

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6712328号

(P6712328)

(45) 発行日 令和2年6月17日 (2020.6.17)

(24) 登録日 令和2年6月2日 (2020.6.2)

(51) Int. Cl.	F I
H04L 9/32 (2006.01)	H04L 9/00 675A
G06F 21/44 (2013.01)	G06F 21/44
G06F 21/60 (2013.01)	G06F 21/60 360
G06Q 20/38 (2012.01)	G06Q 20/38 310

請求項の数 16 (全 100 頁)

(21) 出願番号	特願2018-559670 (P2018-559670)	(73) 特許権者	503260918
(86) (22) 出願日	平成29年1月3日 (2017.1.3)		アップル インコーポレイテッド
(65) 公表番号	特表2019-512192 (P2019-512192A)		Apple Inc.
(43) 公表日	令和1年5月9日 (2019.5.9)		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
(86) 国際出願番号	PCT/US2017/012036		One Apple Park Way,
(87) 国際公開番号	W02017/136092		Cupertino, California 95014, U. S. A.
(87) 国際公開日	平成29年8月10日 (2017.8.10)	(74) 代理人	100094569
審査請求日	平成30年8月1日 (2018.8.1)		弁理士 田中 伸一郎
(31) 優先権主張番号	62/289,656	(74) 代理人	100088694
(32) 優先日	平成28年2月1日 (2016.2.1)		弁理士 弟子丸 健
(33) 優先権主張国・地域又は機関	米国 (US)	(74) 代理人	100103610
(31) 優先権主張番号	62/297,923		弁理士 ▲吉▼田 和彦
(32) 優先日	平成28年2月21日 (2016.2.21)		
(33) 優先権主張国・地域又は機関	米国 (US)		

最終頁に続く

(54) 【発明の名称】 セキュアデバイス機能へのオンラインアクセスの妥当性検査

(57) 【特許請求の範囲】

【請求項 1】

処理サブシステムと、前記処理サブシステムに通信可能に結合された電子デバイスとの間でセキュアなトランザクションを行うための管理エンティティサブシステムを、前記電子デバイス上で実行されるオンラインリソースを介して使用する方法であって、

前記管理エンティティサブシステムにおいて、

前記オンラインリソースに対する妥当性検査要求を前記処理サブシステムから受信する処理であって、前記妥当性検査要求は前記オンラインリソースに関連する妥当性検査要求データを含み、前記妥当性検査要求データは、前記オンラインリソースをあらわす処理識別子を含む、当該処理と、

前記管理エンティティサブシステムで、前記妥当性検査要求データ及び登録データを用いて前記オンラインリソースを妥当性検査する処理であって、前記管理エンティティサブシステムが前記妥当性検査要求を受信する前に、前記登録データは最初に前記管理エンティティサブシステムにとって利用可能にされていた、当該処理と、

前記管理エンティティサブシステムで、妥当性検査レスポンスデータを前記妥当性検査要求データの少なくとも一部分と関連付ける処理と、

前記管理エンティティサブシステムで、前記オンラインリソースが妥当性検査された後、前記妥当性検査レスポンスデータを前記電子デバイスに通信する処理と、

前記管理エンティティサブシステムで、前記妥当性検査レスポンスデータを前記電子デバイスに通信した後、前記電子デバイスからデバイストランザクションデータを受信す

10

20

る処理と、

前記管理エンティティサブシステムで、前記妥当性検査レスポンスデータを用いて前記デバイストラランザクションデータを妥当性検査する処理と、

前記管理エンティティサブシステムで、前記デバイストラランザクションデータが妥当性検査された後、前記処理サブシステムによって使用されるセキュアトラランザクションデータを生成する処理と、が実行され、

前記セキュアトラランザクションデータは、前記デバイストラランザクションデータの少なくとも第1の部分を含み、

前記登録データは、前記処理識別子、及び前記管理エンティティサブシステムと前記処理サブシステムの間の処理共有秘密を含み、

前記オンラインリソースを前記妥当性検査する処理は、前記妥当性検査要求データを解読するために、前記処理共有秘密を用いて、前記妥当性検査要求データから前記処理識別子にアクセスすることを含む、方法。

【請求項2】

前記妥当性検査要求データは妥当性検査セッション識別子を含み、

前記妥当性検査レスポンスデータの少なくとも1つ又は前記妥当性検査要求データの前記少なくとも一部分が、前記妥当性検査セッション識別子を含む、請求項1に記載の方法。

【請求項3】

前記妥当性検査セッション識別子は、前記電子デバイスによって生成されたデータを含む、請求項2に記載の方法。

【請求項4】

前記妥当性検査要求は前記処理サブシステムの支払いサービスプロバイダーサブシステムから前記管理エンティティサブシステムで受信される、請求項3の方法。

【請求項5】

前記妥当性検査セッション識別子は、前記処理サブシステムによって生成されたデータを含む、請求項2に記載の方法。

【請求項6】

処理サブシステムと、前記処理サブシステムに通信可能に結合された電子デバイスとの間でセキュアなトラランザクションを行うための管理エンティティサブシステムを、前記電子デバイス上で実行されるオンラインリソースを介して使用する方法であって、

