用ホスト電子デバイス100又は注文用ホスト電子デバイス100により識別されうる好適な任意の受領側デバイス（例えば、クライアントデバイス100'））と共有されうる好適な任意のサービスプロバイダ価値（「SPV」）データを生成するように動作することができ、そのようなSPVデータを、SP製品への一定のアクセスを得るために受領側デバイスにより後で使用するために、（例えば、実際価値のアイテムとして）受領側デバイス上に記憶することができる。例えば、SPVデータは、受領側デバイス（例えば、デバイス100のセキュアエレメント145）上に記憶され、具体的な貨幣価値のSP製品にアクセスするために受領側デバイスにより使用されるときに、その価値だけ減らされうる実際の貨幣価値とすることができる（例えば、SPVデータは、受領側デバイス上の価値記憶カード上に記憶される\$80とすることができ、受領側デバイスがSP製品にアクセスするために価値記憶カードの資格データを使用するときには一定の量（例えば、乗降提供サービスプロバイダにより提供される、乗降に対して支払う\$12.37、又はトランジットシステムサービスプロバイダに関する1回の乗降にアクセスするための\$2、又はサービスプロバイダのトランジットシステムに連続5時間アクセスするための\$5）だけ減らすことができる）。別の例として、SPVデータは、一定のタイプのSP製品にアクセスする能力により評価することができ、SPVデータを、受領側デバイス上（例えば、デバイス100のセキュアエレメント145内）に記憶し、SP製品にアクセスするために受領側デバイスにより使用されるときに、好適な任意の単位だけ減らし、又は完全に除去してもよい（例えば、SPVデータは、受領側デバイス上の価値記憶カードに記憶され、SP製品にアクセスするために、受領側デバイスが価値記憶カードの資格データを使用するときには、次いで一定の量だけ減らされうる、SP製品への10回の単一の許可パス（例えば、動物園に2人がアクセスするための2パス）を示すことができる）。

【0022】

好適な任意のSP製品アクセスを受領側デバイス及び／又はその所有者及び／又はその所有者の関係者に与えるために、SPVデータを、受領側デバイス上に記憶し、SPサブシステム200（例えば、端末220）により受信されるSPアクセスデータ（例えば、具体的な娯楽イベント又は輸送イベント又は（例えば、受領側デバイスにダウンロードする）メディアデータその他に対する許可）を生成するために受領側デバイスにより利用されるときに、好適な任意の方法（例えば、非接触近接ベース通信5）で調節することができ、SPVデータを、SPサブシステム200とのSPVデータの通信によりSP製品アクセスと引き換えられうる、具体的なSP製品アクセスの購入のレシート（例えば、サービスプロバイダの物理的な商品を受け取るために受領側デバイスのユーザにより提示されるレシート）の証拠として使用するために受領側デバイス上に提供することができる。したがって、SPVデータは、サービスプロバイダ資格データの少なくとも一部分を（例えば、セキュアエレメント145上のサービスプロバイダSSD154aのサービスプロバイダアプレット153aの一部分を、又はセキュアエレメントではなくデバイス100のメモリ104に記憶されうるサービスプロバイダ資格データ123として）定義するために受領側デバイス（例えば、デバイス100及び／又はデバイス100'）上に記憶されう

10

20

30

40

50

る好適な任意のデータとすることができ、それを、次いで、ＳＰ製品にアクセスするためにＳＰアクセスデータの少なくとも一部分として、受領側デバイスによりサービスプロバイダに提供することができる。受領側デバイス上に提供される特定のサービスプロバイダ資格データを、ＳＰサブシステム２００により具体的なユーザの１つ又は複数のアカウントに電子的にリンクされうる特定のＳＰ資格（例えば、種々のタイプの記憶価値カード（例えば、トランジットカード又は電子マネーカードのアカウント）、ギフトカード、ロイヤルティカード、リワードカード／アカウント、ポイントカード／アカウント、メリットカード／アカウント、クラブカード／アカウント、メンバーカード／アカウント、ディスロイヤルティカード／アカウント、ギフトカード／アカウント、スタンプカード／アカウント、クラスカード／アカウント、プライベートラベルアカウントカード／アカウント、金額追加可能なプリペイドアカウントカード／アカウント、金額追加不能なプリペイドアカウントカード／アカウント、パンチカード／アカウント、記憶価値カード／アカウント、同一のデジタル表現、その他）と関連付けることができる。このようなＳＰ資格データを、（例えば、運用エンティティサブシステム４００を介して）ＳＰサブシステム２００により（例えば、ＮＦＣ構成要素１２０のＳＰ資格追加セキュリティドメインのＳＰ資格、又はメモリ１０４のデータ１２３として）デバイス１００上に提供することができ、（例えば、商品若しくはサービス又は他のサービスプロバイダ資格データ（例えば、新たなＳＰＶデータ）に支払うために）サービスプロバイダサブシステム２００との取引に資金提供するためのデバイス注文データの少なくとも一部分として、デバイス１００により後で使用することができる。例えば、ＳＰＩサブシステム２５０は、（例えば、サーバ２１０からＳＰサブシステム２０２及び運用エンティティサブシステム４００を介してデバイス１００に）デバイス１００上に提供するためのＳＰＶデータを生成することができ、次いで、具体的なＳＰ製品にアクセスするためにＳＰＩサブシステム２５０に通信されうるＳＰアクセスデータを生成するために、そのＳＰＶデータをデバイス１００により使用することができる（例えば、デバイス１００は、ＳＰＶデータをＳＰアクセスデータの一部として、ＳＰＩサブシステム２５０の端末２２０への非接触近接ベース通信５として通信することができ、端末２２０をトランジットシステムのゲート付き自動改札機に設けることができ、トランジットシステムは、具体的なＳＰＶデータを伴う具体的なＳＰアクセスデータをデバイス１００から受信するのに応じて、そのトランジットシステムへの具体的なアクセスをデバイス１００のユーザに与えることができ、又はデバイス１００は、ＳＰＶデータをＳＰアクセスデータの一部として、ＳＰＩサブシステム２５０のサーバ２１０への通信経路１５を介したオンライン通信として通信することができ、サーバ２１０は、ＳＰウェブサイト又はポータルを管理することができ、具体的なＳＰＶデータを伴う具体的なＳＰアクセスデータをデバイス１００から受信するのに応じて、具体的なデータ（（例えば、そのＳＰウェブサイトに対する月間契約を証明するための）例えば、具体的なＳＰＶデータを提示できるユーザデバイスにとってのみアクセス可能でありうるウェブサイトの特別なコンテンツ））への具体的なアクセスをデバイス１００のユーザに与えることができる。一部の実施形態では、ＳＰＶデータを生成しうるＳＰＩサブシステムは、ＳＰ製品を実際に提供しうる、発券サブシステム、又はＳＰサブシステム２００の別のＳＰサブシステムの他の好適なパートナサブシステムとすることができる（例えば、第１のＳＰＩサブシステムは、受領側デバイス上に提供するためのＳＰＶデータを生成することができ、受領側デバイスは、次いで、そのＳＰＶデータを使用して第２のＳＰＩサブシステムのＳＰ製品にアクセスすることができる）。デバイス１００のＮＦＣ構成要素１２０の特定のサービスプロバイダ資格アプレット及び／又はデバイス１００のメモリ構成要素１０４の特定のサービスプロバイダ資格データ構造（例えば、データ１２３）を、ＳＰサブシステム２００により生成され、ＳＰサブシステム（例えば、特定のＳＰＩサブシステム）から通信されうるＳＰＶデータにより定義される特定のサービスプロバイダ資格と関連付けることができ、特定のサービスプロバイダ資格は、全てのユーザのための汎用のもの（例えば、デバイス１００を使用しうる具体的な任意の人にＳＰ製品アクセス（例えば、スポーツイベント製品へのアクセス）を提供しうる匿名のＳＰ資格）とすることができ

10

20

30

40

50

、及び／又は特定のユーザのための個人専用のもの（例えば、特定のＳＰ製品アクセス（例えば、特定の輸送旅行ルート製品へのアクセス）に関して具体的なユーザに対して登録されうる個人専用のＳＰ資格）とし、サービスプロバイダサブシステム２００により具体的なユーザの１つ又は複数のアカウントに電子的にリンクすることができる。いくつかのＳＰＶデータを、受領側デバイス上に記憶されたＳＰ価値及び／又は受領側デバイスにより提示されるＳＰ価値を認証するためにＳＰサブシステムによりスキャンされ、そうでなければ検出されうる、具体的なコード又は引き換え可能なデータ構造（例えば、ＱＲコード）として、受領側デバイスにより（例えば、表示出力構成要素上に）提示することができる。

【００２３】

テクノロジープロバイダ又はサービスイネーブラ若しくはブリッジとしても知られる、ＳＰＡサブシステム２０２を、１つ以上のＳＰＩサブシステム（例えば、ＳＰＩサブシステム２５０及び／又はＳＰＩサブシステム２９０）により動作させることができ、及び／又はＳＰＩサブシステムのパートナーとして動作させることができ、運用エンティティサブシステム４００が各ＳＰＩサブシステムと直接通信する必要がない（又はＳＰＩサブシステムに気づく必要もない）ように、かつ、各ＳＰＩサブシステムが運用エンティティサブシステム４００と直接通信する必要がないように、デバイス１００から適切なＳＰＩサブシステムに提供されるデバイス注文データを通信するために運用エンティティサブシステム４００と協働するように、ＳＰＡサブシステム２０２を構成することができる。一部の実施形態では、ＳＰＡサブシステム２０２及びＳＰＩサブシステム（例えば、ＳＰＩサブシステム２５０）を、単一のエンティティ（例えば、単一の制御エンティティにより動作される単一のサブシステム）とすることができ、ＳＰＡサブシステム２０２及びＳＰＩサブシステムを別々のエンティティ（例えば、異なる制御エンティティにより動作される異なるサブシステム）とすることができる。例えば、ＦｅｌｉｃａネットワークをＳＰＡサブシステム２０２の制御エンティティとすることができ、東日本旅客鉄道会社（「ＪＲＥ」）をＳＰＩサブシステム２５０の制御エンティティとすることができ、別の鉄道会社をＳＰＩサブシステム２９０の制御エンティティとすることができる。運用エンティティサブシステム４００と第１のＳＰＩサブシステム２５０（及び／又は第２のＳＰＩサブシステム２９０）の間をインターフェースすることによって、ＳＰＡサブシステム２０２は、運用エンティティサブシステム４００及び各ＳＰＩサブシステムが直接相互作用しなければならないエンティティの数を減らすことができる。つまり、サービスプロバイダサブシステム２００の直接統合点を最小化するために、ＳＰＡサブシステム２０２は、種々のＳＰＩサブシステム及び／又は種々の運用エンティティサブシステムのためのアグリゲータの役割を果たすことができる。ＳＰＡサブシステム２０２は、ＳＰＡサーバ２０４を含み、ＳＰＡサブシステム２０２にとって一意でありうる１つ以上のＳＰＡ鍵１５７及び／又は少なくとも１つのＳＰＡ識別子１６７にアクセスするように図１Ａに示されているが、ＳＰＡサブシステム２０２の構成要素の１つ、一部又は全てを、デバイス１００のプロセッサ構成要素１０２と同一若しくは類似でありうる１つ以上のプロセッサ構成要素、デバイス１００のメモリ構成要素１０４と同一若しくは類似でありうる１つ以上のメモリ構成要素、及び／又はデバイス１００の通信構成要素１０６と同一若しくは類似でありうる１つ以上の通信構成要素を使用して実施してもよい。第１のＳＰＩサブシステム２５０は、ＳＰＩサーバ２１０、ＳＰＩバス２１８、ＳＰＩ端末２２０を含み、第１のＳＰＩサブシステム２５０にとって一意でありうる１つ以上のＳＰＩ鍵１５５ａ及び／又は少なくとも１つのＳＰＩ識別子２６７にアクセスするように図１Ａに示されているが、第１のＳＰＩサブシステム２５０の構成要素の１つ、一部又は全てを、デバイス１００のプロセッサ構成要素１０２と同一若しくは類似でありうる１つ以上のプロセッサ構成要素、デバイス１００のメモリ構成要素１０４と同一若しくは類似でありうる１つ以上のメモリ構成要素、及び／又はデバイス１００の通信構成要素１０６と同一若しくは類似でありうる１つ以上の通信構成要素を使用して実施してもよい。同様に、第２のＳＰＩサブシステム２９０は、ＳＰＩサーバ、ＳＰＩバス、ＳＰＩ端末を含み、第２のＳＰＩサブシステム２９０にとつ

10

20

30

40

50

て一意でありうる1つ以上のSPI鍵及び／又は少なくとも1つのSPI識別子にアクセスすることができ、第2のSPIサブシステム290の構成要素の1つ、一部又は全てを、デバイス100のプロセッサ構成要素102と同一若しくは類似でありうる1つ以上のプロセッサ構成要素、デバイス100のメモリ構成要素104と同一若しくは類似でありうる1つ以上のメモリ構成要素、及び／又はデバイス100の通信構成要素106と同一若しくは類似でありうる1つ以上の通信構成要素を使用して実施してもよい。SPAサブシステム202と第1のSPIサブシステム250が別々のサブシステムである場合、好適な任意の通信経路75を使用して、それらの間でデータを通信することができる。加えて又は代わりに、SPAサブシステム202と第2のSPIサブシステム290が別々のサブシステムである場合、好適な任意の通信経路85を使用して、それらの間でデータを通信してもよい。

10

【0024】

示していないが、金融機関サブシステム350は、決済ネットワークサブシステム（例えば、決済カード機構又はクレジットカード機構）及び／又は発行用バンクサブシステムを含んでもよい。デバイス100のNFC構成要素120の1つ以上の特定の金融機関又は決済資格アプレット（例えば、セキュアエレメント145の金融機関SSD154bの金融機関アプレット153b）を、金融機関サブシステム350により具体的なユーザの1つ又は複数のアカウント（例えば、種々のタイプの決済カードのアカウントは、クレジットカード、デビットカード、チャージカード、記憶価値カード（例えば、トランジットカード）、フリーカード、ギフトカード、その他を含みうる）に電子的にリンクされうる特定の決済資格と関連付けることができる。このような決済資格を、（例えば、運用エンティティサブシステム400を介して）金融機関サブシステム350により（例えば、SSD154bのアプレット153bの金融機関資格情報として）デバイス100上に提供することができ、（例えば、商品若しくはサービス又はサービスプロバイダ資格データ（例えば、SPVデータ）のために支払うために）サービスプロバイダサブシステム200との取引に資金提供するためのデバイス注文データの少なくとも一部分としてデバイス100により後で使用することができる。

20

【0025】

システム1内で生じるいくつかの取引のために、少なくとも1つの取引資格（例えば、サービスプロバイダ資格及び／又は金融機関資格）を、デバイス100上に（例えば、アプレット153の資格情報として）例えば、電子デバイス100のセキュアエレメント145上に、及び／又は他の好適な任意のメモリ部分（例えば、サービスプロバイダ資格データ123として）例えば、メモリ構成要素104）上に）提供することができる。例えば、このような資格を、サービスプロバイダ資格データ123として、（例えば、通信経路15を介して又はサービスプロバイダサブシステム200とデバイス100の間の通信5として）サービスプロバイダサブシステム200から直接的にデバイス100のメモリ104に、又はSPアプレット153aのSP資格情報として（例えば、運用エンティティサブシステム400を介して）セキュアエレメント145上に、少なくとも部分的に提供することができる。好適な任意の資格データを、セキュアエレメントの資格追加セキュリティドメインの少なくとも一部分又は全体としてデバイス100のセキュアエレメント145上に提供することができ、資格データは、資格情報及び資格鍵155aを有する資格アプリケーション又は資格アプレット153aなどの、資格情報及び／又は資格鍵を有する資格アプレットを含むことができる。このような取引資格を、次いで、SP製品の取引（例えば、サービスプロバイダの具体的な商品若しくはサービス又はSPアプレット153a上の新たなSP資格情報を定義するための新たなSPVデータへのアクセス）に資金提供するように機能しうるデバイス取引データの少なくとも一部分を定義するために使用することができる。

30

40

【0026】

運用エンティティサブシステム400を、デバイス100とサービスプロバイダサブシステム200及び／又は他の任意のリモートサブシステム（例えば、金融機関サブシステ

50

ム 3 5 0) の間の仲介役として提供することができ、資格がデバイス 1 0 0 上に提供されるときに及び／又はそのような提供された資格がデバイス 1 0 0 とサービスプロバイダサブシステム 2 0 0 の間の資格データ通信の一部として使用されるときに、新たなセキュリティ層を提供するように、及び／又はよりシームレスなユーザエクスペリエンスを提供するように、運用エンティティサブシステム 4 0 0 を構成することができる。ユーザ固有のアカウントに対するユーザ固有のログイン情報（例えば、ユーザ固有の識別とパスワードの組合せ）により種々のサービスをデバイス 1 0 0 のユーザに供与しうる特定の運用エンティティにより運用エンティティサブシステム 4 0 0 を提供することができる。単なる一例として、運用エンティティサブシステム 4 0 0 を、カリフォルニア州クパチーノの Apple Inc. により提供することができ、デバイス 1 0 0 のユーザへの種々のサービスのプロバイダ（例えば、デバイス 1 0 0 により再生されるメディアを販売／賃貸する iTunes（登録商標）Store、デバイス 1 0 0 上で使用するアプリケーションを販売／賃貸する Apple App Store（登録商標）、デバイス 1 0 0 からのデータを記憶し並びに／又は複数のユーザデバイス及び／若しくは複数のユーザプロフィールを互いに関連付ける Apple iCloud（登録商標）Service、種々の Apple 製品をオンラインで購入する Apple Online Store、デバイス間でメディアメッセージを通信する Apple iMessage（登録商標）Service など）とすることもでき、デバイス 1 0 0 自体（例えば、デバイス 1 0 0 が iPod（登録商標）、iPad（登録商標）、iPhone（登録商標）その他であるとき）及び／若しくはデバイス 1 0 0 のオペレーティングシステム（例えば、デバイスアプリケーション 1 0 3）のプロバイダ、製造者、並びに／又は開発者とすることもできる。運用エンティティサブシステム 4 0 0 を提供しうる運用エンティティ（例えば、Apple Inc.）を、任意のリモート金融機関サブシステム 3 5 0 の任意の金融エンティティとは別個の独立したものとすることができる。例えば、運用エンティティサブシステム 4 0 0 を提供しうる運用エンティティを、金融エンティティサブシステム 3 5 0 によりエンドユーザデバイス 1 0 0 上に提供される任意のクレジットカード又は他の任意の決済資格を供給及び／又は管理しうる任意の決済ネットワーク又は発行用バンクとは別個及び／又は独立したものとすることができる。加えて又は代わりに、運用エンティティサブシステム 4 0 0 を提供しうる運用エンティティ（例えば、Apple Inc.）を、エンドユーザデバイス 1 0 0 上に提供される任意の SP 資格データを供給及び／又は管理しうるサービスプロバイダサブシステム 2 0 0 の任意のサービスプロバイダとは別個の独立したものとすることもよい。例えば、運用エンティティサブシステム 4 0 0 を提供しうる運用エンティティを、非接触近接ベース通信用のサービスプロバイダ端末、オンライン通信用のサービスプロバイダサーバ及び／又はサードパーティアプリケーション若しくはオンラインリソース 1 1 3、及び／又は他の任意の態様のサービスプロバイダサブシステム 2 0 0 を提供しうる、サービスプロバイダサブシステム 2 0 0（例えば、SPA サブシステム 2 0 2、SPI サブシステム 2 5 0、及び／又は SPI サブシステム 2 9 0）の任意のサービスプロバイダとは別個の及び／又は独立したものとすることができる。このような運用エンティティは、ユーザがサービスプロバイダサブシステム 2 0 0 又は他の任意のリモートサブシステムにより供与される資格をデバイス 1 0 0 に提供したいときに、及び／又はそのような提供された資格が取引を行うためにサービスプロバイダサブシステム 2 0 0 との資格データ通信の一部として使用されるときに、よりシームレスなユーザエクスペリエンスをデバイス 1 0 0 のユーザに提供するために、その潜在的な能力を活用して、デバイス 1 0 0 の種々の構成要素（例えば、その運用エンティティがデバイス 1 0 0 を少なくとも部分的に製造又は管理しうるときなどに、デバイス 1 0 0 のソフトウェア及び／又はハードウェア構成要素）を構成又は制御することができる。例えば、一部の実施形態では、（例えば、デバイス 1 0 0 上に資格データを提供する間に、及び／又はデバイス 1 0 0 とサービスプロバイダサブシステム 2 0 0 の間のオンラインベースのセキュリティ保護されたデータ通信の間に）より高いレベルのセキュリティを可能にしうるいくつかのデータを共有及び／又は受信するために、（例えば、通信経路 2 5 を介して）運用エンティティサブシステム 4

