(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6482601号
(P6482601)

(45)発行日　平成31年3月13日(2019.3.13)　(24)登録日　平成31年2月22日(2019.2.22)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G09C 1/00	(2006.01)	G09C	1/00	640D
G06Q 20/38	(2012.01)	G06Q	20/38	310

請求項の数 16　外国語出願　(全 55 頁)

(21)出願番号　特願2017-115083 (P2017-115083)
(22)出願日　平成29年6月12日 (2017.6.12)
(65)公開番号　特開2017-229065 (P2017-229065A)
(43)公開日　平成29年12月28日 (2017.12.28)
審査請求日　平成29年8月18日 (2017.8.18)
(31)優先権主張番号　62/349,003
(32)優先日　平成28年6月12日 (2016.6.12)
(33)優先権主張国　米国(US)

(73)特許権者　503260918
アップル　インコーポレイテッド
Ａｐｐｌｅ　Ｉｎｃ．
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　アップル　パーク　ウェイ　ワン
Ｏｎｅ　Ａｐｐｌｅ　Ｐａｒｋ　Ｗａｙ，Ｃｕｐｅｒｔｉｎｏ，　Ｃａｌｉｆｏｒｎｉａ　９５０１４，　Ｕ．Ｓ．Ａ．
(74)代理人　100094569
弁理士　田中　伸一郎
(74)代理人　100088694
弁理士　弟子丸　健
(74)代理人　100103610
弁理士　▲吉▼田　和彦

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】
運用エンティティサブシステムにおいて、
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前記電子デバイスから受信することと、
前記注文を示す前記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前記サービスプロバイダサブシステムに送信することと、
前記サービスプロバイダサブシステムによる価値に対する前記注文の履行の状況を示す注文状況更新データを前記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前記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、前記受信した注文状況更新データを検証することと
前記価値アイテムを含む注文履行データを前記サービスプロバイダサブシステムから受信することと、
前記受信した注文履行データの少なくとも前記価値アイテムを前記電子デバイスに送信することと、を含み、
前記送信した価値アイテムによって、前記電子デバイスが前記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が可能になることを特徴とする、方法。
【請求項２】
前記検証することは、前記共有秘密を使用して、前記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、請求項１に記載の方法。
【請求項３】
前記共有秘密は、前記注文状況更新データを前記受信する前に前記運用エンティティと前記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、請求項２に記載の方法。
【請求項４】
前記検証した後に、前記受信した注文状況更新データの少なくとも一部分を前記電子デバイスに送信することを更に含む、請求項１に記載の方法。
【請求項５】
運用エンティティサブシステムにおいて、
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前記電子デバイスから受信することと、
前記注文を示す前記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前記サービスプロバイダサブシステムに送信することと、
前記サービスプロバイダサブシステムによる価値に対する前記注文の履行の状況を示す注文状況更新データを前記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前記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、前記受信した注文状況更新データを検証することと
前記価値アイテムを含む注文履行データを前記サービスプロバイダサブシステムから受信することと、
前記受信した注文履行データの少なくとも前記価値アイテムを前記運用エンティティサブシステムから前記電子デバイスのセキュアエレメントにロードすることを含む、方法。
【請求項６】
前記デバイス注文データを受信した後に、前記運用エンティティサブシステムにて、前記運用エンティティ及び前記電子デバイスの共有秘密を使用して、前記受信したデバイス注文データの一部分を解読することと、
前記運用エンティティサブシステムにて、前記運用エンティティ及び前記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、前記受信したデバイス注文データの前記一部分を再暗号化することであって、前記運用注文データは、前記受信したデバイス注文データの前記再暗号化した部分を含む、ことと、
を更に含む、請求項１に記載の方法。
【請求項７】
前記受信したデバイス注文データの前記一部分は、前記注文の前記履行に資金提供するように機能する決済データを含む、請求項１に記載の方法。
【請求項８】
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であって、前記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つのメモリ構成要素と、
少なくとも１つの通信構成要素と、
を備え、前記運用エンティティシステムは、
前記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、前記受信したデバイス注文データは、前記電子デバイスに記憶される前記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、
前記受信したデバイス注文データに基づいて、前記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、前記運用注文データは前記価値アイテムに対する前記注文を示す、運用注文データを送信し、
前記送信した運用注文データに基づいて、前記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、前記サービスプロバイダ履行データは前記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、