前記管理エンティティサブシステムにおいて、

前記オンラインリソースに対する妥当性検査要求を前記処理サブシステムから受信する処理であって、前記妥当性検査要求は前記オンラインリソースに関連する妥当性検査要求データを含み、前記妥当性検査要求データは、前記オンラインリソースをあらわす処理識別子を含む、当該処理と、

前記管理エンティティサブシステムで、前記妥当性検査要求データ及び登録データを用いて前記オンラインリソースを妥当性検査する処理であって、前記管理エンティティサブシステムが前記妥当性検査要求を受信する前に、前記登録データは最初に前記管理エンティティサブシステムにとって利用可能にされていた、当該処理と、

前記管理エンティティサブシステムで、妥当性検査レスポンスデータを前記妥当性検査要求データの少なくとも一部分と関連付ける処理と、

前記管理エンティティサブシステムで、前記オンラインリソースが妥当性検査された後、前記妥当性検査レスポンスデータを前記電子デバイスに通信する処理と、

前記管理エンティティサブシステムで、前記妥当性検査レスポンスデータを前記電子デバイスに通信した後、前記電子デバイスからデバイストラランザクションデータを受信する処理と、

前記管理エンティティサブシステムで、前記妥当性検査レスポンスデータを用いて前記デバイストラランザクションデータを妥当性検査する処理と、

前記管理エンティティサブシステムで、前記デバイストラランザクションデータが妥当

10

20

30

40

50

性検査された後、前記処理サブシステムによって使用されるセキュアトランザクションデータを生成する処理と、が実行され、

前記セキュアトランザクションデータは、前記デバイストランザクションデータの少なくとも第1の部分を含み、

前記妥当性検査レスポンスデータは、ランダムデータを含み、

前記関連付ける処理は、前記管理エンティティサブシステムで前記処理識別子に対して前記ランダムデータを記憶することを含む、方法。

【請求項7】

前記登録データは、前記処理識別子と、前記管理エンティティサブシステムと前記処理サブシステムとの間の処理共有秘密とを含み、

前記セキュアトランザクションデータを前記生成する処理は、前記処理共有秘密を用いて前記デバイストランザクションデータの一部分を暗号化することを含む、請求項6に記載の方法。

【請求項8】

前記処理識別子は、前記オンラインリソースを介した、前記電子デバイスと前記処理サブシステムとの間のトランザクションに一意である妥当性検査セッション識別子を含む、請求項6に記載の方法。

【請求項9】

前記妥当性検査レスポンスデータを前記電子デバイスに前記通信する処理は、

前記管理エンティティサブシステムと前記電子デバイスとの間の共有秘密を用いて、前記管理エンティティサブシステムにおいて、前記ランダムデータに署名することと、

前記署名されたランダムデータを前記電子デバイスと共有することと、を含む、請求項6に記載の方法。

【請求項10】

前記デバイストランザクションデータは、前記デバイストランザクションデータが前記ランダムデータを含むことを判定することによって認証される、請求項9に記載の方法。

【請求項11】

前記妥当性検査レスポンスデータを前記電子デバイスに前記通信する処理は、前記ランダムデータ及び前記処理識別子を前記電子デバイスと共有することを含み、

前記デバイストランザクションデータは、前記デバイストランザクションデータの少なくとも第2の部分が前記管理エンティティサブシステムにおいて前記処理識別子に対して記憶されていることを判定することによって認証される、請求項6に記載の方法。

【請求項12】

前記処理識別子に対して前記ランダムデータを前記記憶することは、前記管理エンティティサブシステムにおいて前記処理識別子に対して記憶された前記ランダムデータを特定の時間を越えない時間保持することを含む、請求項11に記載の方法。

【請求項13】

処理サブシステムと、前記処理サブシステムに通信可能に結合された電子デバイスとの間でセキュアなトランザクションを行うための管理エンティティサブシステムを、前記電子デバイス上で実行されるオンラインリソースを介して使用する方法であって、

前記管理エンティティサブシステムにおいて、

前記オンラインリソースに対する妥当性検査要求を前記処理サブシステムから受信する処理であって、前記妥当性検査要求は前記オンラインリソースに関連する妥当性検査要求データを含み、前記妥当性検査要求データは、前記オンラインリソースをあらゆる処理識別子を含む、当該処理と、