10

20

30

40

50

00とデバイス100のユーザにとってシームレスにかつトランスペアレントに通信するように、デバイス100を構成することができる。示していないが、運用エンティティサブシステム400は、図1A及び図2の電子デバイス100のプロセッサ構成要素102と同一若しくは類似でありうるプロセッサ構成要素、図1A及び図2の電子デバイス100の通信構成要素106と同一若しくは類似でありうる通信構成要素、図2の電子デバイス100のI/Oインターフェース114と同一若しくは類似でありうるI/Oインターフェース、図1A及び図2の電子デバイス100のバス118と同一若しくは類似でありうるバス、図2の電子デバイス100のメモリ構成要素104と同一若しくは類似でありうるメモリ構成要素、及び／又は図2の電子デバイス100の電源構成要素108と同一若しくは類似でありうる電源構成要素を含むこともでき、それらの1つ、一部又は全てを、サーバ410により少なくとも部分的に提供することができる。

10

【0027】

記述したように、デバイス100がサービスプロバイダサブシステム200との取引をより安全に行うことを可能にするために、運用鍵155cを有する運用SSD154cをデバイス100のセキュアエレメント145上又はメモリ構成要素104上に提供することもできる。運用エンティティサブシステム400は、（例えば、デバイス100により運用鍵155cを使用して暗号化されたデータを解読するために）運用鍵155cにアクセスすることもできる。運用エンティティサブシステム400は、鍵155cの管理を担当することができ、管理は、そのような鍵の生成、交換、記憶、使用、及び置換を含むことができる。運用エンティティサブシステム400は、運用エンティティサブシステム400のセキュアエレメントに、そのバージョンの鍵155cを記憶することができる。鍵155cを有するデバイス100の運用SSD154cを、（例えば、バイOMETリック入力構成要素などの、デバイス100の1つ以上の入力構成要素110を介して）デバイス100のユーザの意向及びローカル認証を決定するように構成することができ、そのような決定に応じて、（例えば、デバイス100の資格SSDのサービスプロバイダ資格及び／又は金融機関資格によって）取引を行うために別の具体的なSSDを有効化するように構成することができる。このような運用SSDをデバイス100上に記憶することによって、取引に対するユーザの意向及び取引の認証を確実に決定するその能力を高めることができる。その上、デバイス100のセキュアエレメントの外部又はデバイス100自体の外部に通信されうる取引データの暗号化を高めるために、デバイス100のこのような運用SSDの鍵155cにより提供されるアクセスデータを活用することができる。加えて又は代わりに、このようなアクセスデータは、電子デバイス100のISD152の発行者セキュリティドメイン（「ISD」）鍵156kを含んでもよく、その鍵は、運用エンティティサブシステム400により保持されてもよく、鍵155cに加えて又は鍵の代わりに使用されてもよい。

20

30

【0028】

サービスプロバイダアプリケーション又はオンラインリソース113には、デバイス100とサービスプロバイダサブシステム200の間でオンライン取引（例えば、データ取引、商業取引、購入取引、金融取引など）を促進することを可能にするために、又はデバイス100の他の好適なセキュリティ保護された任意のデバイス機能へのサービスプロバイダサブシステム200によるオンラインアクセスを可能にするために、デバイス100によりアクセスすることができる。アプリケーション113がデバイス100により効果的に利用可能となる前に、初めに、このようなアプリケーション113を運用エンティティサブシステム400により承認し、登録し、そうでなければ有効化することができる。例えば、運用エンティティサブシステム400のアプリケーションストア420（例えば、Apple App Store（登録商標））は、アプリケーション113を表す少なくとも一部のデータを通信経路35を介してサービスプロバイダサブシステム200から受信することができる。その上、一部の実施形態では、運用エンティティサブシステム400は、SPAサブシステム200（例えば、アプリケーション113又はサブシステム202全体）のサービスプロバイダ鍵（例えば、SPA鍵157）を生成し、そうでな

40

50

れば割り当てることができ、そのようなサービスプロバイダ鍵157を（例えば、経路35を介して）サービスプロバイダサブシステム200に提供することができる。代わりに、サービスプロバイダサブシステム200は、SPAサブシステム200（例えば、アプリケーション113又はサブシステム202全体）のサービスプロバイダ鍵157を生成し、そうでなければ割り当ててもよく、そのようなサービスプロバイダ鍵157を（例えば、経路35を介して）運用エンティティサブシステム400に提供してもよい。サービスプロバイダサブシステム200又は運用エンティティサブシステム400のいずれかは、サービスプロバイダ鍵157の管理を担当することができ、管理は、そのような鍵の生成、交換、記憶、使用、及び置換を含むことができる。このようなサービスプロバイダ鍵157をどのように又はどこで生成及び／又は管理しうるかにかかわらず、サービスプロバイダサブシステム200と運用エンティティサブシステム400の両方は、サービスプロバイダ鍵157のバージョンを記憶することができる（例えば、サービスプロバイダサブシステム200及び運用エンティティサブシステム400のそれぞれのセキュアエレメントに、一部の実施形態では、サービスプロバイダサブシステム200により記憶されるサービスプロバイダ鍵157を秘密鍵とすることができ、運用エンティティサブシステム400により記憶されるサービスプロバイダ鍵157を（例えば、非対称鍵暗号化／解読処理に使用するための）対応する公開鍵とすることができ、一部の実施形態では、このようなサービスプロバイダ鍵157を、特にサービスプロバイダアプリケーション113及び／又はサービスプロバイダ資格と関連付けることができ、他の実施形態では、サービスプロバイダ鍵157を複数のサードパーティアプリケーション若しくはウェブリソース又はサービスプロバイダサブシステム200の同一のサービスプロバイダ（例えば、複数のSPIサブシステム）の資格と関連付けうるように、サービスプロバイダ鍵157を特にサービスプロバイダサブシステム200（例えば、SPAサブシステム202）のサービスプロバイダと関連付けることができる。一意のサービスプロバイダ識別子167を生成し、及び／又はそうでなければ運用エンティティサブシステム400及び／又はサービスプロバイダサブシステム200によりアプリケーション113及び／又は1つ以上のサービスプロバイダ資格及び／又はSPサブシステムに割り当て、又はそれらと関連付けることができる。例えば、サービスプロバイダ（又は売買業者）識別子167は、英数字列、ドメイン（例えば、URL、そうでなければウェブリソースタイプのオンラインリソースアプリケーション113用の）、又はサービスプロバイダ（例えば、SPAサブシステム202）及び／又は具体的なサービスプロバイダのオンラインリソース及び／又は具体的なサービスプロバイダ資格を一意に識別しうる（例えば、それらを運用エンティティサブシステム400に対して一意に識別する）他の好適な任意の識別子とすることができる。具体的なサービスプロバイダ鍵157をサービスプロバイダアプリケーション113又はサービスプロバイダ資格又はサービスプロバイダエンティティ（例えば、SPAサブシステム202）の具体的なサービスプロバイダ識別子167と関連付けるために、運用エンティティサブシステム400にとってアクセス可能でありうるテーブル430又は他の好適な任意のデータ構造又は情報ソースを提供することができる。サービスプロバイダのオンラインリソースを具体的なサービスプロバイダ識別子167及び具体的なサービスプロバイダ鍵157と関連付けることができ、それらのそれぞれをサービスプロバイダサブシステム200と運用エンティティサブシステム400の間で安全に共有することができる。テーブル430は、デバイス100がサービスプロバイダアプリケーション113又はデバイスアプリケーション103を介してサービスプロバイダサブシステム200とインターフェースすることを伴いうる取引、そうでなければ鍵157及びサービスプロバイダ識別子167と関連付けられうる取引のために、サービスプロバイダサブシステム200に通信されるセキュリティ保護された任意のデバイスデータ（例えば、デバイス100にとってネイティブな金融機関決済資格データ及び／又はSP資格データを含みうる資格データ）にセキュリティ層を提供するために、運用エンティティサブシステム400が適切なサービスプロバイダ鍵157を決定及び利用すること可能にすることができる。（例えば、通信経路25を介してアプリケーションストア420から）アプリケーション11

10

20

30

40

50

3 にアクセスし、（例えば、プロセッサ 102 により）アプリケーション 113 を実行するようにデバイス 100 を構成することができる。代わりに又は加えて、サービスプロバイダ鍵 157 及びサービスプロバイダ識別子 167 を、サービスプロバイダのサードパーティネイティブアプリケーションではなく又はそれに加えて、サービスプロバイダのウェブサイト（例えば、本明細書ではサービスプロバイダオンラインリソース、一部の実施形態ではサービスプロバイダアプリケーションと呼ばれる 1 つ以上の URL 又はドメイン）又はサービスプロバイダ全体と関連付けてもよい。例えば、サービスプロバイダサブシステム 200 のサービスプロバイダは、具体的なサービスプロバイダウェブサイト又はサービスプロバイダ全体をテーブル 430 内の具体的なサービスプロバイダ鍵 157 及びサービスプロバイダ識別子 167 と関連付けるために運用エンティティサブシステム 400 と協働することができ、それにより、運用エンティティサブシステム 400 が、取引のためにサービスプロバイダサブシステム 200 に通信されるセキュリティ保護された任意のデバイスデータ（例えば、デバイス 100 にとってネイティブな資格データを含む資格データ）にセキュリティ層を提供するために、適切なサービスプロバイダ鍵 157 を決定及び利用することを可能にすることができ、取引は、ターゲット又はウェブリソースがそのサービスプロバイダ鍵 157 及びサービスプロバイダ識別子 167 と関連付けられる URL 又はドメイン（例えば、そのウェブリソース（例えば、store.program.provider.com）の一意のドメイン）に向けられうる、デバイス 100 上で実行中のインターネットアプリケーション又はウェブブラウザを介した取引を行うためにデバイス 100 がサービスプロバイダサーバ 210 とインターフェースすることを伴いうる。このような URL に、（例えば、このようなサービスプロバイダウェブリソースをターゲットにするとときにサービスプロバイダオンラインリソースを考慮しうる、デバイス 100 上のインターネットアプリケーション 113 を使用して）、例えば、通信経路 15 を介してサービスプロバイダサーバ 210 からアクセスするようにデバイス 100 を構成することができる。他の実施形態では、アプリケーション 113 を、特定のサービスプロバイダ、サービスプロバイダサブシステム 200、サービスプロバイダ鍵 157、及び／又はサービスプロバイダ識別子 167 と関連付けなくてもよいが、代わりに、そのようなサービスプロバイダウェブリソースをターゲットとするウェブ表示によりデバイス 100 にとって利用可能であり、それによりサービスプロバイダオンラインリソースの役割を果たす独立したアプリケーションとすることができる。運用エンティティサブシステム 400 によるサービスプロバイダオンラインリソースのこのような登録（例えば、サービスプロバイダサブシステム 200 と運用エンティティサブシステム 400 の間におけるサービスプロバイダ鍵 157 及びサービスプロバイダ識別子 167 のセキュリティ保護されかつ有効にされた（例えば、テーブル 430 に記憶するための）共有）を、サービスプロバイダサブシステム 200 がオンラインリソースの確認された所有者であることを運用エンティティサブシステム 400 に保証するような好適な任意の方法で行うことができる。したがって、サービスプロバイダオンラインリソース（例えば、ネイティブアプリケーション、ドメイン／URL、又は他の好適な任意のウェブリソース、又は恐らくはサービスプロバイダ端末でさえ）及び／又はサービスプロバイダ資格及び／又はサービスプロバイダサブシステム（例えば、SPA サブシステム 202）を、（例えば、図 5 の処理 500 の動作 502 にて登録中に）具体的なサービスプロバイダ識別子 167 及び少なくとも 1 つの具体的なサービスプロバイダ鍵 157 と関連付けることができ、それらのそれぞれを好適な任意の方法でサービスプロバイダサブシステム 200 と運用エンティティサブシステム 400 の間で安全に共有することができ、そのような関連付けを、（例えば、運用エンティティサブシステム 400 とサービスプロバイダサブシステム 200（例えば、SPA サブシステム 202 など）の間のセキュリティ保護された通信を可能にするために）共有秘密として使用するために（例えば、テーブル 430 において）運用エンティティサブシステム 400 にとってアクセス可能にすることができる。

【0029】

図 3 に示すように、また以下でより詳細に説明するように、電子デバイス 100 の特定

10

20

30

40

50

の例は、iPhone（登録商標）などのハンドヘルド電子デバイスとすることができ、筐体101は、デバイス100とユーザ及び／又は周辺環境とが互いにインターフェースしうる、種々の入力構成要素110a～110i、種々の出力構成要素112a～112c、及び種々のI/O構成要素114a～114dへのアクセスを可能にすることができる。例えば、タッチスクリーンI/O構成要素114aが、表示出力構成要素112a及び関連するタッチ入力構成要素110fを含むことができ、ユーザが電子デバイス100と対話することを可能にしうる視覚又はグラフィックユーザインターフェース（「GUI」）180を表示するために、表示出力構成要素112aを使用することができる。GUI180は、表示出力構成要素112aの領域の全て又は一部に表示されうる現在実行中のアプリケーション（例えば、アプリケーション103及び／又はアプリケーション113及び／又はアプリケーション143）の種々のレイヤ、ウィンドウ、画面、テンプレート、要素、メニュー、及び／又は他の構成要素を含むことができる。例えば、図3に示すように、GUI180の1つ以上のグラフィック要素又はアイコン182を有する画面190を表示するように、GUI180を構成することができる。特定のアイコン182が選択されると、そのアイコン182と関連付けられた、サービスプロバイダオンラインリソースアプリケーションなどの新たなアプリケーションを開き、そのアプリケーションと関連付けられたGUI180の対応する画面を表示するように、デバイス100を構成することができる。例えば、「S.P.App」テキストインジケータ181がラベル付けされた特定のアイコン182（すなわち、特定のアイコン183）がデバイス100のユーザにより選択されると、デバイス100は、特定のサードパーティサービスプロバイダアプリケーション（例えば、ネイティブアプリケーション又はハイブリッドアプリケーション）を起動し、そうでなければそのアプリケーションにアクセスしてもよい。別の例として、「インターネット」テキストインジケータがラベル付けされた特定のアイコン182（すなわち、特定のアイコン184）がデバイス100のユーザにより選択された場合、デバイス100は、別のタイプのサービスプロバイダオンラインリソースをデバイス100に提供するための特定のサードパーティサービスプロバイダのウェブリソースのURLに向けられうるインターネットブラウザアプリケーションを起動し、そうでなければそのアプリケーションにアクセスしてもよい。別の例として、「ウォレット」テキストインジケータがラベル付けされた特定のアイコン182（すなわち、特定のアイコン185）がデバイス100のユーザにより選択されると、デバイス100は、ユーザ用のUIが、（例えば、金融機関資格と単一のデバイス上のSP資格の間又は異なる2つのデバイス上の2つのSP資格の間その他の）具体的なタイプの取引のための資格データを生成することを可能にしうる、カード又はパス又は資格管理アプリケーション（例えば、ウォレット又は銀行通帳アプリケーション（例えば、アプリケーション103））を起動し、そうでなければそのアプリケーションにアクセスしてもよい。任意のアプリケーションがアクセスされると、デバイス100は、特定の 방법으로デバイス100を使用して、そのアプリケーションと対話するための1つ以上のツール又は機能を含みうる、特定のユーザインターフェースの画面を表示するように機能することができる（デバイス100のセキュリティ保護された任意の取引を行う（例えば、デバイス100の決済及び／又はSP資格（例えば、資格SSD154a及び／又はSSD154bの資格）によりサービスプロバイダサブシステム200への取引を行う）ためにデバイスユーザにより使用されうる好適な任意のアプリケーション（例えば、サービスプロバイダオンラインリソース113）を使用中のGUI180のそのような表示の特定の例については、例えば、図3A～図3Eを参照されたい）。各アプリケーションのために、表示出力構成要素112aに画面を表示することができ、画面は、種々のユーザインターフェース要素を含むことができる。加えて又は代わりに、各アプリケーションのために、他の種々のタイプの非視覚情報を、デバイス100の他の種々の出力構成要素112を介してユーザに提供してもよい。例えば、一部の実施形態では、デバイス100は、GUIを提供するように機能するユーザインターフェース構成要素を含まなくてもよいが、代わりに、サービスプロバイダサブシステム200との取引を行うための及び／又はデバイス100の他の好適なセキュリティ保護された

10

20

30

40

50

任意の機能を行うための、決済資格及び／又はロイヤルティ資格の使用を選択及び認証するために、オーディオ出力構成要素及び機械的な若しくは他の好適なユーザ入力構成要素を提供することができる。

【0030】

つぎに図4を参照すると、図4は、システム1の運用エンティティサブシステム400の具体的な実施形態に関する更なる詳細を示している。図4に示すように、運用エンティティサブシステム400は、セキュリティ保護されたプラットフォームシステムとすることができ、セキュリティ保護されたモバイルプラットフォーム（「SMP」）ブローカ構成要素440、SMP信頼されたサービスマネージャ（「TSM」）構成要素450、SMP暗号サービス構成要素460、識別管理システム（「IDMS」）構成要素470、不正システム構成要素480、ハードウェアセキュリティモジュール（「HSM」）構成要素490、ストア構成要素420、及び／又は1つ以上のサーバ410を含むことができる。運用エンティティサブシステム400の1つ、一部又は全ての構成要素を、デバイス100のプロセッサ構成要素102と同一若しくは類似でありうる1つ以上のプロセッサ構成要素、デバイス100のメモリ構成要素104と同一若しくは類似でありうる1つ以上のメモリ構成要素、及び／又はデバイス100の通信構成要素106と同一若しくは類似でありうる1つ以上の通信構成要素を使用して実施することができる。運用エンティティサブシステム400の1つ、一部又は全ての構成要素を、任意の金融機関サブシステム及び／又はサービスプロバイダサブシステム200とは別個の独立したものでありうる単一の運用エンティティ（例えば、Apple Inc.）により管理し、所有し、少なくとも部分的に制御し、及び／又はそうでなければ提供することができる。運用エンティティサブシステム400の構成要素は、新たなセキュリティ層及び／又はよりシームレスなユーザエクスペリエンスを提供するために、互いに相互作用することができ、好適な任意の金融機関サブシステム350及び／又は電子デバイス100及び／又はサービスプロバイダサブシステム200と集合的に相互作用することができる。

【0031】

運用エンティティユーザアカウントとのユーザ認証を管理するように、及び／又はサービスプロバイダサブシステムアカウントとのサービスプロバイダ妥当性検査を管理するように、運用エンティティサブシステム400のSMPブローカ構成要素440を構成することができる。デバイス100上の資格の寿命及び提供を管理するように、SMPブローカ構成要素440を構成することもできる。SMPブローカ構成要素440は、デバイス100上のユーザインターフェース要素（例えば、GUI180の要素）を制御しうる主エンドポイントとすることができ、エンドユーザデバイスのオペレーティングシステム又は他のアプリケーション（例えば、デバイス100のアプリケーション103、アプリケーション113、及び／又はアプリケーション143）を、特定のアプリケーションプログラムインターフェース（「API」）を呼び出すように構成することができ、それらのAPIの依頼を処理し、デバイス100のユーザインターフェースを導き出しうるデータで応答するように、及び／又は（例えば、運用エンティティサブシステム400と電子デバイス100の間の通信経路25を介して）デバイス100と通信しうるアプリケーションプロトコルデータユニット（「APDU」）で応答するように、SMPブローカ440を構成することができる。このようなAPDUを、システム1の信頼されたサービスマネージャ（「TSM」）（例えば、運用エンティティサブシステム400とリモートサブシステム（例えば、金融機関サブシステム350及び／又はSPサブシステム200）の間の通信経路のTSM）を介して金融機関サブシステム350から運用エンティティサブシステム400により受信することができる。GlobalPlatformベースのサービス、又は金融機関サブシステムによるデバイス100上への資格提供動作を行うために使用されうる他の好適な任意のサービスを提供するように、運用エンティティサブシステム400のSMP TSM構成要素450を構成することができる。GlobalPlatform又は他の好適なセキュリティ保護された任意のチャンネルプロトコルは、SMP TSM構成要素450が、運用エンティティサブシステム400とリモートサブシ

10

20

30

40

50

テムの間のセキュリティ保護されたデータ通信のためにデバイス100のセキュアエレメント145とTSMの間でデリケートなアカウントデータを適切に通信し及び／又は提供することを可能にする。