前記受信したサービスプロバイダ履行データに基づいて、前記電子デバイスに運用履行データであって、前記運用履行データは前記価値アイテムを含む、運用履行データを送信する、

ように構成されており、

前記価値アイテムは、前記電子デバイスに記憶された価値の残高を更新するように構成されたスクリプトを含む、運用エンティティシステム。

【請求項９】

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であって、前記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つのメモリ構成要素と、

少なくとも１つの通信構成要素と、

を備え、前記運用エンティティシステムは、

前記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、前記受信したデバイス注文データは、前記電子デバイスに記憶される前記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、

前記受信したデバイス注文データに基づいて、前記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、前記運用注文データは前記価値アイテムに対する前記注文を示す、運用注文データを送信し、

前記送信した運用注文データに基づいて、前記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、前記サービスプロバイダ履行データは前記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、

前記受信したサービスプロバイダ履行データに基づいて、前記電子デバイスに運用履行データであって、前記運用履行データは前記価値アイテムを含む、運用履行データを送信する、

ように構成されており、かつ、

前記送信される運用履行データは、前記価値アイテムを前記電子デバイスのセキュアエレメントに提供するように構成されている、運用エンティティシステム。

【請求項１０】

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であって、前記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つのメモリ構成要素と、

少なくとも１つの通信構成要素と、

を備え、前記運用エンティティシステムは、

前記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、前記受信したデバイス注文データは、前記電子デバイスに記憶される前記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、

前記受信したデバイス注文データに基づいて、前記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、前記運用注文データは前記価値アイテムに対する前記注文を示す、運用注文データを送信し、

前記送信した運用注文データに基づいて、前記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、前記サービスプロバイダ履行データは前記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、

前記受信したサービスプロバイダ履行データに基づいて、前記電子デバイスに運用履行データであって、前記運用履行データは前記価値アイテムを含む、運用履行データを送信する、

ように構成されており、かつ、

前記送信される運用履行データは、前記価値アイテムを前記電子デバイスに提供するように構成されており、

前記提供された価値アイテムによって、前記電子デバイスが前記サービスプロバイダシステムの製品にアクセスすることが可能になる、運用エンティティシステム。

【請求項１１】

前記運用エンティティシステムは、前記運用エンティティシステム及び前記電子デバイスのセキュアエレメントの共有秘密を使用して、前記受信したサービスプロバイダ履行データの一部分を暗号化するように更に構成されており、

前記運用履行データは、前記受信したサービスプロバイダ履行データの前記暗号化された部分を含む、請求項１０に記載の運用エンティティシステム。

【請求項１２】

前記受信したサービスプロバイダ履行データの前記一部分は、前記価値アイテムを含む、請求項１１に記載の運用エンティティシステム。

【請求項１３】

前記運用エンティティシステムは、前記運用エンティティシステム及び前記サービスプロバイダシステムの共有秘密を使用して、前記受信したデバイス注文データの一部分を暗号化するように更に構成されており、

前記運用注文データは、前記受信したデバイス注文データの前記暗号化された部分を含む、請求項１０に記載の運用エンティティシステム。

【請求項１４】

前記受信したデバイス注文データの前記一部分は、前記価値アイテムに対する注文の履行に資金提供するように機能する決済データを含む、請求項１３に記載の運用エンティティシステム。

【請求項１５】

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であって、前記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つのメモリ構成要素と、

少なくとも１つの通信構成要素と、

を備え、前記運用エンティティシステムは、

前記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、前記受信したデバイス注文データは、前記電子デバイスに記憶される前記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、

前記受信したデバイス注文データに基づいて、前記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、前記運用注文データは前記価値アイテムに対する前記注文を示す、運用注文データを送信し、

前記送信した運用注文データに基づいて、前記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、前記サービスプロバイダ履行データは前記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、

前記受信したサービスプロバイダ履行データに基づいて、前記電子デバイスに運用履行データであって、前記運用履行データは前記価値アイテムを含む、運用履行データを送信する、