前記管理エンティティサブシステムで、前記妥当性検査要求データ及び登録データを用いて前記オンラインリソースを妥当性検査する処理であって、前記管理エンティティサブシステムが前記妥当性検査要求を受信する前に、前記登録データは最初に前記管理エンティティサブシステムにとって利用可能にされていた、当該処理と、

前記管理エンティティサブシステムで、妥当性検査レスポンスデータを前記妥当性検査

10

20

30

40

50

査要求データの少なくとも一部分と関連付ける処理と、

前記管理エンティティサブシステムで、前記オンラインリソースが妥当性検査された後、前記妥当性検査レスポンスデータを前記電子デバイスに通信する処理と、

前記管理エンティティサブシステムで、前記妥当性検査レスポンスデータを前記電子デバイスに通信した後、前記電子デバイスからデバイストランザクションデータを受信する処理と、

前記管理エンティティサブシステムで、前記妥当性検査レスポンスデータを用いて前記デバイストランザクションデータを妥当性検査する処理と、

前記管理エンティティサブシステムで、前記デバイストランザクションデータが妥当性検査された後、前記処理サブシステムによって使用されるセキュアトランザクションデータを生成する処理と、が実行され、

前記セキュアトランザクションデータは、前記デバイストランザクションデータの少なくとも第1の部分を含み、

前記妥当性検査要求データは、前記オンラインリソースを介した前記電子デバイスと前記処理サブシステムとの間のトランザクションを示すトランザクション識別情報を含み、

前記妥当性検査レスポンスデータはランダムデータを含み、

前記関連付けることは、前記管理エンティティサブシステムにおいて前記トランザクション識別情報に対して前記ランダムデータを記憶することを含み、

前記妥当性検査レスポンスデータを前記電子デバイスに前記通信することは、前記ランダムデータを前記電子デバイスと共有することを含み、

前記デバイストランザクションデータは、デバイストランザクション識別情報を含み、前記デバイストランザクションデータは、

前記デバイストランザクションデータが前記ランダムデータを含むことを判定することと、

前記デバイストランザクションデータの前記デバイストランザクション識別情報が前記潜在的トランザクション識別情報の閾値内にあると判定することによって認証される、方法。

【請求項14】

処理サブシステムと、前記処理サブシステムに通信可能に結合された電子デバイスとの間のセキュアなトランザクションを、前記電子デバイス上で実行されるオンラインリソースを介して行う管理エンティティサブシステムを使用する方法であって、

前記管理エンティティサブシステムにおいて、

前記オンラインリソースに対する妥当性検査要求を前記処理サブシステムから受信する処理あって、前記妥当性検査要求は前記オンラインリソースに関連する妥当性検査要求データを含み、前記妥当性検査要求データは前記オンラインリソースを介した前記電子デバイスと前記処理サブシステムとの間のトランザクションを示すトランザクション識別情報を含む、当該処理と、

前記管理エンティティサブシステムで、前記妥当性検査要求データの少なくとも一部分を用いて前記オンラインリソースを妥当性検査する処理と、

前記管理エンティティサブシステムで、妥当性検査レスポンスデータを、少なくとも前記トランザクション識別情報と関連付ける処理と、

前記管理エンティティサブシステムで、前記オンラインリソースが妥当性検査された後、前記妥当性検査レスポンスデータを前記電子デバイスに通信する処理と、

前記管理エンティティサブシステムで、前記妥当性検査レスポンスデータを前記電子デバイスに通信した後、前記電子デバイスからデバイストランザクションデータを受信する処理と、

前記管理エンティティサブシステムで、前記妥当性検査レスポンスデータ及び前記トランザクション識別情報を用いて前記デバイストランザクションデータを妥当性検査する処理と、

前記管理エンティティサブシステムで、前記デバイストランザクションデータが妥当

10

20

30

40

50

性検査された後、前記処理サブシステムによって使用されるセキュアランザクションデータを生成する処理であって、前記セキュアランザクションデータは、前記デバイスランザクションデータの少なくとも第1の部分である、当該処理を実行する、方法。

【請求項15】

前記妥当性検査レスポンスデータはランダムデータを含み、

前記関連付ける処理は、前記管理エンティティサブシステムにおいて前記ランザクション識別情報に対して前記ランダムデータを記憶することを含み、

前記妥当性検査レスポンスデータを前記電子デバイスに前記通信する処理は、前記ランダムデータを前記電子デバイスと共有することを含み、

前記デバイスランザクションデータはデバイスランザクション識別情報を含み、

前記デバイスランザクションデータは、

前記デバイスランザクションデータが前記ランダムデータを含むことを判定すること、及び

前記デバイスランザクションデータの前記デバイスランザクション識別情報が前記ランザクション識別情報の閾値内にあると判定することによって認証される、請求項14に記載の方法。