【0032】

HSM構成要素490を使用して、鍵を保護し、新たな鍵を生成するように、SMP TSM構成要素450を構成することができる。ユーザ認証及び／又はシステム1の種々の構成要素間の機密データ送信のために提供されうる、鍵管理及び暗号化動作をもたらすように、運用エンティティサブシステム400のSMP暗号サービス構成要素460を構成することができる。SMP暗号サービス構成要素460は、セキュリティ保護された鍵の記憶及び／又は不透明な暗号動作のためにHSM構成要素490を利用することができる。IDMS構成要素470と相互作用して、ファイル上のクレジットカードと関連付けられた情報又は運用エンティティのユーザアカウント（例えば、Apple iCloud（登録商標）アカウント）と関連付けられた他のタイプの商取引資格を取り出すように、SMP暗号サービス構成要素460の決済暗号サービスを構成することができる。このような決済暗号サービスを、メモリ内のそのユーザアカウントの商取引資格（例えば、クレジットカード番号）を記述する平文（例えば、ハッシュされていない）情報を有しうる、運用エンティティサブシステム400の唯一の構成要素となるように構成することができる。（例えば、商業エンティティ固有のサービス（例えば、Apple Inc. によるiMessage（登録商標））を使用して）識別サービス（「IDS」）移送など、デバイス100と別のデバイスの間の好適な任意の通信を可能にするように及び／又は管理するように、IDMS構成要素470を構成することができる。例えば、いくつかのデバイスを、このようなサービスのために自動又は手動で登録することができる（例えば、運用エンティティ400のエコシステム内の全てのデバイスを、サービスのために自動で登録することができる）。このようなサービスは、サービスを使用してメッセージが送信可能となる前に、アクティブな登録を要求しうるエンドツーエンド暗号化メカニズムを提供することができる。運用エンティティサブシステム400が、具体的なユーザアカウントと関連付けられた具体的なクライアントデバイス（例えば、運用エンティティサブシステム400とのファミリーアカウントの複数のデバイス）にとって利用可能でありうる1つ以上の非ネイティブ決済資格を効率的かつ効果的に識別するように機能しうるように、IDMS構成要素470及び／又は他の好適な任意のサーバ又は運用エンティティサブシステム400の一部分は、所与のユーザアカウント又は他のものと関連付けられた任意の電子デバイス上に提供された任意の資格の状況を識別するように、そうでなければ検索するように機能することができる。商取引資格及び／又はユーザについて運用エンティティが知っているデータ（例えば、運用エンティティによりユーザアカウントと関連付けられたデータ（例えば、商取引資格情報）、及び／又は運用エンティティの制御下にありうる他の好適な任意のデータ、及び／又はリモートサブシステムの制御下になくてもよい他の好適な任意のデータ）に基づいて、商取引資格に関する運用エンティティ不正検査を実行するように、運用エンティティサブシステム400の運用エンティティ不正システム構成要素480を構成することができる。種々の要因又は閾値に基づいて資格の運用エンティティ不正スコアを決定するように、運用エンティティ不正システム構成要素480を構成することができる。加えて又は代わりに、運用エンティティサブシステム400は、デバイス100のユーザへの種々のサービスのプロバイダでありうるストア420（例えば、デバイス100により再生されるメディアを販売／賃貸するiTunes（登録商標）Store、デバイス100上で使用するアプリケーションを販売／賃貸するApple App Store（登録商標）、デバイス100からのデータを記憶し及び／又は複数のユーザデバイス及び／又は複数のユーザプロフィールを互いに関連付けるApple iCloud（登録商標）Service、種々のApple製品をオンラインで購入するApple Online Storeなど）を含んでもよい。単なる一例として、アプリケーション113を管理し、デバイス100に（例えば、通信経路25を介して）提供するようにストア420を構成することができ、アプリケーション113は、銀行業務ア

10

20

30

40

50

アプリケーション、サービスプロバイダアプリケーション、電子メールアプリケーション、テキストメッセージングアプリケーション、インターネットアプリケーション、カード管理アプリケーション、又は他の好適な任意の通信アプリケーションなどの好適な任意のアプリケーションとすることができる。（例えば、図４の少なくとも１つの通信経路４９５を介して）運用エンティティサブシステム４００の種々の構成要素間でデータを通信するために、及び／又は運用エンティティサブシステム４００とシステム１の他の構成要素（例えば、図１の通信経路３５を介したサービスプロバイダサブシステム２００及び／又は図１の通信経路２５を介した電子デバイス１００）の間でデータを通信するために、好適な任意の通信プロトコル又は通信プロトコルの組合せを運用エンティティサブシステム４００により使用することができる。

10

【００３３】

図５は、電子デバイスとサービスプロバイダの間のセキュリティ保護された取引を管理するための例示的な処理５００のフローチャートである。電子デバイス１００、サービスプロバイダサブシステム２００、運用エンティティサブシステム４００、及び、任意選択で金融機関サブシステム３５０により処理５００を実施するように示している。しかし、他の好適な任意の構成要素又はサブシステムを使用して処理５００を実施してもよいことを理解されたい。処理５００は、電子デバイスとサービスプロバイダの間のセキュリティ保護された取引を安全かつ効率的に管理するためのシームレスなユーザエクスペリエンスを提供することができ、セキュリティ保護された取引は、サードパーティサービスプロバイダサブシステム２００のサービスプロバイダ資格を電子デバイス１００上に提供するための取引を含むことができ、電子デバイス１００上に提供されたそのようなサービスプロバイダ資格を、次いで、サービスプロバイダサブシステム２００の製品にアクセスするために使用することができる。図５の処理５００に従ってサービスプロバイダ資格を個人専用のものとするためのシステム１の動作に関する以下の議論を容易にするために、図１～図４の概略図のシステム１の種々の構成要素、及びそのような処理中のデバイス１００のグラフィックユーザインターフェース（例えば、カード又は資格管理アプリケーション（例えば、ウォレット又は銀行通帳アプリケーション（例えば、アプリケーション１０３））及び／又はサービスプロバイダオンラインリソース１１３又はデバイス１００の好適な任意のアプリケーションにより提供されうるようなＧＵＩ）を表しうる図３～図３Ｅの画面１９０～１９０の正面図が参照される。説明する動作は、広範なグラフィック要素及び視覚方式により実現されてもよい。したがって、図３～図３Ｅの実施形態は、本明細書にて採用するユーザインターフェース規則に厳密に限定されることを意図していない。むしろ、実施形態は、広範なユーザインターフェーススタイルを含んでもよい。サービスプロバイダサブシステム２００、及び／又はサービスプロバイダオンラインリソース又は鍵又はサーバ又は端末又は識別子又は資格などのその任意の特徴を記述するために用語「サービスプロバイダ」を利用しているが、サブシステム２００は、電子デバイス１００の所有者若しくはユーザ及び／又は運用エンティティサブシステム４００とは別個のものでありうる好適な任意のサードパーティエンティティにより動作される好適な任意のサブシステムでもよいことを理解されたい。例えば、サービスプロバイダサブシステム２００は、資格又はパスをデバイス１００上に提供するための取引を可能にしうる好適な任意のサードパーティサブシステム、及び／又は製品へのアクセスを与えるための取引（例えば、デバイス１００のオペレータに便益をもたらしうる取引）を推進するために、そのような資格又はパス情報をデバイス１００から受信しうる好適な任意のサブシステムとすることができる。

20

30

40

【００３４】

処理５００の動作５０１にて、ＳＰＡサブシステム２０２をＳＰサブシステム２００の各ＳＰＩサブシステムに（例えば、それらの間における好適な任意の登録データの通信によって）登録することができる。例えば、ＳＰサブシステム２００が第１のＳＰＩサブシステム２５０及び第２のＳＰＩサブシステム２９０を含みうる場合、それらのそれぞれは、ＳＰＡサブシステム２０２を介して運用エンティティサブシステム４００と通信するこ

50

とができ、次いで、SPAサブシステム202は、各SPIサブシステムに登録することができる。図5は第1のSPIサブシステム250をSPAサブシステム202に登録することを示しているにすぎないが、2つ以上のSPIサブシステムを単一のSPAサブシステム202に登録してもよいことを理解されたい（例えば、動作501にてSPIサブシステム290をSPAサブシステム202に登録してもよい）。SPAサブシステム202へのSPIサブシステムのこのような登録は、それらの間におけるデータのセキュリティ保護された将来の通信を可能にする好適な任意のデータを共有することを含むことができる（例えば、トランスポート層セキュリティ（「TLS」）を可能にするためなどに、登録動作501にて、SPAサブシステム202とSPIサブシステム250の間において（例えば、通信経路75を介して）少なくとも1つの共有秘密を通信することにより実現することができ、及び／又は、SPAサブシステム202とSPIサブシステム250の間における将来の通信を定義するために使用されうる1つ以上のAPIを定義するために、登録動作501にて、好適な任意のAPI仕様データをSPAサブシステム202とSPIサブシステム250の間で共有することができる）。

【0035】

処理500の動作502にて、SPサブシステム200（例えば、SPAサブシステム202）を運用エンティティサブシステム400に（例えば、それらの間における好適な任意の登録データの通信により）登録することができる。例えば、SPサブシステム200が、SPサブシステム200の1つ以上のSPIサブシステム（（例えば、動作501の登録による）例えば、第1のSPIサブシステム250及び／又は第2のSPIサブシステム290）のためのテクノロジープロバイダ又はサービスネーブラの役割を果たしうるSPAサブシステム202を含む場合、それらのそれぞれは、次いで、SPAサブシステム202を介して運用エンティティサブシステム400と通信することができ、次いで、SPAサブシステム202を運用エンティティサブシステム400に登録することができる。運用エンティティサブシステム400へのSPAサブシステム202のこのような登録は、それらの間におけるデータのセキュリティ保護された将来の通信を可能にする好適な任意のデータを共有することを含むことができる（例えば、登録動作502にて、（例えば、通信経路35を介して）SPAサブシステム202と運用エンティティサブシステム400の間で通信することにより少なくとも1つの共有秘密を実現することができる）。例えば、記述したように、動作502にて登録中に、SPAサブシステム202を具体的なサービスプロバイダ識別子167及び少なくとも1つの具体的なサービスプロバイダ鍵157と関連付けることができ、それらのそれぞれを好適な任意の方法でサービスプロバイダサブシステム200と運用エンティティサブシステム400の間で安全に共有することができ、（例えば、トランスポート層セキュリティ（「TLS」）を可能にするためなどに、運用エンティティサブシステム400とサービスプロバイダサブシステム200（例えば、SPAサブシステム202）の間のセキュリティ保護された通信を可能にするための）共有秘密として使用するために、そのような関連付けを（例えば、テーブル430において）運用エンティティサブシステム400にとってアクセス可能とすることができる。加えて又は代わりに、SPAサブシステム202と運用エンティティサブシステム400の間における将来の通信を定義するために使用されうる1つ以上のAPIを定義するために、登録動作502にて、好適な任意のAPI仕様データをSPAサブシステム202と運用エンティティサブシステム400の間で共有してもよい。

【0036】

処理500の動作504にて、運用エンティティサブシステム400を電子デバイス100に登録することができる。例えば、このような登録に影響を及ぼすために、動作504にて、運用エンティティサブシステム400により電子デバイス100のセキュアエレメント145上にアクセスデータ554を提供することができる。例えば、デバイス100がサービスプロバイダサブシステム200と取引をより安全に行うことを可能にするために、少なくとも部分的に運用エンティティサブシステム400（例えば、サーバ410）からのアクセスデータ554によりデバイス100のセキュアエレメント145上に少

10

20

30

40

50

なくとも1つのアクセス又は運用SSD（例えば、運用SSD154c）を提供することができる。記述したように、（例えば、次いで、（例えば、バス118を介して）通信構成要素106からセキュアエレメント145に渡されうる、運用エンティティサブシステム400のサーバ410とデバイス100の通信構成要素106の間の通信経路25を介したアクセスデータ554として）少なくとも部分的に運用エンティティサブシステム400から直接的に電子デバイス100のセキュアエレメント145上にSSD154cを提供することができる。経路25を介したアクセスデータ554は、SSD154cの少なくとも一部分又は全体としてデバイス100のセキュアエレメント145上に提供することができ、アプレット153c及び／又は鍵155cを含むことができる。（例えば、デバイス100がユーザに販売される前に運用エンティティサブシステム400により）
デバイス100が最初に構成されているときに、動作504を少なくとも部分的に行うことができる。代わりに、デバイス100のユーザがNFC構成要素120のセキュアエレメント145を最初にセットアップするのに応じて、動作504を少なくとも部分的に行ってもよい。加えて又は代わりに、アクセスデータ554は、セキュアエレメント145のISD152のISD鍵156kを含んでもよく、運用エンティティサブシステム400と電子デバイス100の間でセキュリティ保護された送信を可能にするために、鍵155cに加えて又はその代わりに（例えば、共有秘密として）使用されてもよい。アクセスデータ554と関連付けられうる、デバイス100と運用エンティティサブシステム400の間の共有秘密の任意の鍵は、トランスポート層セキュリティ（「TLS」）を可能にするためなどに、（例えば、運用エンティティサブシステム400のテーブル430において）共有秘密鍵と関連付けられうる、デバイス識別子119（例えば、デバイス100の一意の識別子（例えば、概してデバイス100識別子及び／又は具体的にはセキュアエレメント145の識別子（例えば、SEID）））を含むこともできる。（例えば、好適な任意のプッシュ又はプル方式で）デバイス100又は運用エンティティサブシステム400のいずれかにより動作504の通信を開始することができる。

【0037】

処理500の動作506にて、一部の実施形態では運用エンティティサブシステム400を介して、金融機関サブシステム350により電子デバイス100のセキュアエレメント145上に決済又は金融機関資格データ556を提供することができる。例えば、このような資格データ556を、金融機関サブシステム350から直接的に又は運用エンティティサブシステム400を介して電子デバイス100のセキュアエレメント145上に少なくとも部分的に提供することができる（例えば、金融機関サブシステム350と運用エンティティサブシステム400の間の図1Aの通信経路45を介して提供することができ、資格データを、運用エンティティサブシステム400（例えば、サーバ410）とデバイス100の通信構成要素106の間の図1Aの通信経路25を介して資格データ556としてデバイス100に渡すことができ、次いで、（例えば、バス118を介して）通信構成要素106からセキュアエレメント145に渡すことができる）。資格データ556は、金融機関資格SSD154bの少なくとも一部分又は全体としてデバイス100のセキュアエレメント145上に提供することができ、金融機関資格情報及び／又は資格鍵155bを有する資格アプレット153bを含むことができる。デバイス100のユーザが、（例えば、デバイス100上で実行中のオンラインリソース又は他の好適な任意のメカニズムを介して）デバイス100上に提供される具体的な決済又は金融機関資格を選択するときに、動作506を少なくとも部分的に行うことができる。一部の実施形態では、資格データ556は、運用エンティティサブシステム400から金融機関サブシステム350に最初に提供されうる、及び／又は（例えば、デバイス100へのデータ556の取引を保証するために）運用エンティティサブシステム400により追加されうる、運用鍵155cを含み、そうでなければ使用してもよい。デバイス100又は運用エンティティサブシステム400又は金融機関サブシステム350のいずれかによって、（例えば、好適な任意のプッシュ又はプル方式で）動作506の通信を開始することができる。

【0038】

動作506にて、資格データ556により定義されデバイス100上に提供されうる、SSD154bの金融機関資格情報は、その資格により決済を行う（例えば、SPサブシステム200との）例えば、取引に資金提供するために金融機関サブシステムの資金提供アカウントを識別する）のに必要なデータ、例えば、主アカウント番号（「PAN」）、カードセキュリティコード（例えば、カード認証コード（「CVV」））、PAN有効期限、資格と関連付けられた名称その他など、また電子デバイス100が適切な暗号データ（例えば、好適な任意の共有秘密及び共有秘密により機能的出力が少なくとも部分的に決定されうる好適な任意の暗号アルゴリズム又は暗号）を生成するように機能しうる他のデータを含むことができる。ユーザの「実際の」資格又は実際のPAN又は金融機関サブシステム350の実際のユーザアカウントの資金提供PAN（「F-PAN」）ではなく、

10

【0039】

処理500の動作508にて、サービスプロバイダサブシステム200により電子デバイス100のセキュアエレメント145上に、一部の実施形態では運用エンティティサブシステム400を介して、サービスプロバイダ資格データ558を提供することができる。例えば、このようなSP資格データ558を、サービスプロバイダサブシステム200から直接的に又は運用エンティティサブシステム400を介して、電子デバイス100のセキュアエレメント145上に少なくとも部分的に提供することができる（例えば、サービスプロバイダサブシステム200と運用エンティティサブシステム400の間で図1Aの通信経路35を介して部分的に提供することができ、SP資格データを、運用エンティティサブシステム400（例えば、サーバ410）とデバイス100の通信構成要素106の間で図1Aの通信経路25を介してSP資格データ558としてデバイス100に渡すことができ、次いで、（例えば、バス118を介して）通信構成要素106からメモリ104及び／又はセキュアエレメント145に渡すことができる）。SP資格データ558は、SP資格SSD154aの少なくとも一部分又は全体としてデバイス100のセキュアエレメント145上に提供することができ、SP資格情報及び／又はSP資格鍵155aを有する資格アプレット153aを含むことができる。代わりに又は加えて、SP資格データ558は、サービスプロバイダ資格データ123としてメモリ104上に少なくとも部分的に記憶されてもよい。デバイス100のユーザが、（例えば、デバイス100上で実行中のオンラインリソース又は他の好適な任意のメカニズムを介して）デバイス100に提供される具体的なSP資格を選択するときに、動作508を少なくとも部分的に行うことができる。一部の実施形態では、資格データ558は、運用鍵155cを含んでもよく、そうでなければ運用鍵を使用してもよく、運用鍵を、運用エンティティサブシステム400からSPサブシステム200に最初に提供することができ、及び／又は（例えば、デバイス100へのデータ558の取引を保証するために）運用エンティティサブシステム400により追加することができる。SP資格データ558は、デバイス100上に提供されたSP資格により適切に行われうる、非限定的に、SP資格に価値を加える、SP資格から価値を減らす、その他の1つ以上を含むアクションを定義するように、そうでなければ識別するように機能する好適な任意のデータ（例えば、アクションデータ又はパスデータ）、及び／又は、非限定的に、SP資格に加えられる最大価値を含む、そのようなアクションの好適な任意の特徴を定義しうる情報を含むことができ、それらを1つ以上のJavaScript Object Notation（「JSON」）ファイル（例えば、デバイス100のプロセッサ102上で実行中のカード管理アプリケーションを介して）例えば、いくつかの情報がデバイス100のユーザに提示されうるパスファイルでありうる、action.jsonなどの好適な任意の構造に含むことができる。デバイス100又は運用エンティティサブシステム400又はSPサブシステム200のいずれかによって、（例えば、好適な任意のプッシュ又はプル方式で）動作508の通信を開始することができる。SP資格データ（例えば、追加のSP資格データ又は動作508のSP資格データ558）をデバイス100上で更新しうる例示的な一方法について

20

30

40

50

は、処理500の動作510～549に関してより詳細に説明することができる。

【0040】

処理500の動作510にて、デバイス100は、デバイス100上のSP資格に価値を加える（例えば、デバイス100上に既に提供されたSP資格（例えば、動作508にて提供されたSP資格）に価値を加える又はいくつかの価値の新たなSP資格をデバイス100に加える）注文をユーザが生成し提出することを可能にするように機能することができる。図3A～図3Cに示すように、好適な任意のアプリケーション（例えば、デバイスアプリケーション103（例えば、カード管理（例えば、ウォレット）アプリケーション）又はサービスプロバイダオンラインリソース若しくはアプリケーション（例えば、アプリケーション113））を、SP資格価値をデバイスに加える具体的な注文を生成し提出するための1つ以上の選択肢をユーザに提示するためにデバイス100により実行することができる。例えば、図3Aに示すように、GUI180は、サービスプロバイダ資格価値を追加すべきか否かをユーザに尋ねるユーザクエリ301、及び応答選択肢303、305、307、及び309など、クエリ301に応答するためにユーザにより選択されうる1つ以上の好適な応答選択肢を提示しうる、画面190aを提供することができる。任意のSP資格価値の追加を断るために、応答選択肢303を選択することができる。デバイス100上に存在する「SP資格A」（例えば、動作508にてデバイス100上に提供されているSP資格）にSP資格価値を加えるために、応答選択肢305を選択することができる。デバイス100上にまだ提供されていない新たなSP資格にSP資格価値を加えるために、応答選択肢307を選択することができる。デバイス100以外のリモート受領側デバイス（例えば、システム1のクライアントデバイス100'（例えば、図1Aを参照））にSP資格価値を加えるために、応答選択肢309を選択することができ、好適な任意のリモート受領側デバイス識別子（ホストデバイス100のデバイス識別子119と同様に、（例えば、電話番号若しくは電子メールアドレス、又は（例えば、運用エンティティサブシステム400に関して）リモート受領側デバイスと一意に関連付けられうる他の方法）の使用によりリモート受領側デバイスを識別することができる。動作510は、好適な任意のデータフェッチ又は他の好適なサブ動作を含むことができ、1つ以上のSP資格についての更新情報を、（例えば、運用エンティティサブシステム400及び／又は（例えば、運用エンティティサブシステム400を介して）SPサブシステム200から）デバイス100により取得することができる。動作510にて、SP資格データ558による好適な任意のデータ（例えば、アクションデータ）を利用することができ、及び／又は好適な任意の選択肢を提示するために、又はデバイス100による注文の好適な任意の選択又は定義を可能にするために、動作510にて、任意の更新情報又は追加情報をフェッチすることができる。加えて、どのターゲットSP資格に価値を加えるかを（例えば、応答選択肢305～309の1つにより）潜在的に選択するための画面190aを提示する前又は提示した後に、GUI180は、図3Bに示すように、SP資格価値の追加にどのように資金提供するかをユーザに尋ねるユーザクエリ311、及びクエリ311に応答するためにユーザにより選択されうる、応答選択肢313、315、317、及び319などの1つ以上の好適な応答選択肢を提示しうる、画面190bを提示することができる。例えば、金融機関サブシステム350の異なる資金提供アカウントと関連付けられうる「FI資格A」又は「FI資格B」など、動作506にてデバイス100上に既に提供されている可能性がある具体的に存在する金融機関（「FI」）資格を選ぶために、応答選択肢313及び315の一方を選択することができる。加えて又は代わりに、SPサブシステム200（例えば、SPIサブシステム250及び／又はSPIサブシステム290）の異なるSP資格と関連付けられうる「SP資格A」又は「SP資格B」など、動作508にてデバイス100上に既に提供されている可能性がある具体的に存在するSP資格を選ぶために、応答選択肢317及び319の一方を選択してもよい。つぎに、（例えば、図3Aの応答選択肢305～309の1つにより）価値を加えるターゲットSP資格を選択し、かつ（例えば、図3Bの応答選択肢313～319の1つにより）新たなSP資格価値のための資金提供ソースを選択した後に、GUI180は、図3Cに示す