ように構成されており、かつ、

前記運用エンティティシステムは、前記受信したデバイス注文データにより指示された前記サービスプロバイダシステムを識別するように更に構成されており、

前記運用エンティティシステムは、前記識別されたサービスプロバイダシステムが前記運用エンティティシステムにより信頼されているかどうかを判定するように更に構成されており、

前記運用エンティティシステムは、前記識別されたサービスプロバイダシステムが前記運用エンティティシステムにより信頼されていると判定する場合、前記受信したデバイス注文データに基づいて、前記運用注文データを前記サービスプロバイダシステムに送信するように構成されている運用エンティティシステム。

【請求項１６】
非一時的なコンピュータ可読媒体と、
前記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、
前記注文を示す前記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前記サービスプロバイダシステムに送信させ、
前記送信した認可注文データに応じて、前記価値アイテムを含むサービスプロバイダ履行データを前記サービスプロバイダシステムから受信させ、
前記受信したサービスプロバイダ履行データの少なくとも前記価値アイテムを前記ターゲット電子デバイスに送信させ、
前記送信される少なくとも１つの前記価値アイテムは、前記価値アイテムを前記電子デバイスに提供するように構成されており、
前記提供された価値アイテムによって、前記電子デバイスが前記サービスプロバイダシステムの製品にアクセスすることを可能にする、
のに有効なコンピュータ可読命令と、を備える製品。
【発明の詳細な説明】
【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】
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。
【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。

【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。

【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。

【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。

【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るようになっている。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実に追跡するように、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）、ＺｉｇＢｅｅ（例えば、８０２．１５．４プロトコル）、ＷｉＤｉ（登録商標）、Ｅｔｈｅ

ｒｎｅｔ、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、又はそ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力しうる、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うる、実店舗又は任意の物理的な位置に位置しうる、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うる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により通信しうる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うる、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の識別子とすることができる。

【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、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収容し、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収容し、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、ＧｌｏｂａｌＰｌａｔｆｏｒｍ）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（「ＴＳＭＳＤ」）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）などと関連付けられた資格）を形成し、そうで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、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（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（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（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ＳＳＤ１５４ｃ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ＳＳＤ１５４ｃの鍵１５５ｃは、ＳＳＤ１５４ｃと運用エンティティサブシステム４００の間におけるＳＳＤ１５４ｃ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こ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イ、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ＳＳＤ１５４ｂ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ＳＳＤ１５４ｂ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ＳＳＤ１５４ｃは、他のＳＳＤ１５４（例えば、資格ＳＳＤ１５４ａ又は資格ＳＳＤ１５４ｂ）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ＳＳＤ１５４ｃ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ＳＳＤ１５４ａ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。

【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、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するときに、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うるレシート）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分として、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分として、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、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、ＰＡ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にとって一意でありうる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。

【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）、フリートカード、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。

【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。

【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ム３５０）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４００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１００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４００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４００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１００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ァイ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１００自体（例えば、デバイス１００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１００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１０３）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４００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３５０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４００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３５０によりエンドユーザデバイス１００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４００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１００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２００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してもよい。例えば、運用エンティティサブシステム４００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１１３、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２００を提供しうる、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、ＳＰＩサブシステム２５０、及び／又はＳＰＩサブシステム２９０）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２００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１００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２００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１００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１００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１００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１００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１００上に資格データを提供する間に、及び／又はデバイス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２５を介して）運用エンティティサブシステム４００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。

【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、バイオメト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。

【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、そうでなけ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る。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１１３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うる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みうる資格データ）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と関連付けられうる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、特定の方法でデバイス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る。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とリモートサブシス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、ＳＭＰＴＳＭ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ァイ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。

【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。

【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しう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イ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しう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、「仮想」資格又は仮想ＰＡＮ又はデバイスＰＡＮ（「Ｄ－ＰＡＮ」）をデバイス１００上に提供することができる。

【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資格に加えられうる最大価値を含む、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らかの価値の新たな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に示すように、選択肢３２３（例えば、画面１９０ａの応答３０５、３０７、及び３０９の１