【請求項16】

前記オンラインリソースを前記妥当性検査する処理は、前記妥当性検査要求データ及び登録データの前記少なくとも一部分を用いることを含み、

前記登録データは前記妥当性検査要求を受信する前に、最初に前記管理エンティティサブシステムにとって利用可能にされており、

前記登録データは前記管理エンティティサブシステムと前記処理サブシステムとの間の処理共有秘密を含み、

前記セキュアランザクションデータを前記生成する処理は、前記処理共有秘密を用いて前記デバイスランザクションデータの前記第1の部分を暗号化することを含む、請求項14に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

(関連出願（単数又は複数）の相互参照)

本出願は、2016年2月1日に出願された先出願の米国特許仮出願第62/289,656号、2016年2月21日に出願された先出願の米国特許仮出願第62/297,923号、2016年6月12日に出願された先出願の米国特許仮出願第62/348,960号、及び2016年6月12日に出願された先出願の米国特許仮出願第62/348,979号の利益を主張するものであり、それらの各出願は、その全体が参照により本明細書に組み込まれる。

本開示は、セキュアデバイス機能へのオンラインアクセスを妥当性検査することに関し、より具体的には、サードパーティサブシステムによる電子デバイスのセキュア機能へのオンラインアクセスを可能とするための、サードパーティサブシステムの妥当性検査に関する。

【0002】

(開示の背景)

ポータブル電子デバイス（例えば、携帯電話）は、他のエンティティ（例えば販売事業者）との機密データの非接触近接型通信を可能とする近距離無線通信（「NFC」）構成要素を備えることがある。こうしたデータのランザクションにおいては、電子デバイスは、クレジットカードクレデンシャルなどのネイティブ決済クレデンシャルを生成し、アクセスし、及び／又は他のエンティティとの間で共有することが必要となる。しかし、他のタイプの通信（例えば、オンラインランザクション）における電子デバイスによってそのようなネイティブ決済クレデンシャルをセキュアに使用することは、非効率的であることが多い。

【発明の概要】

【0003】

本明細書では、セキュアデバイス機能へのオンラインアクセスを妥当性検査するためのシステム、方法、及びコンピュータ可読媒体を記載する。

【0004】

例として、販売事業者オンラインリソースを介した販売事業者サブシステムと、販売事業者サブシステムに通信可能に結合された電子デバイスとの間でセキュアなトランザクションを行う商業エンティティサブシステムを使用する方法が提供される。本方法は、商業エンティティサブシステムにおいて、販売事業者サブシステムから、販売事業者オンラインリソースに対する妥当性検査要求を受信することと、妥当性検査要求及びその受信前に最初に商業エンティティサブシステムに利用可能にされた登録データを用いてオンライン販売事業者リソースを妥当性検査することと、妥当性検査した後に、妥当性検査要求の少なくとも一部分に関連付けた妥当性検査データを生成することと、電子デバイスに妥当性検査データを通信することと、電子デバイスからデバイストランザクションデータを受信することと、デバイストランザクションデータが妥当性検査データを含むことを判定することと、判定した後、販売事業者サブシステムが使用するためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することと、を含むことができる。

10

【0005】

別の例として、管理エンティティサブシステムを使用して、処理サブシステムと、処理サブシステムと通信可能に結合された電子デバイスとの間のセキュアなトランザクションを、電子デバイス上で実行されるオンラインリソースを介して行う方法を提供することができる。本方法は、管理エンティティサブシステムにおいて、オンラインリソースに対する妥当性検査要求を受信することと、妥当性検査要求は妥当性検査要求データを含むことと、妥当性検査要求データ及び登録データを用いてオンラインリソースを妥当性検査することと、登録データは妥当性検査要求の受信前に最初に管理エンティティサブシステムに利用可能とされていることと、オンラインリソースが妥当性検査された後、妥当性検査レスポンスデータを妥当性検査要求データの少なくとも一部分と関連付けることと、妥当性検査レスポンスデータを電子デバイスに通信することと、妥当性検査レスポンスデータを電子デバイスに通信した後、デバイストランザクションデータを電子デバイスから受信することと、妥当性検査レスポンスデータを用いてデバイストランザクションデータを妥当性検査することと、デバイストランザクションデータが妥当性検査された後、処理サブシステムが使用するためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することと、を含むことができる。