10

20

30

40

50

ように、選択肢 3 2 3（例えば、画面 1 9 0 a の応答 3 0 5、3 0 7、及び 3 0 9 の 1 つ）による価値を加えるためのターゲット S P 資格及び／又は選択肢 3 2 5（例えば、画面 1 9 0 b の応答 3 1 3、3 1 5、3 1 7、及び 3 1 9 の 1 つ）による資金提供資格の従前の選択をユーザが編集することを可能にするユーザクエリ 3 2 1 を提示しうる画面 1 9 0 c を提示することができる。その上、画面 1 9 0 c は、選択肢 3 2 7 にて、選択肢 3 2 3 のターゲット S P 資格に加えられる S P 価値（例えば、減らされうる \$ 8 0 の価値又は月間契約若しくは単一の交通パスなど）を選択する能力をユーザに提供することができる。代わりに又は加えて、画面 1 9 0 c は、選択肢 3 2 9 にて、選択肢 3 2 5 の資金提供資格により資金提供される資金提供量（例えば、所望の新たな S P 資格価値に資金提供するために必要となりうる具体的な貨幣価値）を選択する能力をユーザに提供してもよい。最後に、また動作 5 1 0 にて、図 3 C の画面 1 9 0 c は、ユーザを認証し、認証及び注文提出プロンプト 3 3 1 により選択肢 3 2 5 の選択された資金提供資格を利用するその意向を認証するための 1 つ以上の方法でデバイス 1 0 0 と対話することをユーザに促すことができる。認証プロンプト 3 3 1 の使用は、デバイス 1 0 0 のセキュアエレメントにアクセスし、よって、提出される S P 価値注文に資金提供するために使用される選択肢 3 2 5 の資金提供資格にアクセスするために、個人識別番号（「P I N」）の入力又は生体認証センサとのユーザ対話によるユーザ認証の入力をユーザに促すことを含むことができる。アクセス S S D 1 5 4 c は、他の S S D 1 5 4（例えば、選択肢 3 2 5 の選択された資金提供資格と関連付けられた資格 S S D 1 5 4）が、その資格情報を S P 価値に対するデバイス注文において資金提供情報として有効化するために使用することが可能となる前に、このような認証が生じたかどうかを判定するために、アプレット 1 5 3 c を活用することができる。動作 5 1 0 の単なる一例として、アクセス S S D 1 5 4 c のアプレット 1 5 3 c を、（例えば、G U I 1 8 0 を介してアプリケーションと対話するユーザにより使用されうる、図 3 のバイOMETリック入力構成要素 1 1 0 i などの 1 つ以上の入力構成要素 1 1 0 を介して）デバイス 1 0 0 のユーザの意向及びローカル認証を決定するように構成することができ、そのような決定に応じて、（例えば、資格 S S D 1 5 4 a 又は資格 S S D 1 5 4 b の資格により）S P 価値注文取引に資金提供するために別の具体的な S S D を有効化するように構成することができる。

【0 0 4 1】

動作 5 1 0 にて、具体的な注文のための認証情報が提供されると、処理 5 0 0 は、そのような認証情報及び（例えば、画面 1 9 0 c にて定義されるような）他の好適な任意の注文情報をプロセッサ 1 0 2 により注文依頼データ 5 6 2 としてセキュアエレメント 1 4 5 に提供しうる動作 5 1 2 に進むことができる。例えば、注文依頼データ 5 6 2 は、ユーザにより提供された好適な任意の認証情報のみならず、（例えば、選択肢 3 2 5（例えば、セキュアエレメント 1 4 5 上の F I 資格（例えば、アプレット 1 5 3 b）のアプレット識別子又はセキュアエレメント 1 4 5 上の S P 資格のアプレット識別子）の）資金提供資格の識別及び／又は（例えば、選択肢 3 2 9 の）資金提供量及び／又は（例えば、選択肢 3 2 3（例えば、セキュアエレメント 1 4 5 上の S P 資格（例えば、アプレット 1 5 3 a）のアプレット識別子及び／又は具体的な S P I サブシステムの識別子（例えば、S P I I D 2 6 7）及び／又は具体的な S P A サブシステムの識別子（例えば、S P A I D 1 6 7）及び／又は受領側デバイスの識別子（例えば、ホストデバイス 1 0 0 又はクライアントデバイス 1 0 0 ' のデバイス識別子）の）追加される価値のターゲット S P 資格及び／又は（例えば、選択肢 3 2 7 の）追加される具体的な価値も含むことができる。注文依頼データ 5 6 2 のいくつかの部分は、注文により使用する（例えば、更新する）ために具体的な S P 資格と関連付けられうる（例えば、S P 資格データ 5 5 8 の）好適な任意のアクションデータにより定義されうる 1 つ以上のアクション（例えば、価値の追加／補充）の選択を示すことができる。

【0 0 4 2】

つぎに、動作 5 1 4 及び 5 1 6 にて、処理 5 0 0 は、デバイス 1 0 0（例えば、セキュアエレメント 1 4 5）が決済データ 5 6 4 を生成し、暗号化し、注文応答データ 5 6 6 の

10

20

30

40

50

少なくとも一部分としてデバイス100のプロセッサ102に返信することを含むことができる。このような決済データ564を、動作512の注文依頼データ562により識別される資金提供資格（例えば、ユーザ注文シートの）例えば、画面190cの選択肢325の資金提供資格）の使用によるデバイス100からのSP価値注文に含まれる好適な任意の資金提供又は決済手段として生成することができる。デバイス100のセキュアエレメント145上の資金提供資格が、（例えば、資金提供資格の識別及び注文依頼データ562の認証情報に基づいて）資金提供手段を生成する際に使用するために選択され、認証され、及び／又は有効化されると、デバイス100のセキュアエレメント145（例えば、NFC構成要素120のプロセッサモジュール142）は、その選択された資金提供資格のいくつかの資格データを、運用エンティティサブシステム400による使用のために生成し暗号化することができる。例えば、選択された資金提供資格SSDのアプレットのセキュアエレメント（「SE」）資金提供資格データ（例えば、SSD154bの金融機関資格データ（例えば、金融機関サブシステム350の資金提供アカウントを確実に識別するように機能するトークンデータ及び暗号データ）又はSSD154aのSP資格データ（例えば、提供されたSP資格からの好適な任意の価値データ（例えば、貨幣価値又はいくつかのアクセスデータ））を、動作514にて、その資金提供資格SSDの資格鍵（例えば、鍵155a又は鍵155b）により、暗号化された資金提供資格データとして生成し、及び／又は少なくとも部分的に暗号化し、及び／又は符号化することができ、それにより、そのような暗号化された資金提供資格データを、生成された資金提供資格データにアクセスするために、その資格鍵へのアクセスを有するエンティティ（例えば、金融機関サブシステム350又はSPサブシステム200）のみにより、解読及び／又は復号することができるようになっている。この資金提供資格データは、SPサブシステム200（例えば、選択肢323により識別されSP資格に価値を加えることを担当するSPサブシステム）からの新たなSP資格価値の取得に資金提供するのに必要な全てのデータ、例えば、主アカウント番号（例えば、実際のF-PAN又は仮想のD-PAN）、カードセキュリティコード（例えば、カード認証コード（「C V V」））、有効期限、資格と関連付けられた名称、関連付けられた暗号データ（例えば、セキュアエレメント145と金融機関サブシステム350との間の共有秘密を使用して生成された暗号、及び他の好適な任意の情報）、及び／又は資金提供資格が金融機関資金提供資格であるときの同様のもの、又は資金提供資格がSP資格であるときの1つ以上の好適な価値スクリプトなどを含むことができる。一部の実施形態では、資金提供資格SSDのその資金提供資格データの一部又は全てが、動作514にて、決済データ564を提供しうる、その資金提供資格SSDの鍵により暗号化されると、その暗号化された資金提供資格データを、単独で又は他の好適な任意の注文データの一部である場合に注文依頼データ562の全てではなくても少なくとも一部分（例えば、（例えば、選択肢325（例えば、アプレット識別子）の）資金提供資格の識別及び／又は（例えば、選択肢329の）資金提供量及び／又は（例えば、選択肢323（例えば、具体的なSPIサブシステムの識別子（例えば、SPI ID267）及び／又は具体的なSPAサブシステムの識別子（例えば、SPA ID167）及び／又は受領側デバイスの識別子（例えば、ホストデバイス100又はクライアントデバイス100'のデバイス識別子））の追加された価値のターゲットSP資格及び／又は（例えば、選択肢327の）追加される具体的な価値の識別）と共に、動作514にて、決済データ564を提供しうる暗号化された運用エンティティ（「AE」）資金提供資格データとしてアクセス情報（例えば、アクセスSSD154cの運用鍵155c及び／又はISD152のISD鍵156k）により暗号化することができる。例えば、デバイス100のセキュアエレメント145（例えば、NFC構成要素120のプロセッサモジュール142）は、SP資格価値を加えるSPサブシステムの識別のみならず、資金提供量及び／又は資金提供される価値の量の識別、並びに資金提供資格SSDの暗号化された資金提供資格データを、決済データ564を提供するための暗号化されたAE資格データに暗号化するためにアクセス情報を使用することができる。一部の実施形態では、資金提供資格SSDの資金提供資格データを、アクセス鍵により暗号化する前に資格鍵により

10

20

30

40

50

暗号化せずに生成することができるが、代わりに、そのような資金提供資格データを、アクセス鍵により暗号化し、任意の資格鍵により暗号化されていない決済データ564として提供することができる。一部の実施形態では、このようなアクセス鍵は、運用エンティティサブシステム400の方式と関連付けられた運用エンティティ公開鍵とすることができ、その運用エンティティサブシステム400は、関連付けられた運用エンティティ秘密鍵（例えば、鍵155c）にアクセスすることができる。運用エンティティサブシステム400は、そのような運用エンティティ公開鍵を金融機関サブシステム350に提供することができ、金融機関サブシステム350は、（（例えば、処理500の動作506にて）例えば、金融機関資格データをデバイス100上に提供するときに）、次いで、その運用エンティティ公開鍵をデバイス100と共有することができ、及び／又はSPサブシステム200とSPサブシステム350は、（（例えば、処理500の動作508にて）例えば、SP資格データをデバイス100上に提供するときに）、次いで、その運用エンティティ公開鍵をデバイス100と共有することができる。

【0043】

つぎに、注文依頼データ562の少なくとも一部又は注文を示しうる他のものなどの追加の任意の情報（例えば、（例えば、選択肢325（例えば、アプレット識別子）の）資金提供資格の識別及び／又は（例えば、選択肢329の）資金提供量及び／若しくは（例えば、選択肢323（例えば、具体的なSPIサブシステムの識別子（例えば、SPI ID267）及び／又は具体的なSPAサブシステムの識別子（例えば、SPA ID167）及び／又は受領側デバイスの識別子（例えば、ホストデバイス100又はクライアントデバイス100'のデバイス識別子）の識別）の）追加された価値のターゲットSP資格及び／若しくは（例えば、選択肢327の）追加される具体的な価値及び／若しくは他の好適な任意の情報（例えば、デバイス100自体を識別する任意の情報、デバイスベースの一意の取引又は注文識別子、及び／又はその他）と共に、決済データ564を、動作516にて、注文応答データ566としてセキュアエレメント145からプロセッサ102に、並びに／又は、動作518にて、取引注文データ又はデバイス注文データ568としてプロセッサ102から運用エンティティサブシステム400と一緒に送信することができる。したがって、デバイス注文データ664の少なくとも一部分（例えば、暗号化されたAE資金提供資格データ）を、暗号化に使用されたそのアクセス情報（例えば、運用鍵155c及び／又はISD鍵156k）へのアクセスを有し、デバイス注文データ568の決済データ564の暗号化されたAE資金提供資格データを生成したエンティティ（例えば、運用エンティティサブシステム400）のみにより解読することができる。このようなデバイス注文データ568を、動作514～518にて生成し、次いで、（例えば、通信構成要素106及び通信経路25を介して）運用エンティティサブシステム400に送信することができる。動作514～518は、デバイス注文データ568の一部としてデバイス100のセキュアエレメント145により生成され送信される任意の資金提供資格データが、デバイス100の別の部分により解読できないような方法で、最初に暗号化されていることを保証することができる。つまり、デバイス注文データ568の資金提供資格データを、デバイス100のうちそのセキュアエレメントの外部の任意の部分に露出されず、その部分によりアクセスできない資金提供資格鍵により暗号化された資金提供資格データとして、暗号化することができる。その上、デバイス注文データ568のこのような暗号化された資金提供資格データを、デバイス100のうちそのセキュアエレメントの外部の任意の部分に露出されず、その部分によりアクセスできないアクセス鍵（（例えば、本明細書にて「アクセス情報」と呼ばれる）例えば、運用鍵155c及び／又は156k）により暗号化されたAE資金提供資格データとして、暗号化することができる。したがって、デバイス100から運用エンティティサブシステム400に通信されるデバイス注文データ568は、決済手段を識別する注文データ及び資金提供されるアイテムを識別する注文データを含みうる注文を定義することができ、決済手段を識別する注文データは、資金提供ソースを確実に識別するように機能しうる、決済データ564の資金提供資格データ（例えば、金融機関サブシステム350のユーザアカウント及び／又はSPサ

10

20

30

40

50

ブシステム 200 により提供される（例えば、選択肢 325 により識別されうる）SP 資格の記憶された価値）並びに資金提供のために使用される（例えば、選択肢 329 により識別されうるような）その資金提供ソースの価値の量を含むことができ、資金提供されるアイテムを識別する注文データは、SP 資格及びその SP 資格に加えられる価値を識別する、（例えば、選択肢 323 及び 327 により識別されうるような）好適な任意のデータとすることができ、そのデータは、SP サブシステムの好適な任意の SP 製品（例えば、商品又はサービス）、又は SP サブシステムの他の SP 製品にアクセスする際に使用するためにデバイス上並びにその価値に対して受領側デバイス（例えば、受領側デバイスの識別子（例えば、ホストデバイス 100 又はクライアントデバイス 100' のデバイス識別子）上に記憶される好適な任意の SP 資格価値を識別することができる。例えば、アイテムを識別する注文データは、購入されるアイテムを識別する記述（（例えば、選択肢 323 及び／又は選択肢 327 にて）例えば、ユーザにより入力及び／又は編集されうる記述及び／又はシステム 1（例えば、デバイス 100 及び／又はシステム 1 の他の好適な任意のサブシステム）により少なくとも部分的に生成されうる記述）など、注文によりどの SP 資格が購入される（例えば、資金提供される）かを指定するオブジェクトを定義するデータを含むことができ、（例えば、動作 502 にて）SPA サブシステム 202（例えば、SPA インプリメータ）及び／又は運用エンティティサブシステム 400 により定義されうるオブジェクト内に 1 つ以上の鍵を有するオブジェクトなど、具体的な注文についての状況を含むことができ、注文依頼を処理するために SPA サブシステム 202 により必要とされうる任意のデータを含むことができる。例えば、このようなオブジェクトは、アイテムタイプに固有であり運用エンティティサブシステム 400 と SPA サブシステム 202 の間の取決めとして定義されうる 1 つ以上の鍵を含むことができる。アイテムを識別する注文データは、注文により使用する（例えば、更新する）具体的な SP 資格と関連付けられうる（例えば、SP 資格データ 558 の）好適な任意のアクションデータにより定義されうる 1 つ以上のアクション（例えば、価値／補充の追加）の選択を示す好適な任意のデータを含むことができる。SP 資格のアクションデータのこのようなアクションを、注文を生成するためにデバイス 100 上で使用する前に、SP サブシステム 200 及び／又は運用エンティティサブシステム 400 により定義することができ、そのようなアクションデータは、処理 500 の注文及び価値取引を可能にする、SP サブシステム 200 と運用エンティティサブシステム 400 の間の取決めの一部分とすることができる。

【0044】

つぎに、処理 500 の動作 520 にて、運用エンティティサブシステム 400 は、デバイス注文データ 568 を受信し、運用注文データ 570 を生成するために処理することができる。例えば、運用エンティティサブシステム 400 は、デバイス注文データ 568 を受信することができ、次いで、運用エンティティサブシステム 400 にて利用可能なアクセス情報（例えば、鍵 155c 及び／又は鍵 156k（例えば、運用エンティティサブシステム 400 とデバイス 100 の間の共有秘密））を使用して、デバイス注文データ 568 の暗号化された AE 資金提供資格データを解読することができる。これにより、運用エンティティサブシステム 400 は、決済データ 564 の資金提供資格データを（例えば、暗号化された資金提供資格データとして）暗号化された状態に維持しながら、注文のターゲットとなりうるサービスプロバイダサブシステム（例えば、デバイス注文データ 568 内の好適な任意の SP 識別データ（例えば、選択肢 323 により識別されるターゲット SP と関連付けられうる SPI ID 267 及び／又は SPA ID 167）により識別されうる SP サブシステム 200）の暗号化されていない識別を決定することを可能にすることができる。これは、運用エンティティサブシステム 400 が、そのような資金提供資格データを決済データ 564 の暗号化された資金提供資格データとして動作 514 にてデバイス 100 のセキュアエレメント 145 により暗号化した資金提供資格鍵（例えば、鍵 155a 又は鍵 155b）へのアクセスを有しなくてもよいためである。加えて又は代わりに、注文のターゲットとなりうるサービスプロバイダサブシステム（例えば、ターゲット SP サブシステム）の識別を、決済データ 564（例えば、暗号化された資金提供資格デ

10

20

30

40

50

ータ）と共に注文応答データ５６６及び／又はデバイス注文データ５６８に含まれる追加のデータにより識別してもよい。デバイス注文データ５６８が運用エンティティサブシステム４００により受信されると、デバイス注文データ５６８の少なくとも一部分を解読するために、運用エンティティサブシステム４００が、どのアクセス情報（例えば、鍵１５５ｃ及び／又は鍵１５６ｋのどちらか）を動作５２０にて使用すべきかを知らうるよう、デバイス注文データ５６８は、デバイス１００又は少なくともそのセキュアエレメント１４５を識別する好適な任意の情報（例えば、デバイス識別子１１９）を含むことができる。例えば、運用エンティティサブシステム４００は、複数のアクセス鍵及び／又は複数のＩＳＤ鍵にアクセスすることができ、それらのそれぞれは、具体的なデバイス（例えば、ホストデバイス１００又はクライアントデバイス１００'）又は具体的なデバイスの具体的なセキュアエレメントに固有のものとして行うことができる。

10

【００４５】

つぎに、また処理５００の動作５２０にて、運用エンティティサブシステム４００は、注文のターゲットとなるサービスプロバイダサブシステムを（例えば、動作５２０におけるデバイス注文データ５６８の何らかの処理により）識別した後に、運用エンティティサブシステム４００は、その識別されたターゲットサービスプロバイダサブシステムと関連付けられうるＳＰ鍵（例えば、ＳＰＡ鍵１５７）を識別し、次いで、そのＳＰ鍵を使用してデバイス注文データ５６８の少なくとも一部分を再暗号化することができる。つまり、動作５２０にて、好適なアクセス情報を使用してデバイス注文データ５６８の少なくとも一部分を解読した後（例えば、決済データ５６４の暗号化されたＳＥ資金提供資格データ及びデバイス注文データ５６８に含まれる他の任意の情報を実現するためにデバイス注文データ５６８の暗号化されたＡＥ資金提供資格データを解読した後）に、運用エンティティサブシステム４００は、次いで、動作５２０にて、デバイス注文データ５６８内で識別されたターゲットＳＰ情報と関連付けられうる適切なＳＰ鍵１５７により、解読されたデバイス注文データ５６８（例えば、決済データ５６４の暗号化されたＳＥ資金提供資格データ）の少なくとも一部分を再暗号化することができる。例えば、このようなＳＰ鍵１５７を、デバイス注文データ５６８内で識別されたターゲットＳＰ識別子情報を運用エンティティサブシステム４００のテーブル４３０内のデータと比較することにより決定することができる。この決定された適切なＳＰ鍵１５７によって、運用エンティティサブシステム４００は、デバイス注文データ５６８の少なくとも一部分（例えば、決済データ５６４の暗号化されたＳＥ資金提供資格データ）を、暗号化されたＳＰ資金提供資格データとしてＳＰ鍵１５７で再暗号化することができる。このような暗号化されたＳＰ資金提供資格データを、動作５２０にて、運用注文データ５７０の少なくとも一部分として少なくとも部分的に生成することができ、次いで、そのような運用注文データ５７０を、動作５２２にてターゲットＳＰサブシステムに送信することができる。例えば、運用注文データ５７０は、このような暗号化されたＳＰ資金提供資格データ、及び、非限定的に、（例えば、選択肢３２５の）資金提供資格の識別並びに／又は（例えば、選択肢３２９の）資金提供量並びに／又は（例えば、選択肢３２３（例えば、具体的なＳＰＩサブシステムの識別子（例えば、ＳＰＩ ＩＤ２６７）及び／若しくは具体的なＳＰＡサブシステムの識別子（例えば、ＳＰＡ ＩＤ１６７）並びに／又は受領側デバイスの識別子（例えば、ホストデバイス１００又はクライアントデバイス１００'のデバイス識別子）の識別）の追加された価値のターゲットＳＰ資格並びに／又は（例えば、選択肢３２７の）追加される具体的な価値並びに／又は他の好適な任意の情報（例えば、デバイス１００自体を識別する任意の情報、デバイスベースの一意の取引若しくは注文識別子、運用エンティティサブシステム４００により生成された運用ベースの一意の取引若しくは注文識別子、及び／又はその他）を含む、デバイス注文データ５６８からの好適な任意のデータなどの他の好適な任意のデータを含むことができる。例えば、デバイス注文データ５６８は、ＳＰＡ ＩＤ１６７のみならずＳＰＩ ＩＤ２６７も含むことができるが、運用エンティティサブシステム４００は、運用注文データ５７０の暗号化されたＳＰ資金提供資格データとしてデバイス注文データ５６８の暗号化されたＳＥ資金提供資格データを暗号化するために使用するた