つ）による価値を加えるためのターゲットＳＰ資格及び／又は選択肢３２５（例えば、画面１９０ｂの応答３１３、３１５、３１７、及び３１９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３２１を提示しうる画面１９０ｃを提示することができる。その上、画面１９０ｃは、選択肢３２７にて、選択肢３２３のターゲットＳＰ資格に加えられるＳＰ価値（例えば、減らされうる＄８０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１９０ｃは、選択肢３２９にて、選択肢３２５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ＳＰ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５１０にて、図３Ｃの画面１９０ｃは、ユーザを認証し、認証及び注文提出プロンプト３３１により選択肢３２５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１００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３３１の使用は、デバイス１００のセキュアエレメントにアクセスし、よって、提出されるＳＰ価値注文に資金提供するために使用される選択肢３２５の資金提供資格にアクセスするために、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入力をユーザに促すことを含むことができる。アクセスＳＳＤ１５４ｃは、他のＳＳＤ１５４（例えば、選択肢３２５の選択された資金提供資格と関連付けられた資格ＳＳＤ１５４）が、その資格情報をＳＰ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１５３ｃを活用することができる。動作５１０の単なる一例として、アクセスＳＳＤ１５４ｃのアプレット１５３ｃを、（例えば、ＧＵＩ１８０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のバイオメトリック入力構成要素１１０ｉなどの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、資格ＳＳＤ１５４ａ又は資格ＳＳＤ１５４ｂの資格により）ＳＰ価値注文取引に資金提供する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。

【００４１】

動作５１０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５００は、そのような認証情報及び（例えば、画面１９０ｃ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１０２により注文依頼データ５６２としてセキュアエレメント１４５に提供しうる動作５１２に進むことができる。例えば、注文依頼データ５６２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３２５（例えば、セキュアエレメント１４５上のＦＩ資格（例えば、アプレット１５３ｂ）のアプレット識別子又はセキュアエレメント１４５上のＳＰ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３２９の）資金提供量及び／又は（例えば、選択肢３２３（例えば、セキュアエレメント１４５上のＳＰ資格（例えば、アプレット１５３ａ）のアプレット識別子及び／又は具体的な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）追加される価値のターゲット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も含むことができる。注文依頼データ５６２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、価値の追加／補充）の選択を示すことができる。

【００４２】

つぎに、動作５１４及び５１６にて、処理５００は、デバイス１００（例えば、セキュアエレメント１４５）が決済データ５６４を生成し、暗号化し、注文応答データ５６６の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（「ＣＶＶ」））、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に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　ＩＤ２６７及び／又はＳＰＡ　ＩＤ１６７）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りうるように、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することができる。

【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に含まれう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／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際に使用するために、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う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５２２にて、好適な任意の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えないためである。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　ＩＤ１６７のみならずＳＰＩ　ＩＤ２６７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際に使用するために、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　ＩＤ２６７と関連付けられたＳＰＩサブシステム２５０）を定義する際に使用するために、ＳＰＩ　ＩＤ２６７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を識別する際に使用するために）例えば、ＳＰＡ　ＩＤ１６７ではなくＳＰＩ　ＩＤ２６７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　ＩＤ１６７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　ＩＤ２６７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　ＩＤ１６７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ＳＰＡ－ＳＰＩ鍵１５５ｄ（例えば、ＳＰＩサブシステム２５０とＳＰＡサブシステム２０

２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　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）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　ＳＳＤ１５４ｂ）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に含まれう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と関連付けられたアカウント（例えば、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らすことができ、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ＳＳＤ１５４ｂ）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２５０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　ＳＳＤ１５４ａ）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１５５ａ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５２８ａ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５２８ａ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ＳＳＤ１５４ａのアプレット１５３ａ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１５５ａ）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により受信されうるときに、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に、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）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、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、好適な任意のスキャナ又は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応答せずに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　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４

００が購入オブジェクトに応答しうるような「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ＳＰＡ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ＳＰＡ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、ＳＰＩ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ＳＰＡ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ＳＰＡサブシステム２０２に命令しうる、例えば、ＳＰＡ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ＳＰＡサブシステム２０２に戻すことができる）。ＳＰＡ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ＳＰＡ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ＳＰＩサブシステム２５０と通信することができる。例えば、ＳＰＡサブシステム２０２は、動作５３２にて、ＳＰＩ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ＳＰＡ更新依頼データ５８２をＳＰＩサブシステム２５０に通信することができ、次いで、ＳＰＩ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ＳＰＩ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、ＳＰＡ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ＳＰＡ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ＳＰＡ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。ＳＰＡ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ＳＰＶ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ＳＰＶ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ＳＰサブシステムの間のＳＰＶ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、ＳＰＡ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、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）ＳＰＶ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ＳＰ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ＳＰ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することができ、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ない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るようになっている。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（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、静止画プレイヤ、ゲームプレイヤ、他のメディアプレイヤ、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ＡｐｐｌｅＷａｔｃｈ（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。