20

30

【0006】

更に別の例として、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介して処理サブシステムに通信可能に結合されている電子デバイスとの間のセキュアなトランザクションを可能とする管理エンティティサブシステムを使用する方法を提供することができる。本方法は、管理エンティティサブシステムにおいて、オンラインリソースを登録することと、管理エンティティサブシステムと処理サブシステムとの間で処理共有秘密を確立することを含むことと、オンラインリソースに対する妥当性検査要求を受信することと、妥当性検査要求はオンラインリソースを示す処理識別子を含み、また妥当性検査要求は、オンラインリソースを介した、電子デバイスと処理サブシステムとの間の潜在的トランザクションに一意である妥当性検査セッション識別子を更に含むことと、妥当性検査セッション識別子と処理共有秘密を用いて処理識別子が示すオンラインリソースを妥当性検査することと、を含むことができる。

40

【0007】

更に別の例として、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介して処理サブシステムに通信可能に結合された電子デバイスとの間でセキュアなトランザクションを行うために管理エンティティサブシステムを使用する方法を提供する

50

ことができる。本方法は、管理エンティティサブシステムにおいて、オンラインリソースに対する妥当性検査要求を受信することであって、この妥当性検査要求は妥当性検査要求データを含み、また妥当性検査要求データは、オンラインリソースを介した、電子デバイスと処理サブシステムとの間の潜在的トランザクションを示す潜在的トランザクション識別情報を含むことと、妥当性検査要求データの少なくとも一部分を用いてオンラインリソースを妥当性検査することと、妥当性検査レスポンスデータを少なくとも潜在的トランザクション識別情報と関連付けることと、オンラインリソースが妥当性検査された後、妥当性検査レスポンスデータを電子デバイスに通信することと、妥当性検査レスポンスデータを電子デバイスに通信した後、デバイストランザクションデータを電子デバイスから受信することと、妥当性検査レスポンスデータ及び潜在的トランザクション識別情報を用いてデバイストランザクションデータを妥当性検査することと、デバイストランザクションデータが妥当性検査された後、処理サブシステムが使用するためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することと、を含むことができる。

10

【0008】

この「発明の概要」は、本明細書で説明する主題のいくつかの態様の基本的理解を提供するように、いくつかの例示的实施形態を要約することのみを目的として提供されるものに過ぎない。したがって、この「発明の概要」に説明した特徴は、単なる例であって、いかなる方式でも、本明細書で説明される主題の範囲又は趣旨を狭めるものとして解釈すべきではないことを理解されたい。特に明記しない限り、一実施例のコンテキストで説明される特徴は、1つ以上の他の実施例のコンテキストで説明される特徴と組合せてもよいし、それとともに使用されてもよい。本明細書で説明される主題の、他の特徴、態様、及び利点は、以下の「発明を実施するための形態」、図、及び「特許請求の範囲」から明らかとなるであろう。

20

【図面の簡単な説明】

【0009】

以下の説明では以下の図面を参照し、同様の参照文字は全体にわたって同様の部分を参照する。

【0010】

【図1】セキュアデバイス機能へのオンラインアクセスを妥当性検査するための例示的なシステムの概略図である。

30

【図1A】図1のシステムのより詳細な別の概略図である。

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

【図2A】図1～図2の例示の電子デバイスのより詳細な別の概略図である。

【図3】図1～図2Aの例示の電子デバイスの正面図である。

【図3A】セキュアデバイス機能へのオンラインアクセスを妥当性検査するプロセスを図示する図1～図3のうちの1つ以上の例示の電子デバイスのグラフィカルユーザインタフェースの画面の正面図である。

【図3B】セキュアデバイス機能へのオンラインアクセスを妥当性検査するプロセスを図示する図1～図3のうちの1つ以上の例示の電子デバイスのグラフィカルユーザインタフェースの画面の正面図である。

40

【図3C】セキュアデバイス機能へのオンラインアクセスを妥当性検査するプロセスを図示する図1～図3のうちの1つ以上の例示の電子デバイスのグラフィカルユーザインタフェースの画面の正面図である。

【図3D】セキュアデバイス機能へのオンラインアクセスを妥当性検査するプロセスを図示する図1～図3のうちの1つ以上の例示の電子デバイスのグラフィカルユーザインタフェースの画面の正面図である。

【図4】図1及び図1Aのシステムの例示の商業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】セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセ

50

スのフローチャートである。

【図6】セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセスのフローチャートである。

【図7】セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセスのフローチャートである。

【図8】セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセスのフローチャートである。

【図9】セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセスのフローチャートである。

【発明を実施するための形態】

10

【0011】

処理（又は販売事業者）サブシステムは、パートナ・ペイメント・サービス・プロバイダ（PSP）の有無にかかわらず、処理サブシステムの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又はウェブサイト）が、PSPに組み込まれた決済フォームの有無にかかわらず、機密データ（例えば、セキュアエレメント決済クレデンシャルデータ）をユーザ電子デバイスからセキュアに受信するために使用される前に、信頼された管理（又は商業）エンティティサブシステムによって妥当性検査され得る。更に、オンラインリソースの妥当性検査に加えて、オンラインリソースが機能して、処理サブシステムとのトランザクションにおいて機密データを共有するオプションをユーザデバイスに提示する前に、特定のトランザクションを可能とするためのオンラインリソース使用を再許可するために、このようなオプションの選択に応じた追加的なセッション妥当性検査プロセスが実行され得る。

20

【0012】

図1及び図1Aでは、1つ以上のクレデンシャルが、金融機関（又はトランザクション若しくは発行者）サブシステム350から、商業（又は管理）エンティティサブシステム400と連携して、電子デバイス100に供給され、電子デバイス100はこのようなクレデンシャルを使用して販売事業者（又は処理）サブシステム200及び関連付けられた取得銀行（又は取得者）サブシステム300とのトランザクション（例えば、財務トランザクション又は任意の他の好適なセキュアなデータトランザクション）を行うことができる（例えば、電子デバイス100のセキュアデバイス機能）、システム1を示す。一方、図2～図3はシステム1の電子デバイス100の特定の実施形態に関する更なる詳細を示し、図3A～図3Dは、このようなトランザクション実行中のシステム1の電子デバイス100のグラフィカルユーザインタフェースとして代表的な例示画面190a～190dを示しており、図4は、システム1の商業エンティティサブシステム400の特定の実施形態に関する更なる詳細を示すとともに、図5～図9は、（例えば、このような財務トランザクションを行う）セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセスのフローチャートである。

30

【0013】

図1の説明

図1は、販売事業者サブシステムとのトランザクション（例えば、オンライン決済又は非接触近接型決済）における電子デバイス上のクレデンシャルのセキュアな使用を可能とする販売事業者（又は処理）サブシステムの妥当性検査など、サードパーティサブシステムによる電子デバイスのセキュア機能へのオンラインアクセスを可能とするサードパーティサブシステムの妥当性検査を可能にし得る例示的なシステム1の概略図である。例えば、図1に示すように、システム1は、電子デバイス100、ならびに電子デバイス100に1つ以上のクレデンシャルをセキュアに供給するための、商業（又は管理）エンティティサブシステム400及び金融機関（又はトランザクション若しくは発行者）サブシステム350を含むことができる。また、図1に示すように、システム1は販売事業者（又は処理）サブシステム200を含んでもよく、それによって、このように供給されたクレデンシャルは、販売事業者サブシステム200とのトランザクション（例えば、財務トラン

40

50

ザクション又は任意の他の公的なセキュアなデータトランザクション)を行うために電子デバイス100によって使用され得る。例えば、販売事業者サブシステム200からの潜在的トランザクションデータの受信に応じて、電子デバイス100は、販売事業者サブシステム200との特定の財務トランザクションに資金供給するため、非接触近接型通信5(例えば、近距離無線通信又はBluetooth(登録商標)通信)として、及び/又はオンライン型通信684(例えば、ネットワーク電気通信など)として、供給されたクレデンシャルのセキュアデバイスデータを、販売事業者サブシステム200と共有することができる。システム1はまた、金融機関サブシステム350とのトランザクションを完了するために、このような非接触近接型通信5及び/又はこのようなオンライン型通信684を利用し得る取得銀行(又は取得者)サブシステム300も含むことができる。

10

【0014】

システム1は、電子デバイス100と販売事業者サブシステム200との間の通信を可能とする通信経路15と、販売事業者サブシステム200と取得銀行サブシステム300との間の通信を可能とする通信経路25と、取得銀行サブシステム300と金融機関サブシステム350との間の通信を可能とする通信経路35と、金融機関サブシステム350の決済ネットワークサブシステム360と金融機関サブシステム350の発行銀行サブシステム370との間の通信を可能とする通信経路45と、金融機関サブシステム350と商業エンティティサブシステム400との間の通信を可能とする通信経路55と、商業エンティティサブシステム400と電子デバイス100との間の通信を可能とする通信経路65と、金融機関サブシステム350と電子デバイス100との間の通信を可能とする通信経路75と、商業エンティティサブシステム400と販売事業者サブシステム200との間の通信を可能とする通信経路85と、を含むことができる。経路15、25、35、45、55、65、75、85のうち1つ以上は、1つ以上の信頼されたサービスマネージャ(「TSM」)によって少なくとも部分的に管理され得る。任意の好適な回路、デバイス、システム、又は、通信ネットワークを作成するように機能し得るこれらの組合せ(例えば、1つ以上の通信タワー、電気通信サーバ等を含み得る有線通信インフラ及び/又は無線通信インフラ)は、任意の好適な有線又は無線通信プロトコルを用いて通信を提供可能にし得る経路15、25、35、45、55、65、75、85のうち1つ以上を提供するのに使用することができる。例えば、経路15、25、35、45、55、65、75、85のうち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)、イーサネット(登録商標)、Bluetooth(登録商標)、BLE、高周波数システム(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ブリッジング、無線及び携帯電話ならびに個人用電子メールデバイス(例えば、GSM(登録商標)、GSM(登録商標)+EDGE、CDMA、OFDMA、HSPA、multi-band等)により使用され得る任意の通信プロトコル、低出力のWireless Personal Area Network(6LoWPAN)モジュールにより使用され得る任意の通信プロトコル、あらゆる他の通信プロトコル、又はこれらのあらゆる組合せをサポートすることができる。