20

30

40

50

に、及び／又は、動作522にて、運用エンティティサブシステム400から運用注文データ570を通信するためのターゲットSPサブシステム（例えば、そのSPA ID167と関連付けられたSPAサブシステム202）を定義する際に使用するために、SPA ID167のみを利用してSP鍵157を識別することができる（例えば、そのような暗号化を行うためにSP鍵157を識別する際に使用するために、）例えば、SPI ID267ではなくSPA ID167のみを、運用エンティティサブシステム400によりテーブル430内で識別することができる）。しかし、デバイス注文データ568のSPI ID267を、そのターゲットSPAサブシステム202により後で使用するために（例えば、動作526にて、SPA注文データ574をターゲットとするSPIサブシステム250を識別するために）運用注文データ570に含めることができる。一部の
10 実施形態では、動作520は、運用エンティティサブシステム400が、動作520の暗号化及び／又は動作522におけるデータ570の通信が可能となる前に、識別されたターゲットSP情報と関連付けられたSPサブシステム（例えば、デバイス注文データ568のSPA ID167と関連付けられうるSPAサブシステム202）が、運用エンティティサブシステム400により現在信頼されているSPサブシステムであることを保証
20 することを含むことができる。例えば、動作520にて、運用エンティティサブシステム400は、運用エンティティサブシステム400が動作520の暗号化及び／又は動作522におけるデータ570の通信を続行する前に、（例えば、動作502にて）SPAサブシステム202が運用エンティティサブシステム400に適切に登録されていること、及びまだ信頼されたパートナーであることを保証するように機能することができる。したがって、注文データのいくつかをSPサブシステム200に通信する前にデバイス100と運用エンティティサブシステム400の間でデバイス注文データ568を通信することによって、（例えば、デバイス100により注文が行われるのを防止するために）運用エンティティサブシステム400がSPサブシステム200の好適な任意の不正検査及び／又は妥当性検査及び／又は確認を行うことを可能にすることができる。動作520及び522は、運用注文データ570の一部として運用エンティティサブシステム400から送信
30 される資金提供用のSP資格データを、SP鍵157（例えば、動作502にて共有されている、SPサブシステム200と運用エンティティサブシステム400の間の共有秘密）へのアクセスを有していないエンティティにより解読できないような方法で暗号化し、ことを保証するように機能することができる。次いで、動作522にて、好適な任意の
30 プロトコルを使用して通信経路35を介して運用エンティティサブシステム400により運用注文データ570をSPサブシステム200（例えば、SPAサブシステム202のサーバ204）に転送することができる。代わりに、示していないが、動作522にて経路35を介してSPサブシステム200と運用注文データ570を共有するのではなく、運用エンティティサブシステム400は、デバイス100を介して（例えば、通信経路25、次いで通信経路15を介して、及び／又は非接触近接ベース通信5として）SPサブシステム200と運用注文データ570を共有してもよい。

【0046】

このような運用注文データ570がSPサブシステム200（例えば、SPAサブシステム202）により受信されると、SPサブシステム200は、動作524にて、SPA
40 注文データ574を生成するために、そのような運用注文データ570を処理するように機能することができる。例えば、SPAサブシステム202は、運用注文データ570を受信することができ、次いで、SPAサブシステム202にて利用可能なSP情報（例えば、SPA鍵157（例えば、SPサブシステム200と運用エンティティサブシステム400の間の共有秘密））を使用して、運用注文データ570の暗号化されたSP資金提供資格データを解読することができる。これにより、SPAサブシステム202が、決済
50 データ564のSE資金提供資格データを（例えば、暗号化されたSE資金提供資格データとして）暗号化された状態に維持しながらも、注文のターゲットとなりうるサービスプロバイダ発行者サブシステム（例えば、SPIサブシステム290又はSPAサブシステム202と関連付けられうる他の任意のSPIサブシステムではなく、デバイス注文デー

タ５６８内の好適な任意のＳＰ識別データ（例えば、選択肢３２３により識別されるターゲットＳＰと関連付けられうるＳＰＩ ＩＤ２６７）により識別されうるＳＰＩサブシステム２５０）の暗号化されていない識別を決定することを可能にすることができる。これは、ＳＰＡサブシステム２０２が、そのような資金提供資格データを決済データ５６４の暗号化されたＳＥ資金提供資格データとして動作５１４にてデバイス１００のセキュアエレメント１４５により暗号化した資金提供資格鍵（例えば、鍵１５５ａ又は鍵１５５ｂ）へのアクセスを有しないためである。加えて又は代わりに、注文のターゲットとなりうるサービスプロバイダサブシステム（例えば、ターゲットＳＰＩサブシステム）の識別を、決済データ５６４（例えば、暗号化されたＳＥ資金提供資格データ）と共に、注文応答データ５６６及び／又はデバイス注文データ５６８に含まれうる追加のデータ、及び／又は運用注文データ５７０に含まれうる追加のデータにより識別してもよい。運用注文データ５７０は、ターゲットＳＰＩサブシステムを識別する好適な任意の情報（例えば、ＳＰＩサブシステム２５０のＳＰＩ ＩＤ２６７）を含むことができ、それにより、運用注文データ５７０がＳＰＡサブシステム２０２により受信されると、ＳＰＡサブシステム２０２は、その識別された情報に基づいて、ターゲットＳＰＩサブシステムとの共有秘密（例えば、ＳＰＡ－ＳＰＩ共有秘密鍵（例えば、動作５０１にて共有されうる鍵））を識別して、動作５２４にて使用し、運用注文データ５６８の少なくとも一部分を暗号化できるようになっている。

【００４７】

例えば、また処理５００の動作５２４にて、ＳＰＡサブシステム２０２は、（例えば、動作５２４における運用注文データ５７０の何らかの処理を通じて）注文のターゲットとなるサービスプロバイダサブシステムを識別することができた後に、ＳＰＡサブシステム２０２は、その識別されたターゲットサービスプロバイダサブシステムと関連付けられうる、ターゲットＳＰＩサブシステムとの共有秘密（例えば、ＳＰＡ－ＳＰＩ共有秘密鍵（例えば、動作５０１にて共有されうる鍵））を識別し、次いで、そのＳＰＡ－ＳＰＩ鍵を使用して運用注文データ５７０の少なくとも一部分を再暗号化することができる。つまり、動作５２４にて、好適なＳＰＡ鍵情報を使用して運用注文データ５７０の少なくとも一部分を解読した後（決済データ５６４の暗号化されたＳＥ資金提供資格データ及び運用注文データ５６８内に含まれうる他の任意の情報を実現するために、例えば、ＳＰＡ鍵１５７（例えば、ＡＥサブシステム４００とＳＰＡサブシステム２０２の間の共有秘密）を使用して運用注文データ５７０の暗号化されたＳＰ資金提供資格データを解読した後）に、ＳＰＡサブシステム２０２は、次いで、動作５２４にて、解読された運用注文データ５７０（例えば、決済データ５６４の暗号化されたＳＥ資金提供資格データ）の少なくとも一部分を、運用注文データ５７０内で識別されたターゲットＳＰ情報と関連付けられうる適切なＳＰＡ－ＳＰＩ共有秘密鍵により再暗号化することができる。例えば、このようなＳＰＡ－ＳＰＩ共有秘密鍵１５５ｄを、運用注文データ５７０内で識別されたターゲットＳＰ識別子情報をＳＰＡサブシステム２０２のテーブル中のデータと比較することにより決定することができる。この決定された適切なＳＰＡ－ＳＰＩ鍵１５５ｄによって、ＳＰＡサブシステム２０２は、運用注文データ５７０の少なくとも一部分（例えば、決済データ５６４の暗号化されたＳＥ資金提供資格データ）を暗号化されたＳＰＩ資金提供資格データとして再暗号化することができる。このような暗号化されたＳＰＩ資金提供資格データを、動作５２４にて、ＳＰＡ注文データ５７４の少なくとも一部分として生成することができ、次いで、そのようなＳＰＡ注文データ５７４を、動作５２６にて、ターゲットＳＰＩサブシステムに送信することができる。例えば、ＳＰＡ注文データ５７４は、このような暗号化されたＳＰＩ資金提供資格データ、及び、非限定的に、（例えば、選択肢３２５の）資金提供資格の識別並びに／又は（例えば、選択肢３２９の）資金提供量並びに／又は（例えば、選択肢３２３（例えば、具体的なＳＰＩサブシステムの識別子（例えば、ＳＰＩ ＩＤ２６７）及び／若しくは具体的なＳＰＡサブシステムの識別子（例えば、ＳＰＡ ＩＤ１６７）及び／又は受領側デバイスの識別子（例えば、ホストデバイス１００又はクライアントデバイス１００’のデバイス識別子）の識別）の追加された価値のターゲット

10

20

30

40

50

SPサブシステム／SP資格並びに／又は（例えば、選択肢327の）追加される具体的な価値並びに／又は他の好適な任意の情報（例えば、注文デバイス100自体を識別する任意の情報、デバイスベースの一意の取引若しくは注文識別子、運用エンティティサブシステム400により生成された運用ベースの一意の取引若しくは注文識別子、SPAサブシステム202により生成されたSPAベースの一意の取引若しくは注文識別子、及び／又はその他）を含む、デバイス注文データ568による好適な任意のデータなどの他の好適な任意のデータを含むことができる。例えば、運用注文データ570は、SPA ID 167のみならずSPI ID 267も含むことができるが、SPAサブシステム202は、運用注文データ570の暗号化されたSE資金提供資格データをSPA注文データ574の暗号化されたSPI資金提供資格データとして暗号化するために使用するために、及び／又は、動作526にてSPAサブシステム202からSPA注文データ574を通信するためにターゲットSPIサブシステム（例えば、そのSPI ID 267と関連付けられたSPIサブシステム250）を定義するために使用するために、SPI ID 267のみを利用してSPI鍵155aを識別することができる（（例えば、そのような暗号化を行うためのSPI鍵155aを識別するために使用するために）例えば、SPA ID 167ではなくSPI ID 267のみを、SPAサブシステム202によりテーブル中にて識別することができる）。しかし、運用注文データ570のSPA ID 167を、そのターゲットSPIサブシステム250により後で使用するために（例えば、好適な任意の応答データ（例えば、動作534ではSPI購入オブジェクトデータ584及び／又は動作542ではSPI価値データ592）によりSPA注文データ574に応答するためにSPAサブシステム202を識別するために）SPA注文データ574に含めることができる。一部の実施形態では、動作524は、SPAサブシステム202が、識別されたターゲットSPI情報と関連付けられたSPIサブシステム（例えば、運用注文データ570のSPI ID 267と関連付けられうるSPIサブシステム250）が、動作524の暗号化及び／又は動作526におけるデータ574の通信が可能となる前に、SPAサブシステム202により現在信頼されているSPサブシステムであることを保証することを含むことができる。例えば、動作524にて、SPAサブシステム202は、SPAサブシステム202が動作524の暗号化及び／又は動作526におけるデータ574の通信を続行する前に、（例えば、動作501にて）SPIサブシステム250がSPAサブシステム202に適切に登録されていること、及びまだ信頼されたパートナーであることを保証するように機能することができる。したがって、SPIサブシステム250にSPA注文データ574を通信する前に、運用エンティティサブシステム400とSPAサブシステム202の間で運用注文データ570を通信することによって、SPAサブシステム202が、（例えば、デバイス100により行われる注文を保護するために）SPIサブシステム250の好適な任意の不正検査及び／又は妥当性検査及び／又は確認を実行することを可能にすることができる。動作524及び526は、SPA注文データ574の一部としてSPAサブシステム202から送信された暗号化されたSPI資金提供資格データを、SPA-SPI鍵155d（例えば、SPAサブシステム202とSPIサブシステム250の間の共有秘密）へのアクセスを有していないエンティティにより解読できないような方法で、暗号化できることを保証するように機能することができる。次いで、動作526にて、好適な任意のプロトコルを使用して通信経路75を介してSPAサブシステム202によりSPA注文データ574をSPIサブシステム250（例えば、SPIサブシステム250のサーバ210）に転送することができる。

【0048】

このようなSPA注文データ574がSPIサブシステム250により受信されると、SPIサブシステム250は、動作528にて、注文決済データ578を識別するために、そのようなSPA注文データ574を処理するように機能することができる。例えば、SPIサブシステム250は、SPA注文データ574を受信することができ、次いで、SPIサブシステム250にて利用可能であるようなSP情報（例えば、SPA ID 167及びSPIサブシステム250のテーブルを使用して動作528にて識別されうるS

10

20

30

40

50

PA-SPI鍵155d（例えば、SPIサブシステム250とSPAサブシステム202の間の共有秘密）を使用して、SPA注文データ574の暗号化されたSPI資金提供資格データを解読することができる。これにより、SPIサブシステム250が、SPA注文データ574の暗号化されたSPI資金提供資格データを解読することにより、決済データ564の暗号化されたSE資金提供資格データを決定することを可能にすることができる。動作528の処理は、非限定的に、（例えば、選択肢325の）資金提供資格の識別並びに／又は（例えば、選択肢329の）資金提供量の識別並びに／又は（例えば、選択肢323（例えば、具体的なSPIサブシステムの識別子（例えば、SPI ID 267）及び／若しくは具体的なSPAサブシステムの識別子（例えば、SPA ID 167）並びに／又は受領側デバイスの識別子（例えば、ホストデバイス100又はクライアントデバイス100'のデバイス識別子）の）ターゲットSPサブシステム／追加された価値のSP資格の識別及び／又は（例えば、選択肢327の）追加される具体的な価値の識別及び／又は他の好適な任意の情報（例えば、注文デバイス100自体を識別する任意の情報、注文デバイス100により生成されたデバイスベースの一意の取引若しくは注文識別子、運用エンティティサブシステム400により生成された運用ベースの一意の取引若しくは注文識別子、SPAサブシステム202により生成されたSPAベースの一意の取引若しくは注文識別子、及び／又はその他）を含む、デバイス注文データ568からの好適な任意のデータなど、SPA注文データ574の好適な任意の情報を明らかにすることができる。例えば、動作528における資金提供資格及び／又は資金提供資格を担当するエンティティの識別を、その注文決済データを処理して、資金提供のための適切なエンティティに通信するために、決済データ564（例えば、注文決済データ578）の取得された暗号化されたSE資金提供資格データと組み合わせることができる。示すように、例えば、SPIサブシステム250は、動作528にて、注文決済データ578（例えば、決済データ564の暗号化されたSE資金提供資格データ）と、デバイス100上に提供された金融機関資格（（例えば、動作506にて提供された）例えば、FI SSD 154b）からのSE資金提供資格データの金融機関サブシステム350など、その決済データを担当するエンティティとを識別することができ、次いで、動作528aにて、注文に資金提供することを可能にするために、SPIサブシステム250は、そのような注文決済データ578を識別された担当するエンティティ（例えば、通信経路55を介して金融エンティティサブシステム350）と通信することができる。例えば、金融機関サブシステム350は、動作528aにて、SPIサブシステム250から他の好適な任意のデータ（例えば、（例えば、選択肢329の）資金提供量及び／又はSPA注文データ574に含まれるか又はその他の方法で（例えば、選択肢323の）追加された価値のターゲットSPサブシステム／SP資格の識別）と共に決済データ564（例えば、注文決済データ578）の暗号化されたSE資金提供資格データを受信することができ、次いで、金融機関サブシステム350は、資金提供資格データを有効にし明らかにするために、（例えば、暗号化されたSE資金提供資格データを生成した、金融機関サブシステム350と注文デバイス100の間の共有秘密でありうる鍵155bにより）暗号化されたSE資金提供資格データを解読することができ、次いで、金融機関サブシステム350は、資金提供資格データが、（例えば、選択肢329の）依頼された資金提供量を有する資金提供アカウントを識別しうるかどうかを判定することができ、次いで、金融機関サブシステム350は、SPサブシステム200の便益（例えば、SPIサブシステム250の便益）のために注文の資金提供を確認又は否定することができる。つまり、動作528aは、金融機関サブシステム350が、注文データの資金提供資格データにより識別された金融エンティティサブシステム350のアカウントからSPIサブシステム250に、又はSPIサブシステム250と関連付けられた取得用バンクのアカウント）に資金を移転することを認可することをもたすことができ、それにより、デバイス100により生成された決済データ564が、デバイス100の金融機関資格（（例えば、動作506にて提供された）例えば、金融機関SSD 154b）からの資金提供資格データを含むときに、SPIサブシステム25

10

20

30

40

50

0 が、デバイス 100 により生成された注文から資金提供資格データの便益を受けることができるようになっている。代わりに、デバイス 100 により生成された決済データ 564 がデバイス 100 の SP 資格（例えば、（例えば、動作 508 にて提供されたような）SP SSD 154 a）からの資金提供資格データを含むときなど、決済データ 564（例えば、注文決済データ 578）の資金提供資格データが、（例えば、動作 528 における SPA 注文データ 574 の処理により）SPI サブシステム 250 の責任を負っていると判定された場合、動作 528 は、次いで、SPI サブシステム 250 が、デバイス 100 から SPI サブシステム 250 に資金又は価値を移転して戻すことを認可又は確認することを含むことができる（例えば、決済データ 564（例えば、注文決済データ 578）の暗号化された SE 資金提供資格データを、（例えば、デバイス—SPI 共有秘密 SPI 鍵 155 a を使用して）SPI サブシステム 250 により解読することができ、及び／又は資金提供資格データを、SP 価値（（例えば、動作 508 にて）例えば、SPI サブシステム 250 によりデバイス 100 上に従前に提供されている価値）をデバイス 100 から回収するために SPI サブシステム 250 により使用することができる）。

【0049】

決済データ 564（例えば、注文決済データ 578）の資金提供資格データにより識別された資金又は他の好適な価値を、認可できるとき、及び／又はデバイス 100 により依頼された注文（例えば、デバイス注文データ 568 及び／又は運用注文データ 570 及び／又は SPA 注文データ 574 により識別されうる注文）に資金提供するために動作 528 及び／又は動作 528 a にて SPI サブシステム 250 により受信したと確認できるときに、SPI サブシステム 250 は、資金提供された注文を履行するために動作 540 にてサービスプロバイダ価値（「SPV」）データ 590 を生成するように機能することができる。例えば、SPI サブシステム 250 は、（例えば、価値アイテムとして）適切な受領側電子デバイス（例えば、注文用ホスト電子デバイス 100 又は注文データ（（例えば、選択肢 323 の）例えば、デバイス識別子情報）により識別されうる好適な任意の受領側デバイス（例えば、クライアントデバイス 100'））と共有されうる好適な任意の SPV データ 590 を生成するように機能することができ、そのような SPV データ 590 を、非限定的に、（例えば、選択肢 329 の）注文データ 574 の資金提供量及び／又は（例えば、選択肢 323 の）注文データ 574 の追加された価値のターゲット SP サブシステムの識別／SP 資格及び／又は（例えば、動作 528 及び／動作 528 a にて）注文のために受信された（例えば、選択肢 329 の）資金の価値及び／又は（例えば、選択肢 327 の）追加される具体的な価値の識別を含む好適な任意のデータに基づいて生成することができる。SPV データ 590 は、受領側デバイス（例えば、セキュアエレメント又は他のもの）上に記憶され、具体的な貨幣価値の SP 製品にアクセスするために受領側デバイスにより使用されたときにその価値だけ減らされうる実際の貨幣価値とすることができる（例えば、SPV データ 590 は、（例えば、SP 資格 SSD 154 a のアプレット 153 a の）価値カードに記憶される \$80 とすることができ、次いで、受領側デバイスが、SP 製品にアクセスするために、価値記憶カードの資格データ（例えば、乗降提供サービスプロバイダにより提供されたその価値の乗降に支払う \$12.37、又はトランジットシステムサービスプロバイダに関する 1 回の乗降にアクセスするための \$2、又はサービスプロバイダのトランジットシステムに連続 5 時間アクセスするための \$5）を使用するときに（例えば、truth-on-card スクリプトハンドシェイク又はセキュアエレメント上の価値を更新するための好適な任意のコマンドにより）いくらかの量だけ減らすことができる）。一部の実施形態では、SPV データ 590 がデバイス 100 のセキュアエレメント 145 上の SP 資格 SSD に記憶されるように機能することができる場合、その SPV データの少なくとも一部分を、SP サブシステム 200 の共有秘密及びその SP 資格 SSD（例えば、鍵 155 a）により暗号化することができ、そのような SPV データが（例えば、動作 547 にて）その SP 資格 SSD により受信されるときに、その共有秘密を使用してデバイス 100 上で後で解読することができる。別の例として、SPV データ 590 を、一定のタイプの SP 製品アクセスを与える能力により評価するこ