【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。

【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、ダイアル、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。

【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、４２４ｋｂｐｓ）での近接範囲通信を可能にすることができ、ＩＳＯ／ＩＥＣ７８１６、ＩＳＯ／ＩＥＣ１８０９２、ＥＣＭＡ－３４０、ＩＳＯ／ＩＥＣ２１４８１、ＥＣＭＡ－３５２、ＩＳＯ１４４４３、及び／又はＩＳＯ１５６９３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、３７０Ｍｂｐｓ）での近接範囲通信を可能にしてもよく、ＴｒａｎｓｆｅｒＪｅｔ（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、１３．５６ＭＨｚ）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、耐タンパー性としうる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合した電子デバイス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Ｎ

ＦＣ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、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。

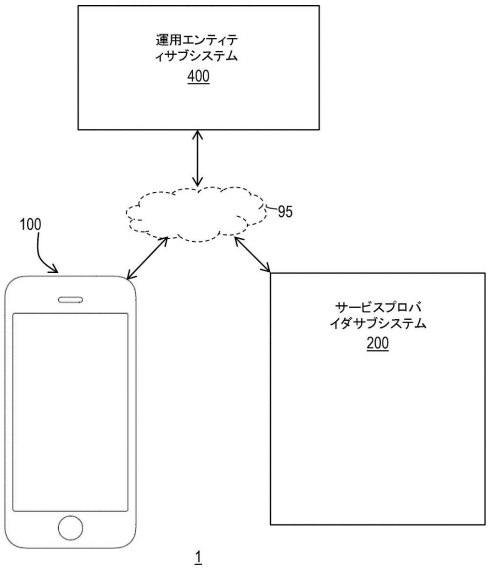
【００７２】

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。

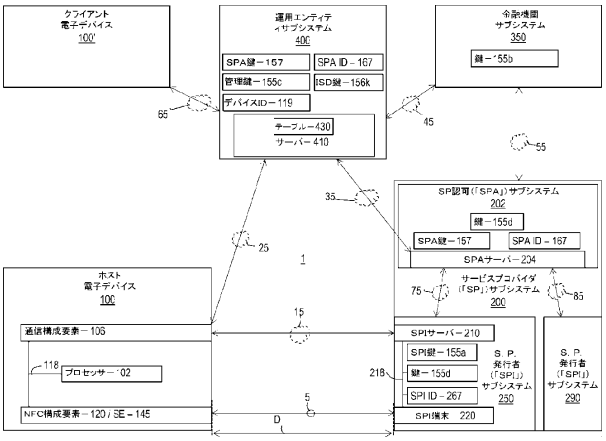
【００７３】

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。

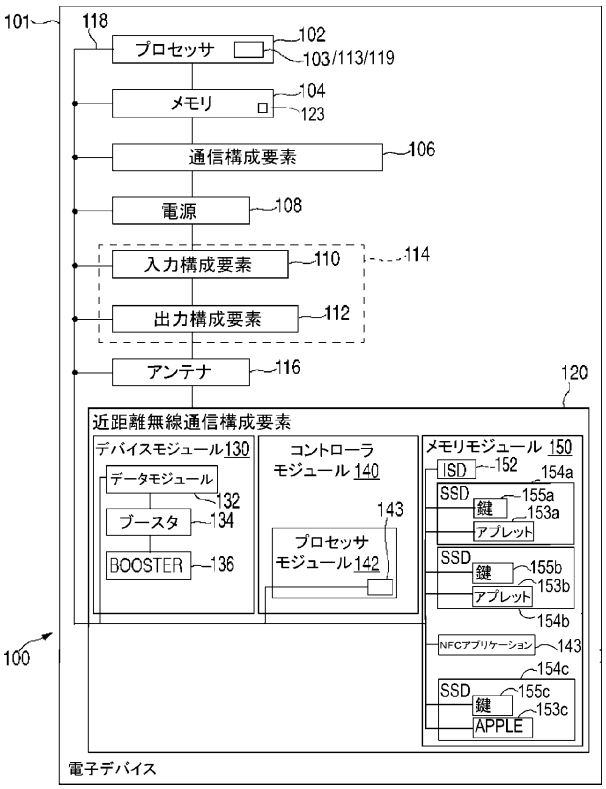
【図１】


運用エンティティサブシステム
400
95
100
サービスプロバイダサブシステム
200
1