20

30

40

【0015】

図1Aの説明

ここで図1Aを参照すると、図1Aは、上記したシステム1の、図1のより詳細な図を示している。図1Aに示すように、例えば、電子デバイス100は、プロセッサ102、通信構成要素106及び/又は近距離無線通信(「NFC」)構成要素120を含むことができる。NFC構成要素120は、耐タンパ性プラットフォームを(例えば、単一チップ又は複数チップセキュアマイクロコントローラとして)提供するように構成され得るセキュアエレメント145を含むか、又は他の方法で提供することができ、このプラットフォームは、認証され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

50

Global Platformのような業界標準の権限者)によって定められ得る規則及びセキュリティ要件に従って、アプリケーションならびにそれらの機密データ及び暗号化データ(例えば、クレデンシャルアプレット及び、図1Aに示すような、クレデンシャル鍵155a'及びアクセス鍵155a、ならびに/又は発行者のセキュリティドメイン(1SD)鍵156kなどの関連付けられたクレデンシャル鍵)をセキュアにホスティングし得る。以下により詳細に説明するように、デバイス100の(例えば、NFC構成要素120の)セキュアエレメント145上のクレデンシャルアプレット又は決済アプリケーションは、資金供給口座又は他の金融商品若しくは信用元(例えば、金融機関サブシステム350における)を識別するための十分な詳細を含むトランザクションデータとして決済クレデンシャルデータを提供するように構成することができ、このような決済クレデンシャルデータは、財務トランザクションを促進するために、販売事業者サブシステム200及び/又は商業エンティティサブシステム400との1つ以上の通信の中でデバイス100によって使用され得る。NFC構成要素120は、このようなホスト決済クレデンシャルデータを、販売事業者サブシステム200との非接触近接型通信5(例えば、近距離無線通信)として(例えば、デバイス100のユーザがデバイス100に記憶されたクレデンシャルを使用して、近接して配置された販売事業者端末220と非接触近接型通信を介して財務トランザクションを行い得る、実在の店舗又は任意の物理的所在地に配置され得る販売事業者サブシステム200の販売事業者端末220との通信)、通信するように構成され得る。代替的に、又は追加的に、任意の好適な有線又は無線プロトコル(例えば、通信経路15、65及び/又は75のうちの1つ以上を介して)を用いて、任意の好適な決済クレデンシャルデータを(例えば、オンライン型通信684として)1つ以上の他の電子デバイス又はサーバ若しくはサブシステム(例えば、任意の好適なオンライン通信を介する販売事業者サブシステム200の販売事業者サーバ210のような、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)と通信することを可能とするように、通信構成要素106がデバイス100に設けられてもよい。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性能を制御するように機能し得る任意の処理回路を含むことができる。例えば、プロセッサ102は、販売事業者サブシステム200との財務トランザクションに資金供給するためにデバイス100によりデータ(例えば、トランザクションデータの決済クレデンシャルデータ)が通信され得る方法を、少なくとも部分的に決定し得る、1つ以上のアプリケーション(例えば、アプリケーション103及び/又はオンラインリソース若しくは販売事業者アプリケーション113)をデバイス100上で実行するように構成され得る。また、図1Aに示すように、デバイス100は、プロセッサ102又はデバイス100の任意の他の好適な部分にとってアクセス可能となり得る任意の好適なデバイス識別情報又はデバイス識別子119を含むことができる。デバイス識別情報119は、デバイス100を一意に識別し、販売事業者サブシステム200とのトランザクションを促進し、かつ/又はデバイス100との好適なセキュアな通信を可能とするため、商業エンティティサブシステム400及び/又は販売事業者サブシステム200及び/又は金融機関サブシステム350によって利用され得る。一例として、デバイス識別情報119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に関連付けられ得る任意の一意の識別子とすることができる。