10

20

30

40

50

とができ、SPVデータ590を、受領側デバイス（例えば、セキュアエレメント又は他のもの）上に記憶することができ、SP製品にアクセスするために受領側デバイスにより使用されるときに、好適な任意の単位だけ減らし、又は完全に除去し、又は認証することができる（例えば、SPVデータ590を、受領側デバイス上の価値記憶カード上に記憶でき、次いで、受領側デバイスが、SP製品にアクセスするために価値記憶カードの資格データを使用するとき、一定の量だけ減らせる、SP製品に対する10回分の許可パス（例えば、動物園への2人分のアクセスのための2つのパス）を示すことができ、又はSPVデータ590を、受領側デバイス上に記憶し、次いで、一定のSP製品にアクセスするために権限を証明するために（例えば、SPウェブサイトのデータSP製品への月間全アクセス契約の所有権を証明するために又はトランジットシステムSP製品への月間全アクセスパスの所有権を証明するために）使用中にSPサブシステムにより認証することができる）。このようなSPVデータ590は、SP製品にアクセスするために受領側デバイスにより後で使用するために実際の価値を受領側デバイス（例えば、セキュアエレメント又は他のもの）上に成功裏に記憶しうる、好適な任意のスクリプト（例えば、個人専用のスクリプト）及び／又はAPDU若しくは他の好適なデータを含むことができる。いくつかのSPVデータ590は、受領側デバイス上に記憶され及び／又は受領側デバイスにより提示されるSP価値を認証するために、SPサブシステムによりスキャンされ、そうでなければ検出されうる具体的なコード又は引き換え可能なデータ構造（例えば、QRコード）として、（例えば、好適な任意の出力構成要素及び／又は通信構成要素を介して）受領側デバイスにより提示されうる好適な任意のデータを含むことができる。

【0050】

処理500の動作542にて、SPIサブシステム250は、（例えば、好適な任意の通信プロトコルを使用して通信経路75を介して）SPVデータ590をSPI価値データ592の少なくとも一部分としてSPAサブシステム202に通信することができる。SPI価値データ592は、SPVデータ590と共に、非限定的に、SPVデータ590に関する（例えば、選択肢325の）資金提供資格を識別するデータ並びに／又はSPVデータ590に関する（例えば、選択肢329の）資金提供量を識別するデータ並びに／又はSPVデータ590の（例えば、選択肢323（例えば、具体的なSPIサブシステムの識別子（例えば、SPI ID267）及び／若しくは具体的なSPAサブシステムの識別子（例えば、SPA ID167）並びに／又は受領側デバイスの識別子（例えば、ホストデバイス100又はクライアントデバイス100'のデバイス識別子）の）追加された価値のターゲットSPサブシステム／SP資格並びに／又はデバイス上に存在するか若しくはデバイス上に提供される具体的なSP資格の識別子）を識別するデータ並びに／又はSPVデータ590により追加される（例えば、選択肢327の）具体的な価値を識別するデータ及び／又は他の好適な任意の情報（例えば、注文デバイス100自体を識別する任意の情報、注文デバイス100により生成されたデバイスベースの一意の取引若しくは注文識別子、運用エンティティサブシステム400により生成された運用ベースの一意の取引若しくは注文識別子、SPAサブシステム202により生成されたSPAベースの一意の取引若しくは注文識別子、SPIサブシステム250により生成されたSPIベースの一意の取引若しくは注文識別子）、及び／又はその他）を含む他の好適な任意のデータを含むことができる。一部の実施形態では、SPVデータ590を信頼されていないエンティティにより傍受され使用される恐れなしに、SPIサブシステム250から安全に通信しうるように、少なくともSPVデータ590又はSPI価値データ592のより多くの若しくは全てのデータを、動作542にてSPI価値データ592をSPAサブシステム202に通信する前に、SPIサブシステム250とSPAサブシステム202の間の共有秘密（例えば、SPA-SPI鍵155d）を使用して暗号化し、そうでなければセキュリティ保護することができる。

【0051】

処理500の動作544にて、SPAサブシステム202は、（例えば、好適な任意の通信プロトコルを使用して通信経路35を介して）SPI価値データ592のうちの少な

くともSPVデータ590をSPA価値データ594（例えば、注文履行データ）の少なくとも一部分として運用エンティティサブシステム400に通信することができる。SPAサブシステム202は、運用エンティティサブシステム400に登録されたデバイスであるとSPAサブシステム202により判定されうる受領側デバイスのデバイス識別子など、SPI価値データ592からの好適な任意のデータを識別することにより、このようなSPVデータのターゲットとして運用エンティティサブシステム400を識別することができる。SPA価値データ594は、SPVデータ590と共に、非限定的に、SPVデータ590に関する（例えば、選択肢325の）資金提供資格を識別するデータ並びに／又はSPVデータ590に関する（例えば、選択肢329の）資金提供量を識別するデータ並びに／又は追加された価値のターゲットSPサブシステム／SP資格を識別するデータ（例えば、SPVデータ590の選択肢323の（例えば、具体的なSPIサブシステムの識別子（例えば、SPI ID267）及び／若しくは具体的なSPAサブシステムの識別子（例えば、SPA ID167）並びに／又は受領側デバイスの識別子（例えば、ホストデバイス100又はクライアントデバイス100'）のデバイス識別子並びに／又はデバイス上に存在する若しくはデバイス上に提供される具体的なSP資格の識別子）並びに／又は（例えば、選択肢327の）SPVデータ590により追加される具体的な価値を識別するデータ並びに／又は他の好適な任意の情報（例えば、注文デバイス100自体を識別する任意の情報、注文デバイス100により生成されたデバイスベースの一意の取引若しくは注文識別子、運用エンティティサブシステム400により生成された運用ベースの一意の取引若しくは注文識別子、SPAサブシステム202により生成されたSPAベースの一意の取引若しくは注文識別子、SPIサブシステム250により生成されたSPIベースの一意の取引若しくは注文識別子）、及び／又はその他）を含む他の好適な任意のデータを含むことができる。一部の実施形態では、SPVデータ590を信頼されていないエンティティにより傍受され使用される恐れなしにSPAサブシステム202から安全に通信しうるように、SPA価値データ594のうちの少なくともSPVデータ590を、動作544にてSPA価値データ594を運用エンティティサブシステム400に通信する前に、SPAサブシステム202と運用エンティティサブシステム400の間の共有秘密（例えば、SPA鍵157）を使用して暗号化し、そうでなければセキュリティ保護することができる。一部の実施形態では、SPA価値データ594の少なくとも一部分としてSPAサブシステム202から運用エンティティサブシステム400に通信するために、（例えば、SPA鍵157により）SPVデータ590を再びセキュリティ保護する前に、SPI価値データ592のうちの少なくともSPVデータ590を、SPAサブシステム202とSPIサブシステム250の間の共有秘密（例えば、SPA-SPI鍵155d）を使用して、初めに解読することができ、そうでなければセキュリティ保護せず、又は有効にすることができる。

【0052】

処理500の動作546にて、運用エンティティサブシステム400は、SPA価値データ594のうちの少なくともSPVデータ590をデバイスSP価値データ596の少なくとも一部分として、適切な受領側電子デバイスに通信することができる（例えば、（図5に示すように）好適な任意の通信プロトコルを使用する通信経路25を介して注文用又はホスト電子デバイス100に、又は好適な任意の通信プロトコルを使用する通信経路65を介して（図5に示していない）クライアント電子デバイス100'に、（例えば、動作504と同様の動作にて）好適な任意の方法でデバイス100'を運用エンティティサブシステム400に登録してもよく、関連付けてもよい）通信することができる）。運用エンティティサブシステム400は、受領側デバイスのデバイス識別子などの好適な任意のデータをSPA価値データ594から識別することにより、適切な受領側電子デバイスを、このようなSPVデータのターゲットとして識別することができる。デバイスSP価値データ596は、SPVデータ590と共に、非限定的に、SPVデータ590に関する（例えば、選択肢325の）資金提供資格を識別するデータ並びに／又はSPVデータ590に関する（例えば、選択肢329の）資金提供量を識別するデータ並びに／又はSP

10

20

30

40

50

Vデータ590の（例えば、選択肢323（例えば、具体的なSPIサブシステムの識別子（例えば、SPI ID267）及び／若しくは具体的なSPAサブシステムの識別子（例えば、SPA ID167）並びに／又は受領側デバイスの識別子（例えば、ホストデバイス100又はクライアントデバイス100'のデバイス識別子）並びに／又はデバイス上に存在する若しくはデバイス上に提供される具体的なSP資格の識別子）の）追加された価値のためのターゲットSPサブシステム／SP資格を識別するデータ並びに／又はSPVデータ590により追加された（例えば、選択肢327の）具体的な価値を識別するデータ並びに／又は他の好適な任意の情報（例えば、注文デバイス100自体を識別する任意の情報、注文デバイス100により生成されたデバイスベースの一意の取引若しくは注文識別子、運用エンティティサブシステム400により生成された運用ベースの一意の取引若しくは注文識別子、SPAサブシステム202により生成されたSPAベースの一意の取引若しくは注文識別子、SPIサブシステム250により生成されたSPIベースの一意の取引若しくは注文識別子）、及び／又はその他）を含む他の好適な任意のデータを含むことができる。一部の実施形態では、SPVデータ590を信頼されていないエンティティにより傍受又は使用される恐れなしに運用エンティティサブシステム400から安全に通信しうるように、デバイスSP価値データ596のうちの少なくともSPVデータ590を、動作546にてデバイスSP価値データ596を受領側デバイスに通信する前に、運用エンティティサブシステム400と受領側電子デバイスの間の共有秘密（（例えば、デバイス100のための）例えば、鍵155c及び／又は鍵156k）を使用して暗号化し、そうでなければセキュリティ保護することができる。このような実施形態では、デバイスSP価値データ596の少なくとも一部分として運用エンティティサブシステム400から通信するためにSPVデータ590を再びセキュリティ保護する前に、運用エンティティサブシステム400とSPAサブシステム202の間の共有秘密を使用して、SPA価値データ594のうちの少なくともSPVデータ590を初めに解読することができ、そうでなければセキュリティ保護せず、又は有効にすることができる。一部の実施形態では、示すように、動作546にて、このようなデバイスSP価値データ596を受領側電子デバイスのセキュアエレメント（例えば、デバイス100のセキュアエレメント145）に通信することができる。例えば、デバイスSP価値データ596の少なくとも一部分（例えば、SPVデータ590の少なくとも一部分）を、デバイスSP価値データ597として、（例えば、新たなSP価値を受領側デバイスに記憶／追加するために）動作547にてセキュアエレメント145のSP資格SSD（例えば、SP資格SSD154a又は同様なSSD）又はデバイス100の他の好適な任意のメモリに提供することができ、次いで、動作548にて、そのようなSPVデータがデバイス100に成功裏に提供されたことを示すために更新データ598をプロセッサ102と共有することができ、デバイス100の好適な任意のアプリケーション（例えば、プロセッサ102上で実行中の資格管理又はウォレットアプリケーション）は、そのような更新データ598を利用して図3Eの画面190eを提示し、メッセージ335により注文のSP価値の追加が成功したことを示すことができる（例えば、完了した注文による受領側デバイス上の具体的なSP資格の新たな価値をメッセージ335により示すことができる）。同様のデータを、デバイス100上への提供の成功を運用エンティティサブシステム400に示すためにデバイス100から運用エンティティサブシステム400に、また恐らく、デバイス100上への提供の成功をSPサブシステム200に示すために運用エンティティサブシステム400からSPサブシステム200に転送することができる。代わりに、一部の実施形態では、このようなデバイスSP価値データ596を、（例えば、セキュアエレメントではなくデバイス100のメモリ104に記憶されうるサービスプロバイダ資格データ123として）セキュアエレメント以外の受領側デバイス上に記憶するために通信してもよい。

【0053】

SPVデータ590が（例えば、動作546及び／又は動作547にてデバイスSP価値データ596の少なくとも一部分として）受領側デバイス上に成功裏に記憶されると、

10

20

30

40

50

動作510にて開始された注文を完了することができる。次いで、好適な任意のSP製品への好適な任意のアクセスを得るために、受領側デバイスに追加された新たなSP資格価値を好適な任意の方法で受領側デバイスにより使用することができる。例えば、デバイス100は、SPVデータ590の受領側デバイスとすることができ、ターゲットSPサブシステム200の好適な任意のSP製品への好適な任意のアクセスを得るために、動作549にて、少なくとも部分的にSPVデータ590に基づきうる好適な任意のSPアクセスデータ599を、適切なターゲットSPサブシステム200に通信することができる。示すように、デバイス100は、SPIサブシステム250と関連付けられた好適な任意のSP製品にアクセスする際に使用するために、動作549にてSPアクセスデータ599を生成しSPIサブシステム250に通信するために、受信したSPVデータ590を好適な任意の方法で利用することができる。例えば、デバイス100は、動作549aにて、デバイス100及び／又はその所有者及び／又はその所有者の関係者に、好適な任意のSP製品599a（例えば、具体的な娯楽イベント若しくは輸送イベントの許可又は（例えば、デバイス100へのダウンロード又はストリーミングのための）好適な任意のメディアデータの取得その他）へのアクセスを与えるために、SPサブシステム200による受領のために（例えば、SPIサブシステム250の端末220による受領のためにNFC構成要素120からの）非接触近接ベース通信5として、及び／又は、SPサブシステム200による受領のために（例えば、通信経路15を介したSPIサーバ210による受領のために通信構成要素106からの）好適な任意のオンラインベース通信として、及び／又は、SPサブシステム200による受領のために好適な任意の方法でデバイス100により提示される好適な任意のデータとして、SPアクセスデータ599を通信することができる（例えば、好適な任意のスキナ又はSPサブシステム200若しくはそのオペレータの他の好適な検知入力構成要素による受領のためにデバイス100の出力構成要素112を介した視覚及び／又は聴覚及び／又は他の好適な任意のデータの提示（例えば、デバイス100上に記憶されたSP価値を認証するためにSPサブシステム200によりスキャンされうる具体的なQRコードとしてSPアクセスデータ599をデバイス100の表示出力構成要素112上に提示することができる））。SPVデータをSPアクセスデータ599としてSPサブシステム200と通信することにより、SP製品599aへのアクセスと引き換えられうる、具体的なSP製品アクセスの購入のレシート（例えば、サービスプロバイダの物理的な商品を受け取るために又はサービスプロバイダの具体的なサービスにアクセスするためにデバイス100のユーザにより提示されうるレシート）の証拠（例えば、デバイス注文に資金提供するための証拠）として、SPアクセスデータ599を提供することができる。したがって、SPVデータ590は、SP製品にアクセスするために受領側デバイスによりSPアクセスデータ599の少なくとも一部分としてサービスプロバイダに提供されうるサービスプロバイダ資格データの少なくとも一部分を定義するために受領側デバイス上に記憶されうる好適な任意のデータとすることができる。

【0054】

少なくとも注文用電子デバイスとサービスプロバイダ発行者サブシステムの間のデバイス注文を実行する処理500中の好適な任意の時点（単数又は複数）（例えば、受信機応答を伴わない具体的な動作の後に好適な任意の継続時間が生じた後、又は好適な任意のタイマが経過した後）で、運用エンティティサブシステム400は、電子デバイスの代わりに電子デバイス上の資格及びサービスプロバイダとの通信を管理するためにデバイス注文の状況を追跡するように機能することができる。例えば、動作522にて運用エンティティサブシステム400からSPサブシステム200（例えば、SPAサブシステム202）に通信された運用注文データ570は、SPサブシステム200との新たな注文を開始するための注文データを含むことができる。SPサブシステム200は、（上で説明したように、例えば、動作524、526、528、528a、540、542、及び／又は544にて）受領側電子デバイス上に提供するための新たなSP資格データに資金提供することを試みるために注文データ570のそのような注文を処理することに加えて、SP

10

20

30

40

50

サブシステム 200 は、運用エンティティサブシステム 400 と共有される購入オブジェクトの形をとりうる注文確認により注文データ 570 のそのような注文に応答するように機能することができる。例えば、示すように、処理 500 の動作 536 にて、SP サブシステム 200（例えば、SPA サブシステム 202）は、SPA 注文購入オブジェクトデータ 586 を生成し運用エンティティサブシステム 400 に通信するように機能することができ、SPA 注文購入オブジェクトデータ 586（例えば、注文状況更新データ）を、動作 522 にて運用注文データ 570 として SP サブシステム 200 に、運用エンティティサブシステム 400 により提供された注文への応答として、又は、動作 530 にて（例えば、動作 522 にて注文が SP サブシステム 200 に最初に提供された後の好適な任意の時点で）運用更新依頼データ 580 により運用エンティティサブシステム 400 から SP サブシステム 200 に提供されうるような、その注文に関する後の任意の運用状況更新依頼への応答として通信することができ、又はそのような購入オブジェクトデータを、運用エンティティサブシステム 400 からの具体的な依頼に回答せずに SP サブシステム 200 により提供することができる。

【0055】

運用注文データ 570 並びに／又はそのような任意の運用更新依頼データ 580 の注文状況依頼は、処理されている注文を一意に示しうる好適な任意データの（（例えば、選択肢 325 の）例えば、資金提供資格を識別するデータ並びに／又は（例えば、選択肢 329 の）資金提供量を識別するデータ並びに／又は（例えば、選択肢 323（例えば、具体的な SPI サブシステムの識別子（例えば、SPI ID 267）及び／若しくは具体的な SPA サブシステムの識別子（例えば、SPA ID 167）並びに／又は受領側デバイスの識別子（例えば、ホストデバイス 100 又はクライアントデバイス 100' のデバイス識別子）の）追加された価値のターゲット SP サブシステム／SP 資格を識別するデータ、など）並びに／又は（例えば、選択肢 327 の）追加される具体的な価値を識別するデータ並びに／又は他の好適な任意の情報（例えば、注文デバイス 100 自体を識別する任意の情報、注文デバイス 100 により生成されたデバイスベースの一意の取引若しくは注文識別子、運用エンティティサブシステム 400 により生成された運用ベースの一意の取引若しくは注文識別子、SPA サブシステム 202 により生成された SPA ベースの一意の取引若しくは注文識別子、及び／又はその他）を含むことができ、そのような注文状況依頼への応答として通信されうる SPA 注文購入オブジェクトデータ 586 は、（例えば、運用エンティティサブシステム 400 に関して、運用エンティティサブシステム 400 が、同一の SP サブシステムにより及び／又は異なる SP サブシステムにより同時に異なる複数の注文を追跡するように機能しうるように）処理されている注文を一意に示しうる好適な任意の情報も含むことができる。例えば、SPA 注文購入オブジェクトデータ 586 は、全ての注文／取引にわたって一意でありうる一意の識別子（例えば、SPA サブシステム 202 により生成された SPA ベースの一意の取引若しくは注文識別子及び／又は運用エンティティサブシステム 400 により生成された運用ベースの一意の取引若しくは注文識別子及び／又は注文デバイス 100 により生成されたデバイスベースの一意の取引若しくは注文識別子）、並びに注文状況（例えば、処理されている注文の現在の状況を示す情報、「保留中」（例えば、動作 524 における受領と動作 544 における SPV データ 590 の共有の間である注文の状況）、「完了」（例えば、動作 544 における SPV データ 590 の共有の後又は同データを受領側デバイス上に提供したことを確認した後である注文の状況）、又は「失敗」（（例えば、動作 528 及び／又は動作 528a にて）例えば、注文データの資金提供資格が注文に資金提供するための認証又は承認に失敗した場合の注文の状況）など）、状況メッセージ（例えば、現在の状況を記述しうる好適な任意のシステム生成メッセージ（例えば、なぜ失敗したか、いつ完了したかなどの注文状況の詳細））、及び／又は、SPA サブシステム 202 により決定されうるような現在の状況に基づいて（例えば、購入オブジェクトにより識別された現在の注文状況に基づいて）注文に関して実施されうる 1 つ以上の利用可能なアクションのアレイ（例えば、現在の注文状況が「保留中」である場合、利用可能なアクションは、SPA サブシステム 202