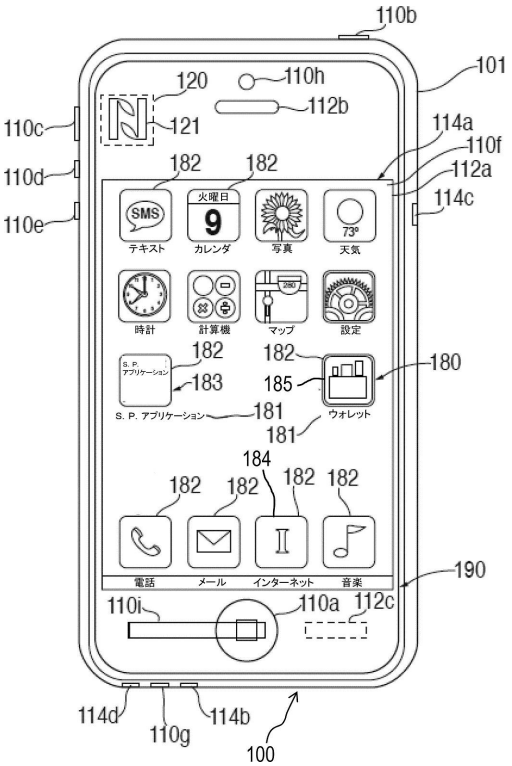
【図１Ａ】


クライアント電子デバイス
100'
運用エンティティサブシステム
400'
SPA鍵－157
SPA ID－167
管理鍵－155c
ISD鍵－156k
デバイスID－119
テーブル－430
サーバー 410
令記機関サブシステム
350
鍵－155b
55
45
35
SP認可（「SPA」）サブシステム
202
鍵－155d
SPA鍵－157
SPA ID－167
SPAサーバー－204
25
1
ホスト電子デバイス
100
サービスプロバイダ（「SP」）サブシステム
200
75
85
15
通信構成要素－106
SPIサーバー－210
118
プロセッサー－102
SPI鍵－155a
鍵－155d
S. P. 発行者（「SPI」）サブシステム
230
218
SPI ID－267
5
NFC構成要素－120 / SE－145
D
SPI端末 220

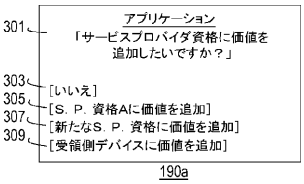
【図２】


101
118
プロセッサ
102
103/113/119
メモリ
104
123
通信構成要素
106
電源
108
入力構成要素
110
114
出力構成要素
112
アンテナ
116
120
近距離無線通信構成要素
デバイスモジュール130
データモジュール
132
ブースタ
134
BOOSTER
136
コントローラモジュール 140
143
プロセッサモジュール142
メモリモジュール 150
ISD
152
154a
SSD
鍵
155a
153a
アプレット
SSD
鍵
155b
153b
アプレット
154b
NFCアプリケーション
143
154c
SSD
鍵
155c
153c
APPLE
100
電子デバイス

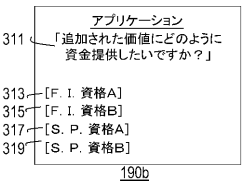
【図３】


110b
101
120
110h
112b
121
110c
110d
110e
114a
110f
112a
114c
182
182
SMS
テキスト
火曜日
9
カレンダ
写真
73°
天気
時計
計算機
マップ
設定
S. P. アプリケーション
182
183
182
185
180
S. P. アプリケーション
181
ウオレット
181
184
182
182
182
182
電話
メール
インターネット
音楽
190
110i
110a
112c
114d
110g
114b
100