10

20

30

40

50

に保留中の注文のキャンセルを指示することにより、運用エンティティサブシステム 400 が購入オブジェクトに回答しうるような「キャンセル」となりうる）を含むことができる。例えば、動作 536 にて、運用エンティティサブシステム 400 により受信された S P A 注文購入オブジェクトデータ 586 の購入オブジェクトが注文状況「保留中」及び利用可能なアクション「キャンセル」を含む場合、運用エンティティサブシステム 400 は、保留中の注文をキャンセルするために S P A サブシステム 202 への命令で応答することができる（例えば、S P I サブシステム 250 への命令を通信することにより）注文をキャンセルすること及び新たな S P A 注文購入オブジェクトデータ 586 の更新された購入オブジェクトを、「保留中」から「キャンセルされた」に更新された注文状況と共に送ることを S P A サブシステム 202 に命令しうる、例えば、S P A 注文購入オブジェクトデータ 586 の購入オブジェクトの一意に識別された注文のキャンセルアクションを S P A サブシステム 202 に戻すことができる）。S P A サブシステム 202 は、動作 522 にて運用注文データ 570 に対する注文状況依頼及び／又は動作 530 にて運用更新依頼データ 580 に対する注文状況依頼を運用エンティティサブシステム 400 から受信し、次いで、動作 536 にて S P A 注文購入オブジェクトデータ 586 の購入オブジェクトを生成し通信する前に、動作 532 及び 534 にて注文の S P I サブシステム 250 と通信することができる。例えば、S P A サブシステム 202 は、動作 532 にて、S P I サブシステム 250 からの識別された注文の現在の状況を依頼しうる S P A 更新依頼データ 582 を S P I サブシステム 250 に通信することができ、次いで、S P I サブシステム 250 は、動作 534 にて、識別された注文の現在の状況を含みうる依頼の応答として S P I 注文購入オブジェクトデータ 584 を生成し通信することができ、それを、次いで、S P A 注文購入オブジェクトデータ 586 の購入オブジェクトの少なくとも一部分を定義するために S P A サブシステム 202 により使用することができる。動作 536 にて好適な任意の S P A 注文購入オブジェクトデータ 586 を受信することに応じて、運用エンティティサブシステム 400 は、動作 538 にて、関連するデバイス購入オブジェクトデータ 588 を生成しデバイス 100（例えば、プロセッサ 102）に通信するように機能することができ、デバイス 100 の好適な任意のアプリケーション（例えば、プロセッサ 102 上で実行中の資格管理又はウォレットアプリケーション）は、そのようなデバイス購入オブジェクトデータ 588 を利用して図 3D の画面 190d を提示し、（例えば、注文購入オブジェクトデータ 586 により示されるような）注文の現在の注文状況を示すメッセージ 333 と共に示すことができる。S P A サブシステム 202 から受信された任意の注文状況が、運用エンティティサブシステム 400 により認証として信頼されていること、及び、（例えば、受信された注文状況が「完了」である場合に）実際の S P V データが受領側デバイスにより受信されなかった場合でも、運用エンティティサブシステム 400 が、（例えば、具体的な注文取引に関して通信される全ての購入オブジェクト及び S P V データを追跡し続けることにより）資金提供の責任及び注文デバイスと S P サブシステムの間 S P V データを管理しうるように、注文の資金提供の証拠として使用されうることを証明するために、S P A 注文購入オブジェクトデータ 586 の少なくとも一部分（例えば、購入オブジェクト）を、S P A サブシステム 202 と運用エンティティサブシステム 400 の間の好適な任意の共有秘密（例えば、鍵 157）により暗号化し、署名し、そうでなければセキュリティ保護することができる。したがって、デバイス注文を履行するために受領側デバイスに価値を実際に加えるために、（例えば、動作 524～528 及び 540～598 を好適な任意の回数繰り返して）S P V データ 590 を生成し、運用エンティティサブシステム 400 を介して S P サブシステム 200 から受領側デバイス（例えば、デバイス 100 又はデバイス 100'）に通信することと並行して、（例えば、運用エンティティサブシステム 400 及び／又はデバイス 100（例えば、デバイス 100 の好適な任意のアプリケーション（例えば、プロセッサ 102 上で実行中の資格管理又はウォレットアプリケーション））にて状況を更新するために）デバイス注文の状況を追跡するために、運用エンティティサブシステム 400 を介して S P サブシステム 200 と注文デバイス 100 及び／又は任意の受領側デバイスの間で（例えば、動作 530～538 を好適

10

20

30

40

50

な任意の回数繰返して) 購入オブジェクトデータを通信することができる。

【0056】

システム1の任意の2つの通信エンティティの間で、好適な任意のAPI(単数又は複数)を使用することができる。運用エンティティサブシステム400は、データ570及び/又はデータ580の状況依頼によりAPIエンドポイントを呼び出して具体的な注文の現在の状況を取り出すことができ、コ呼び出しへのAPI応答は、SPAサブシステム202からのSPA注文購入オブジェクトデータ586の購入オブジェクトとすることができる。SPサブシステム200と共に運用エンティティサブシステム400により使用されるこのようなAPIは、デバイス注文データを運用エンティティサブシステム400と通信するための注文デバイス100(例えば、プロセッサ102上で実行中の資格管理又は他の好適なアプリケーション)に由来しうるAPIの継続とすることができる。運用エンティティサブシステム400とSPAサブシステム202の間で通信される任意のデータを、JavaScript Object Notation(「JSON」)ファイル又は辞書などの好適な任意のタイプ及び/又は構造のファイルの内部で通信ことができ、UTF-8文字列エンコーディングなどの好適な任意の方法で文字列エンコーディングを行うことができる。例えば、SPA注文購入オブジェクトデータ586は、鍵購入を伴うJSON辞書により表されうる購入オブジェクト(例えば、注文状況依頼の好適な任意の確認)とすることができる。一部の実施形態では、「状況Code」鍵などの具体的な鍵を、1つ、一部又は全てのAPI応答に含まれうる応答ヘッダ(例えば、応答ヘッダJSONデータ構造)内で定義されうるオプション鍵とすることができる。依頼が成功裏に処理されエラーが生じなかった場合、このような「状況Code」鍵を応答ヘッダに含まなくてもよい。しかし、このような「状況Code」鍵が応答ヘッダ内に存在する場合、受信サーバは、データの残り部分(例えば、JSONデータ構造の残り部分)をパーシングする必要があると判定するように機能することができる。例えば、デバイス注文又はデバイス注文状況依頼の処理においてエラーが生じた場合、購入オブジェクトは、SPA注文購入オブジェクトデータ586の構造(例えば、JSONデータ構造)に存在しなくてもよい。

【0057】

図5の処理500に示される動作は、単なる例示にすぎず、既存の動作を修正又は省略し、更なる動作を追加し、いくつかの動作の順序を変更してもよいことを理解されたい。したがって、デバイス注文が、注文デバイス100のセキュアエレメント上の資金提供資格を使用して生成されてもよく、注文デバイス100のその同一のセキュアエレメント上及び/又はあるセキュアエレメント上、そうでなければ別の受領側デバイス上の新たなSP価値の追加にリモートSPサブシステム200から資金提供してもよい。運用エンティティサブシステム400は、SPサブシステム200と注文デバイス100と任意の受領側デバイスの間の全ての通信の導管の役割を果たすことにより取引全体の中心的役割を担うことができ、それにより、運用エンティティサブシステム400及び他のサブシステム/デバイスの1つ以上にとって利用可能な1つ以上の共有秘密を使用することにより、デリケートな資格データをサブシステムの間で安全に通信するために、運用エンティティサブシステム400が信頼されたサービスマネージャの役割を果たすことを可能にすることができる。一部の実施形態では、運用エンティティサブシステム400は、ホストデバイス100及び/若しくはクライアントデバイス100'のセキュアエレメントに並びに/又はセキュアエレメントから資格データを安全に通信する(例えば、SP資格データ及び/又は金融機関資格データを暗号化通信する)ように機能しうる、システム1内の唯一のサブシステムとなることができ、それにより、運用エンティティサブシステム400は、処理500中にSPサブシステムと1つ以上のユーザ電子デバイスの間で通信される全ての注文取引データのためのゲートキーパの役割を果たしうようになっている。したがって、資格がデバイス100上に提供されるときに、及び/又はそのような提供された資格が注文取引に資金提供するためにデバイス100とサービスプロバイダサブシステム200の間の資格データ通信の一部として使用されるときに、新たなセキュリティ層を提供する

及び／又はよりシームレスなユーザエクスペリエンスを提供するように、運用エンティティサブシステム400を構成することができる。

【0058】

図6は、セキュリティ保護された取引（例えば、注文）を管理するための、例示的な処理600のフローチャートである。処理600の動作602にて、運用エンティティサブシステムは、電子デバイスに記憶されるサービスプロバイダサブシステムの価値に対する注文を示すデバイス注文データを電子デバイスから受信することができる（例えば、運用エンティティサブシステム400は、デバイス注文データ568を電子デバイス100から受信することができる）。処理600の動作604にて、運用エンティティサブシステムは、注文を示すデバイス注文データの少なくとも一部分を含みうる運用注文データをサービスプロバイダサブシステムに送信することができる（例えば、運用エンティティサブシステム400は、運用注文データ570をサービスプロバイダサブシステム200に送信することができる）。処理600の動作606にて、運用エンティティサブシステムは、サービスプロバイダサブシステムによる価値に対する注文の履行の状況を示す注文状況更新データをサービスプロバイダサブシステムから受信することができる（例えば、運用エンティティサブシステム400は、注文購入オブジェクトデータ586をSPサブシステム200から受信することができる）。処理600の動作608にて、運用エンティティサブシステムは、運用エンティティ及びサービスプロバイダサブシステムの共有秘密を使用して、受信した注文状況更新データを検証することができる（例えば、運用エンティティサブシステム400は、（例えば、運用エンティティサブシステム400とSPサブシステム200の間の共有秘密（例えば、鍵157）を使用して妥当性（例えば、注文購入オブジェクトデータ586のソース）を確認することができる）。検証は、共有秘密を使用して、受信した注文状況更新データの少なくとも一部分を解読すること、復号すること、及び署名削除することのうちの少なくとも1つを含むことができ、共有秘密は、注文状況更新データを受信する前に、（例えば、処理500の動作502における登録にて）運用エンティティとサービスプロバイダサブシステムの間で共有されたデータを含むことができる。検証した後に、運用エンティティサブシステムは、受信した注文状況更新データの少なくとも一部分を電子デバイスに送信することができる（例えば、運用エンティティサブシステム400は、オブジェクトデータ588を通信することができる）。運用エンティティサブシステムは、注文の価値を含む注文履行データをサービスプロバイダサブシステムから受信することができ（例えば、運用エンティティサブシステム400は価値データ594を受信することができ）、価値の少なくとも一部分を電子デバイスに（例えば、価値データ596としてセキュアエレメント145に）送信することができ、価値は、電子デバイスがサービスプロバイダサブシステムの製品にアクセスすることを可能にすることができる（例えば、デバイス100は、価値データ596を使用して製品599aにアクセスすることができる）。運用エンティティサブシステムは、運用エンティティ及び電子デバイスの共有秘密を使用して、受信したデバイス注文データの一部分を解読することができ、次いで、運用エンティティ及びサービスプロバイダサブシステムの共有秘密を使用して、受信したデバイス注文データの一部分を再暗号化することができ、（例えば、動作604の）運用注文データは、受信したデバイス注文データの再暗号化した部分を含むことができ、それは、注文の履行に資金提供するように機能する決済データ（例えば、決済データ564）を含むことができる。

【0059】

図6の処理600に示される動作は、単なる例示にすぎず、既存の動作を修正又は省略し、更なる動作を追加し、具体的な動作の順序を変更してもよいことを理解されたい。

【0060】

記述したように、電子デバイス100には、非限定的に、音楽プレイヤー（例えば、カリフォルニア州クパチーノのApple Inc. により供給可能なiPod（登録商標））、ビデオプレイヤー、静止画プレイヤー、ゲームプレイヤー、他のメディアプレイヤー、音楽レコーダ、ムービー若しくはビデオカメラ又はレコーダ、静止画カメラ、他のメディアレコ

ーダ、ラジオ、医療用機器、家庭用若しくは商業用機器、輸送車両用計器、楽器、計算機、セルラー電話（例えば、Apple Inc. により供給可能な iPhone（登録商標））、他の無線通信デバイス、携帯情報端末、リモートコントローラ、ページャ、コンピュータ（例えば、デスクトップ、ラップトップ、タブレット（例えば、Apple Inc. により供給可能な iPad（登録商標））、サーバなど）、モニタ、テレビ、ステレオ装置、セットアップボックス、セットトップボックス、モデム、ルータ、プリンタ、又はそれらの任意の組合せを含むことができる。一部の実施形態では、電子デバイス 100 は、単一の機能を実行することができ（例えば、SP 価値に対するデバイス注文を行う専用デバイス）、他の実施形態では、電子デバイス 100 は、複数の機能を実行することができる（例えば、SP 価値に対するデバイス注文を行う、音楽を再生する、及び電話呼出しを送受信するデバイス）。電子デバイス 100 は、ユーザがどこを移動していても SP 価値に対するデバイス注文を行うように構成されうる、任意のポータブル、モバイル、ハンドヘルド、又は微細電子デバイスとすることができる。一部の微細電子デバイスは、iPod（登録商標）などのハンドヘルド電子デバイスよりも小さなフォームファクタを有することができる。例示する微細電子デバイスを、非限定的に、腕時計（例えば、Apple Inc. による Apple Watch（登録商標））、リング、ネックレス、ベルト、ベルト用アクセサリ、ヘッドセット、靴用アクセサリ、仮想現実デバイス、眼鏡、他のウェアラブル電子機器、スポーツ用品用アクセサリ、フィットネス機器用アクセサリ、キーホルダ、又はそれらの任意の組合せを含みうる、種々の対象物に組み込むことができる。代わりに、電子デバイス 100 は、ポータブルでなくてもよく、代わりに概ね据え置き型でもよい。

10

20

【0061】

メモリ 104 は、例えば、ハードドライブ、フラッシュメモリ、リードオンリーメモリ（「ROM」）などの永続的メモリ、ランダムアクセスメモリ（「RAM」）などの半永続的メモリ、他の好適な任意のタイプの記憶構成要素、又はそれらの任意の組合せを含む、1つ以上の記憶媒体を含むことができる。メモリ 104 は、電子デバイスアプリケーション用のデータを一時的に記憶するために使用される1つ以上の異なるタイプのメモリでありうるキャッシュメモリを含むことができる。メモリ 104 は、電子デバイス 100 内に固定的に組み込まれてもよく、又は、電子デバイス 100 に対して反復的に挿入し取り出しうる1つ以上の好適なタイプのカード（例えば、加入者識別モジュール（「SIM」）カード又はセキュアデジタル（「SD」）メモリカード）に組み込まれてもよい。通信構成要素 106 は、好適な任意のデータを任意のリモートサーバ又は他の好適なエンティティ（例えば、好適な任意のインターネット接続）に通信するように機能するときに、オンライン通信構成要素と呼ばれる場合がある。電子デバイス 100 の地理的位置を決定するように通信構成要素 106 を構成することができる。例えば、通信構成要素 106 は、全地球測位システム（「GPS」）又はセルタワー測位技術若しくはWi-Fi技術を使用しうる地域内若しくはサイト内測位システムを利用することができる。

30

【0062】

ユーザがデバイス 100 と対話又はインターフェースすることを可能にするために、1つ以上の入力構成要素 110 を設けることができる。例えば、入力構成要素 110 は、非限定的に、タッチパッド、ダイヤル、クリックホイール、スクロールホイール、タッチスクリーン、1つ以上のボタン（例えば、キーボード）、マウス、ジョイスティック、トラックボール、マイク、カメラ、スキャナ（例えば、バーコードスキャナ、又はバーコード、QRコードその他などのコードから製品識別情報を取得しうる他の好適な任意のスキャナ）、近接センサ、光検出器、動きセンサ、生体認証センサ（例えば、ユーザ認証のために電子デバイス 100 にとってアクセス可能でありうる特徴処理アプリケーションと共に動作しうる、指紋リーダ又は他の特徴認識センサ）、及びそれらの組合せを含む、種々の形態をとることができる。動作中のデバイス 100 と関連付けられたコマンドを選択又は発行するための1つ以上の専用制御機能を提供するように、各入力構成要素 110 を構成することができる。

40

50

【0063】

電子デバイス100は、デバイス100のユーザに情報（例えば、グラフィック、聴覚、及び／又は触覚情報）を提示しうる1つ以上の出力構成要素112を含むこともできる。例えば、電子デバイス100の出力構成要素112は、非限定的に、音声スピーカ、ヘッドホン、音声ラインアウト、表示装置、アンテナ、赤外線ポート、触覚出力構成要素（例えば、回転機、バイブレータなど）、又はそれらの組合せを含む、種々の形態をとることができる。

【0064】

電子デバイス100のプロセッサ102は、電子デバイス100の1つ以上の構成要素の動作及びパフォーマンスを制御するように機能しうる任意の処理回路構成を含むことができる。例えば、プロセッサ102は、入力構成要素110から入力信号を受信することができ、及び／又は出力構成要素112を通じて出力信号を駆動することができる。図2に示すように、アプリケーション103、アプリケーション113、及び／又はアプリケーション143などの1つ以上のアプリケーションを実行するためにプロセッサ102を使用することができる。各アプリケーション103／113／143には、非限定的に、1つ以上のオペレーティングシステムアプリケーション、ファームウェアアプリケーション、メディア再生アプリケーション、メディア編集アプリケーション、NFC低出力モードアプリケーション、バイオメトリック特徴処理アプリケーション、又は他の好適な任意のアプリケーションを含むことができる。例えば、プロセッサ102は、アプリケーション103／113／143をユーザインターフェースプログラムとしてロードして、入力構成要素110又はデバイス100の他の構成要素により受信された命令又はデータによって、情報を記憶し及び／又は出力構成要素112によりユーザに提供しうる方法を、どのように操作しうるかを決定することができる。アプリケーション103／113／143には、（例えば、バス118を介して）メモリ104から又は（例えば、通信構成要素106を介して）別のデバイス若しくはサーバからなど、好適な任意のソースからプロセッサ102によりアクセスすることができる。プロセッサ102は、単一のプロセッサ又は複数のプロセッサを含むことができる。例えば、プロセッサ102は、少なくとも1つの「汎用」マイクロプロセッサ、汎用マイクロプロセッサと特定用途マイクロプロセッサの組合せ、命令セットプロセッサ、グラフィックプロセッサ、ビデオプロセッサ、及び／又は関連チップセット、及び／又は特定用途マイクロプロセッサを含むことができる。プロセッサ102は、キャッシュ目的のオンボードメモリを含むこともできる。

【0065】

電子デバイス100は、近距離無線通信（「NFC」）構成要素120を含むこともできる。NFC構成要素120は、電子デバイス100とサービスプロバイダサブシステム200（例えば、サービスプロバイダ決済端末220）の間の非接触近接ベースの取引又は通信を可能にしうる、好適な任意の近接ベース通信メカニズムとすることができる。NFC構成要素120は、比較的低いデータ速度（例えば、424 kbps）での近接範囲通信を可能にすることができ、ISO／IEC 7816、ISO／IEC 18092、ECMA-340、ISO／IEC 21481、ECMA-352、ISO 14443、及び／又はISO 15693などの好適な任意の規格に準拠することができる。代わりに又は加えて、NFC構成要素120は、比較的高いデータ速度（例えば、370 Mbps）での近接範囲通信を可能にしてもよく、Transfer Jet（登録商標）プロトコルなどの好適な任意の規格に準拠してもよい。NFC構成要素120とサービスプロバイダサブシステム200の間の通信は、凡そ2～4センチメートルの範囲など、NFC構成要素とサービスプロバイダサブシステム200の間における好適な任意の近接範囲距離（例えば、図1におけるNFC構成要素120とサービスプロバイダ決済端末220の間の距離Dを参照）内で生じることができ、好適な任意の周波数（例えば、13.56 MHz）で動作することができる。例えば、NFC構成要素のこのような近接範囲通信は、NFC構成要素が他のNFCデバイスと通信しうること及び／又は無線周波数識別（「RFID」）回路構成を有するタグから情報を取り出すことを可能にしうる、磁界誘導により生じ

10

20

30

40

50

ることができる。このようなNFC構成要素は、製品情報を取得し、決済情報を移転し、そうでなければ外部デバイスと通信する（例えば、NFC構成要素120とサービスプロバイダ端末220の間で通信する）方法を提供することができる。

【0066】

NFCコントローラモジュール140とNFCメモリモジュール150は、耐タンパー性というセキュアエレメント145の少なくとも一部分を独立して又は組み合わされて提供することができる。例えば、このようなセキュアエレメント145は、よく識別された信頼された権限者の集合（例えば、金融機関サブシステム及び／又はGlobalPlatformなどの業界標準の権限者）により定められうる規則及びセキュリティ要件に従って、アプリケーション及びそれらの機密及び暗号データ（例えば、アプレット153及び鍵155）を安全にホスティングすることが可能でありうる、（例えば、単一又は複数チップのセキュアマイクロコントローラとして）耐タンパー性プラットフォームを提供するように構成することができる。NFCメモリモジュール150は、メモリ104の一部分、又はNFC構成要素120に固有の少なくとも1つの専用チップとすることができる。NFCメモリモジュール150は、SIM上に、電子デバイス100のマザーボードの専用チップ上に、又は外部プラグインメモリカードとして常駐してもよい。NFCメモリモジュール150を、NFCコントローラモジュール140から完全に独立させることができ、デバイス100の様々な構成要素により提供することができ、及び／又は様々なリムーバブルサブシステムにより電子デバイス100に提供することができる。セキュアエレメント145は、デリケートなデータ又はアプリケーションを電子デバイス100上に記憶するために使用されうる、チップ内の高度にセキュリティ保護された耐タンパー性ハードウェア構成要素とすることができる。汎欧州デジタル移動通信（「GSM」）ネットワーク、ユニバーサル移動体通信システム（「UMTS」）及び／又はロングタームエボリューション（「LTE」）規格ネットワークに適した電子デバイス100に使用されうる、ユニバーサル集積回路カード（「UICC」）又は加入者識別モジュール（「SIM」）カードなどのリムーバブル回路カード内にセキュアエレメント145の少なくとも一部分を設けることができる。代わりに又は加えて、デバイス100の製造中に電子デバイス100に組み込まれうる集積回路内にセキュアエレメント145の少なくとも一部分を設けてもよい。代わりに又は加えて、電子デバイス100にプラグイン、挿入、そうでなければ結合されうる、マイクロセキュアデジタル（「SD」）メモリカードなどの周辺デバイス内にセキュアエレメント145の少なくとも一部分を設けてもよい。

【0067】

図1のサービスプロバイダサブシステム200のサービスプロバイダ端末220は、電子デバイス100からのNFC通信（例えば、デバイス100が端末220から一定の距離に来たとき又は端末220に近接したときの通信5）を検出し、読み取り、そうでなければ受信するリーダを含むことができる。したがって、このようなサービスプロバイダ端末と電子デバイス100の間のNFC通信が、無線で生じること、よって、それぞれのデバイスの間に明瞭な「見通し線」を必要としないことに留意されたい。記述したように、NFCデバイスモジュール130は、受動的又はアクティブとすることができる。受動的であるとき、このようなサービスプロバイダ端末の好適なリーダの応答範囲内にあるときにのみNFCデバイスモジュール130をアクティブ化することができる。具体例として、このようなサービスプロバイダ端末のリーダは、比較的低電力の電波を発することができ、電波は、NFCデバイスモジュール130により利用されるアンテナ（例えば、共有アンテナ116又はNFC固有のアンテナ134）に電力供給し、それにより、そのアンテナが好適なNFC通信情報をNFCデータモジュール132からアンテナ116又はアンテナ134を介してそのようなサービスプロバイダ端末にNFC通信として送信することを可能にするために使用することができる。アクティブであるとき、NFCデバイスモジュール130は、電子デバイス100にとってローカルな電力ソース（例えば、電源108）を取り込み、そうでなければ電力ソースにアクセスすることができ、電力ソースは、共有アンテナ116又はNFC固有のアンテナ134が、受動的なNFCデバイスモジ

10

20

30

40

50

ジュール130の場合のように無線周波数信号を反射するのではなく、NFC通信情報をNFCデータモジュール132からアンテナ116又はアンテナ134を介してサービスプロバイダ端末220にNFC通信としてアクティブに送信することを可能にすることができる。サービスプロバイダ端末220は、サービスプロバイダサブシステム200のサービスプロバイダにより（例えば、ストアにて製品又はサービスをデバイス100のユーザに直接販売するためのサービスプロバイダのストアにて）提供されうる。NFC構成要素120について近距離無線通信に関して説明してきたが、好適な非接触近接ベースの任意のモバイル決済又は電子デバイス100とこのようなサービスプロバイダ端末の間の他の好適な任意のタイプの非接触近接ベース通信を提供するように構成要素120を構成してもよいことを理解されたい。例えば、電磁／静電結合技術を伴う通信などの好適な任意の近距離通信を提供するようにNFC構成要素120を構成することができる。代わりに、一部の実施形態では、プロセッサ102又はデバイス100の他の任意の部分にとって利用可能なデータを、デバイス100のNFC構成要素120とサービスプロバイダサブシステム200の端末220の間の好適な任意の非接触近接ベース通信5として通信することを可能にする好適な任意の構成要素を含むようにデバイス100のNFC構成要素120を構成してもよいが、NFC構成要素120は、資格アプレットを安全に記憶するように機能するセキュアエレメントを含んでもよく、含まなくてもよい。

【0068】

図1～図6に関して説明した処理の1つ、一部又は全てをそれぞれソフトウェアにより実施することができるが、ハードウェア、ファームウェア、又はソフトウェア、ハードウェア、及びファームウェアの任意の組合せで実装してもよい。これらの処理を実行するための命令を、マシン又はコンピュータ可読媒体上に記録されたマシン又はコンピュータ可読コードとして実装することもできる。一部の実施形態では、コンピュータ可読媒体は、非一時的なコンピュータ可読媒体とすることができる。このような非一時的なコンピュータ可読媒体の例には、非限定的に、リードオンリーメモリ、ランダムアクセスメモリ、フラッシュメモリ、CD-ROM、DVD、磁気テープ、リムーバブルメモリカード、及びデータ記憶デバイス（例えば、図2のメモリ104及び／又はメモリモジュール150）が含まれる。他の実施形態では、コンピュータ可読媒体は、一時的なコンピュータ可読媒体とすることができる。このような実施形態では、コンピュータ可読コードを分散形式で記憶し実行するように、一時的なコンピュータ可読媒体をネットワーク接続されたコンピュータシステム全体に分散させることができる。例えば、このような一時的なコンピュータ可読媒体を、好適な任意の通信プロトコルを使用して1つの電子デバイスから別の電子デバイスに通信することができる（（例えば、アプリケーション103の少なくとも一部分、及び／又はアプリケーション113の少なくとも一部分、及び／又はアプリケーション143の少なくとも一部分として）例えば、通信構成要素106を介してコンピュータ可読媒体を電子デバイス100に通信することができる）。このような一時的なコンピュータ可読媒体は、コンピュータ可読コード、命令、データ構造、プログラムモジュール、又は他のデータを搬送波又は他の搬送メカニズムなどの変調されたデータ信号内に他のデータを具現化することができ、任意の情報配信媒体を含むことができる。変調されたデータ信号は、1つ以上の特徴セットを有する信号としてもよく、信号中に情報を符号化するような方法で変化させてもよい。

【0069】

システム1のモジュール又は構成要素又はサブシステムのいずれか、それぞれ又は少なくとも1つを、ソフトウェア構成、ファームウェア構成、1つ以上のハードウェア構成要素、又はそれらの組合せとして提供してもよいことを理解されたい。例えば、システム1のモジュール又は構成要素又はサブシステムのいずれか、それぞれ又は少なくとも1つを、1つ以上のコンピュータ又は他のデバイスにより実行されうる、プログラムモジュールなどのコンピュータ実行可能命令の一般的な文脈で説明することができる。一般に、プログラムモジュールは、1つ以上の具体的なタスクを実行しうるか若しくは1つ以上の具体的な概要データタイプを実装しうる、1つ以上のルーチン、プログラム、オブジェクト、

10

20

30

40

50

コンポーネント、及び／又はデータ構造を含むことができる。システム１のモジュール及び構成要素及びサブシステムの数、構成、機能、及び相互接続が例示にすぎないこと、及び存在するモジュール、構成要素、及び／又はサブシステムの数、構成、機能、及び相互接続を修正又は省略してもよく、追加のモジュール、構成要素、及び／又はサブシステムを追加してもよく、いくつかのモジュール、構成要素、及び／又はサブシステムの相互接続を改変してもよいことも理解されたい。

【００７０】

システム１のモジュール又は構成要素又はサブシステムの１つ以上の少なくとも一部分は、好適な任意の方法でシステム１のエンティティ（例えば、アプリケーション１０３の少なくとも一部分及び／又はアプリケーション１１３の少なくとも一部分及び／又はアプリケーション１４３の少なくとも一部分として）例えば、デバイス１００のメモリ１０４）に記憶されることができ、そうでなければエンティティに対してアクセス可能とすることができる。例えば、ＮＦＣ構成要素１２０のモジュールのいずれか又はそれぞれを、好適な任意の技術を使用して（例えば、１つ以上の集積回路デバイスとして）実装してもよく、様々なモジュールが、構造、性能、及び動作において同一でもよく、同一でなくてもよい。システム１のモジュール又は他の構成要素のいずれか又はそれぞれを、拡張カード上に搭載してもよく、システムマザーボード上に直接搭載してもよく、システムチップセット構成要素（例えば、「ノースブリッジ」チップ）に組み込んでもよい。

【００７１】

システム１のモジュール又は構成要素のいずれか又はそれぞれ（例えば、ＮＦＣ構成要素１２０のモジュールのいずれか又はそれぞれ）は、種々のバス規格に適合された１つ以上の拡張カードを使用して実装された専用システムとすることができる。例えば、モジュールの全てを相互接続トされた様々な拡張カード上に搭載してもよく、１つの拡張カード上に搭載してもよい。ＮＦＣ構成要素１２０に関して、例のみとして、ＮＦＣ構成要素１２０のモジュールは、拡張スロット（例えば、ペリフェラルコンポーネントインターコネクト（「ＰＣＩ」）スロット又はＰＣＩエクスプレススロット）を通じてデバイス１００のマザーボード又はプロセッサ１０２とインターフェースすることができる。代わりに、ＮＦＣ構成要素１２０は、リムーバブルである必要はないが、モジュールの利用に専用のメモリ（例えば、ＲＡＭ）を含みうる１つ以上の専用モジュールを含んでもよい。他の実施形態では、ＮＦＣ構成要素１２０をデバイス１００に組み込むことができる。例えば、ＮＦＣ構成要素１２０のモジュールが、デバイス１００のデバイスメモリ１０４の一部分を利用することができる。システム１のモジュール又は構成要素のいずれか又はそれぞれ（例えば、ＮＦＣ構成要素１２０のモジュールのいずれか又はそれぞれ）は、それ自体の処理回路構成及び／又はメモリを含むことができる。代わりに、システム１のモジュール又は構成要素のいずれか又はそれぞれ（例えば、ＮＦＣ構成要素１２０のモジュールのいずれか又はそれぞれ）は、処理回路構成及び／又はメモリを、ＮＦＣ構成要素１２０の他の任意のモジュール及び／又はデバイス１００のプロセッサ１０２及び／又はメモリ１０４と共有してもよい。

【００７２】

電子デバイスとサービスプロバイダの間のセキュリティ保護された取引を管理するためのシステム、方法、及びコンピュータ可読媒体について説明してきたが、それらには、本明細書に説明する主題の趣旨及び範囲から逸脱せずに、いかなる方法でも多くの変更を施してよいことを理解されたい。当業者から見て、請求された主題からの本質的でなく、現在既知であるか又は後で考案された変更は、請求項の範囲内と均等であると明示的に考えられる。したがって、当業者にとって現在既知であるか又は今後既知となる明白な置換は、定義された要素の範囲内にあるものと定義される。

【００７３】

したがって、当業者は、限定ではなく例示を目的として提示される説明した実施形態とは異なる方法で本発明を実践できることを理解するであろう。

10

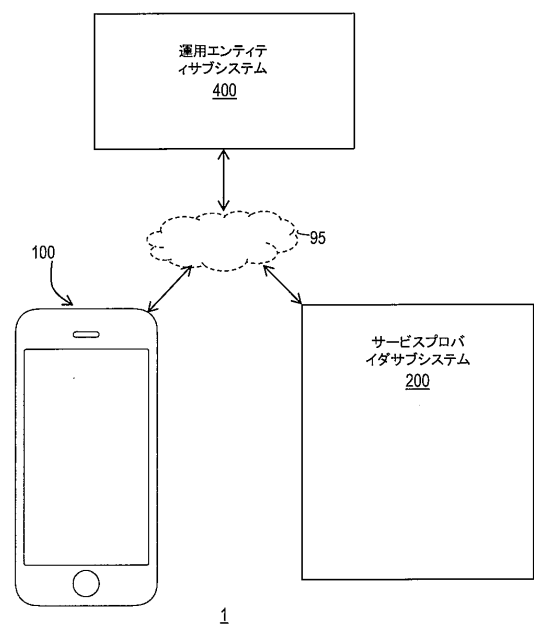
20

30

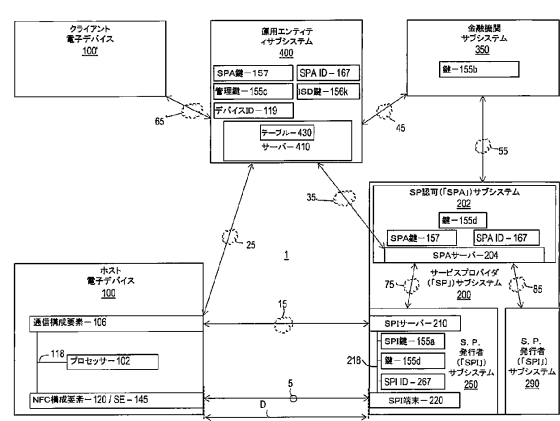
40

50

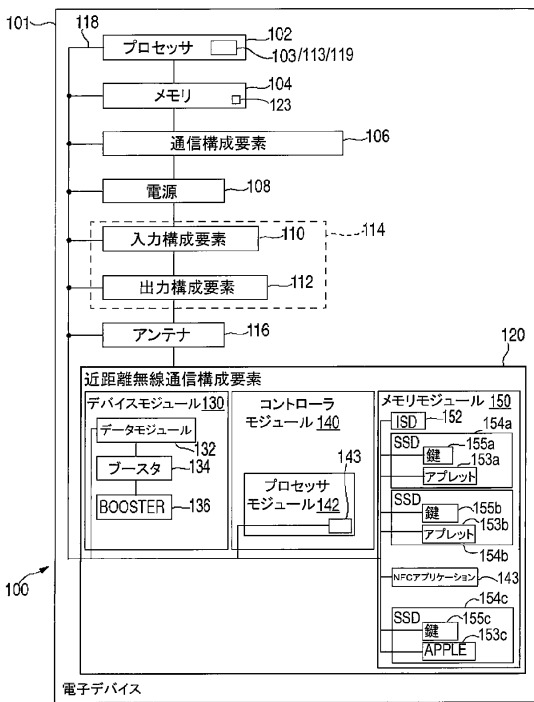
【図面】
【図 1】



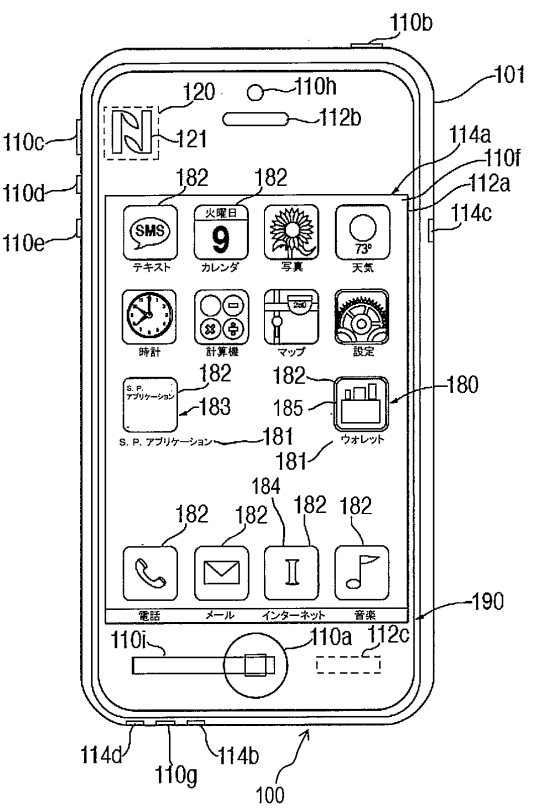
【図 1 A】



【図 2】



【図 3】



10

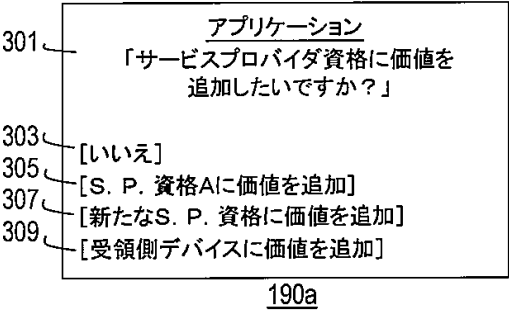
20

30

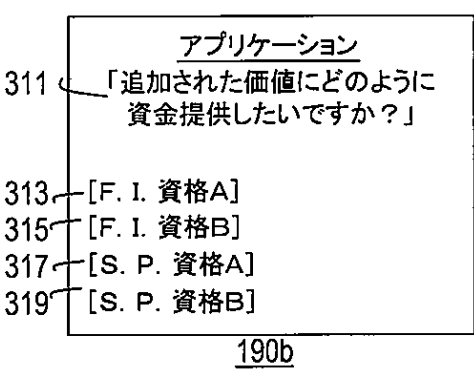
40

50

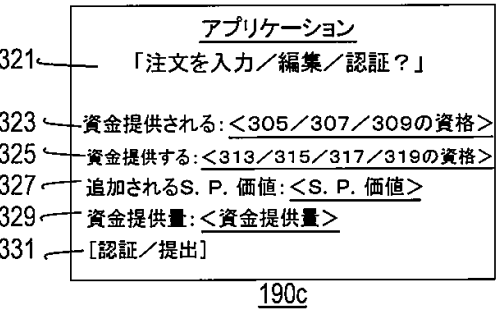
【図 3 A】



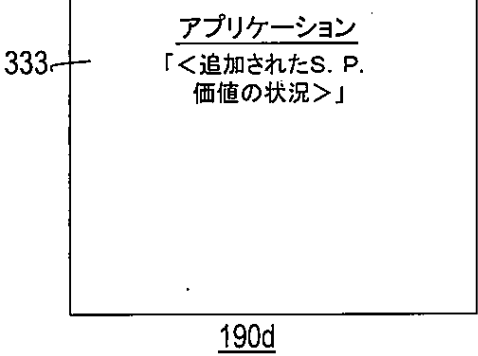
【図 3 B】



【図 3 C】



【図 3 D】



10

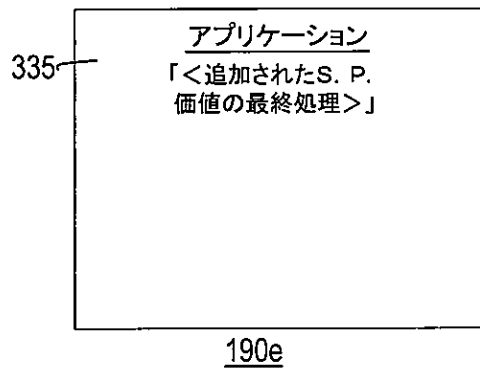
20

30

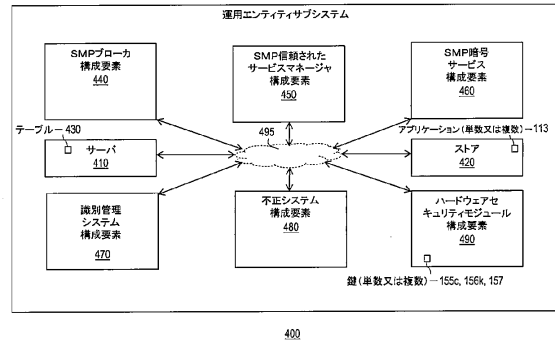
40

50

【図 3 E】

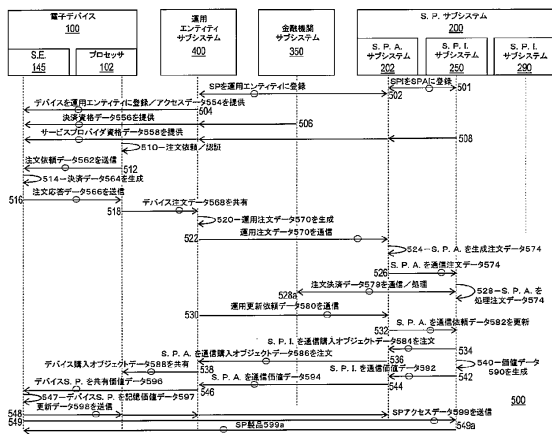


【図 4】

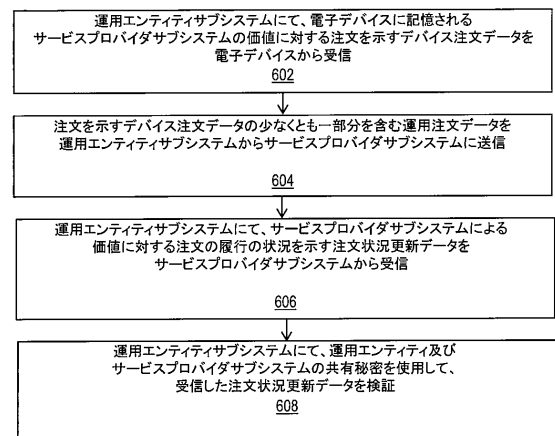


10

【図 5】



【図 6】



20

30

40

50

フロントページの続き

 米国(US)
(74)代理人 100139712
 弁理士 那須 威夫
(74)代理人 100210239
 弁理士 富永 真太郎
(72)発明者 マシュー シー バイイントン
 アメリカ合衆国 95014 カリフォルニア州 クパチーノ インフィニット ループ 1
(72)発明者 クリストファー シャープ
 アメリカ合衆国 95014 カリフォルニア州 クパチーノ インフィニット ループ 1
(72)発明者 ユーサフ エイチ ヴァイド
 アメリカ合衆国 95014 カリフォルニア州 クパチーノ インフィニット ループ 1
合議体
審判長 須田 勝巳
審判官 脇岡 剛
審判官 吉田 美彦
(56)参考文献 特開平11-003387 (JP, A)
 特表2015-533236 (JP, A)
 特表2015-528164 (JP, A)
 特表2015-506605 (JP, A)
 特表2015-524326 (JP, A)
(58)調査した分野 (Int.Cl., DB名)
 G09C1/00-5/00
 H04K1/00-3/00
 H04L9/00-9/04