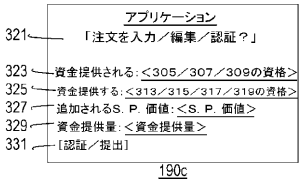
【図３Ａ】



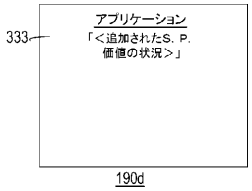
【図３Ｂ】



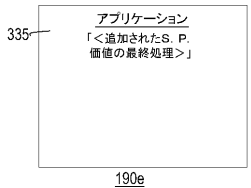
【図３Ｃ】



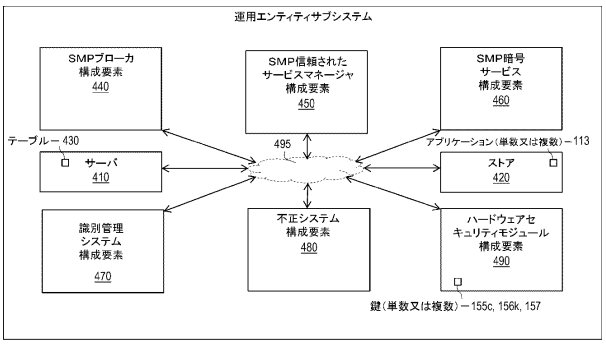
【図３Ｄ】



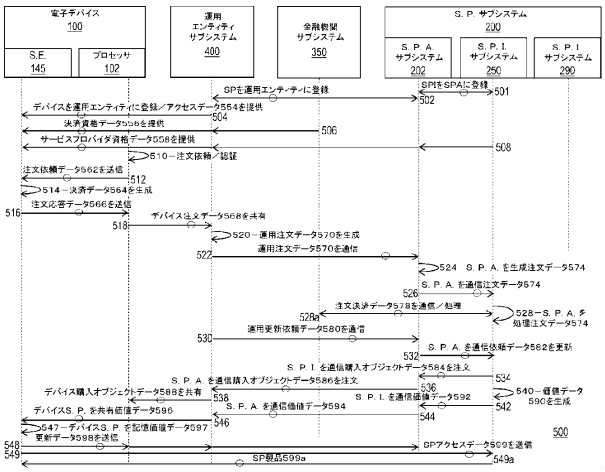
【図３Ｅ】



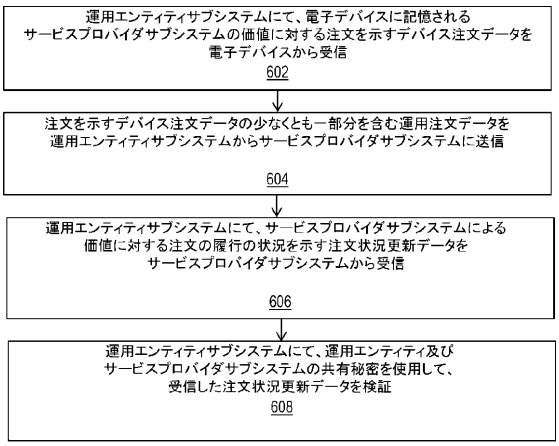
【図４】



【図５】



【図６】



フロントページの続き

(74)代理人 100067013
弁理士 大塚 文昭
(74)代理人 100086771
弁理士 西島 孝喜
(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

審査官 行田 悦資

(56)参考文献 特開平１１－００３３８７（ＪＰ，Ａ）
特開２０００－１７４７９７（ＪＰ，Ａ）
特開２００７－２５８７８９（ＪＰ，Ａ）
特開２００９－０４２９３３（ＪＰ，Ａ）
特開２００１－３４４５２４（ＪＰ，Ａ）
特開２００２－３６８７３０（ＪＰ，Ａ）
特表２０１６－５１３３１７（ＪＰ，Ａ）
特開２０１０－１１３４６２（ＪＰ，Ａ）
国際公開第２００５／０１１１９２（WO，Ａ１）
特開２００４－３５５０８５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｑ ２０／３８
Ｇ０９Ｃ １／００