【0016】

販売事業者サブシステム200は、図1Aに示すような、任意の好適な販売事業者サーバ210を含むことができ、それは、任意の好適な通信プロトコル(例えば、Wi-Fi、Bluetooth(登録商標)、セルラ、有線ネットワークプロトコル等)を介して、(例えば、通信経路85を介して)商業エンティティサブシステム400の通信構成要素と、及び/又は、(例えば、通信経路25を介して)取得銀行300の通信構成要素と、及び/又は(例えば、通信経路15を介して)デバイス100の通信構成要素と、あらゆる好適なデータを通信するように構成され得る任意の好適な構成要素又はサブシステムを含むことができる。例えば、販売事業者サーバ210は、デバイス100の通信構成要素106と、潜在的トランザクションデータ660を、次のような任意の好適なオンライ

10

20

30

40

50

ンコンテキスト内で通信するように機能することができ、これには、デバイス100のユーザが、デバイス100上で実行中であり得る任意の好適な販売事業者オンラインリソース113を介するトランザクションを行うために販売事業者サーバ210と通信している場合の、次のオンラインリソースが含まれる。

販売事業者サーバ210によって管理され得るデバイス100上で動作中のサードパーティ販売事業者アプリケーション113（例えば、ネイティブアプリケーション）、又はデバイス100上で動作中であって、ターゲット又はウェブリソースが販売事業者サーバ210（例えば販売事業者のウェブサイト）によって管理され得るユニフォームリソースロケータ（「URL」）に向けられ得るインターネットアプリケーション113（例えば、アップル インコーポレイテッドによるSafari（登録商標））

10

販売事業者ウェブサイトに向けられたウェブ表示を用いた販売事業者アプリケーション（例えば、販売事業者アプリケーション内にバンドルされたインターネットブラウザであって、それによってハイブリッドアプリと呼ばれ得るものを生成することでウェブ技術（例えば、HTML、JavaScript（登録商標）、CSS等）を用いて構築できるアプリをネイティブアプリとしてパッケージング可能なもの、及び／又は

販売事業者のウェブサイトに向けられたウェブ表示を用いた非販売事業者アプリケーション。

したがって、販売事業者サーバ210とデバイス100との間の通信は、無線で、及び／又は有線経路を介して（例えば、インターネット上で）生じ得ることに留意されたい。販売事業者サーバ210は、販売事業者サブシステム200の販売事業者によって（例えば、ウェブサイトデータをホストする、かつ／又はサードパーティアプリケーションデータを管理するウェブサーバとして）提供されてもよい。追加的に、又は代替的に、図1Aに示すように、販売事業者サブシステム200は、任意の販売事業者端末220（例えば、販売事業者決済端末）を含むことができ、それは、デバイス100の非接触近接型通信構成要素（例えば、デバイス100のNFC構成要素120との非接触近接型通信5）と任意の好適なデータを通信するように構成され得る好適な構成要素又はサブシステムを含むことができる。また、図1Aに示すように、販売事業者サブシステム200は、販売事業者鍵157及び／又は販売事業者識別子（「ID」）167を含むことができる。図示していないが、販売事業者サブシステム200はまた、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と同一又は同様であり得る販売事業者プロセッサ構成要素、（例えば、サーバ210の一部として）図1A及び図2の電子デバイス100の通信構成要素106と同一又は同様であり得る販売事業者通信構成要素、図2の電子デバイス100のI/Oインタフェース114と同一又は同様であり得る販売事業者I/Oインタフェース、図2の電子デバイス100のバス118と同一又は同様であり得る販売事業者バス、図2の電子デバイス100のメモリ構成要素104と同一又は同様であり得る販売事業者メモリ構成要素、及び／又は図2の電子デバイス100の電源構成要素108と同一又は同様であり得る販売事業者電源構成要素、も含むことができる。

20

30

【0017】

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360（例えば、決済カード組合又はクレジットカード組合）及び／又は発行銀行サブシステム370を含むことができる。例えば、発行銀行サブシステム370は、特定のクレデンシャルにより負担し得る債務を完済する消費者の能力に対する主たる責任を引き受け得る金融機関とすることができる。デバイス100のNFC構成要素120の特定のクレデンシャルアプレットをそれぞれ、特定のユーザのアカウント（単数又は複数）に電子的にリンクされ得る特定の決済カードに関連付けることができる。クレジットカード、デビットカード、チャージカード、ストアドバリューカード、フリートカード（fleet card）、ギフトカード等を含む様々なタイプの決済カードが好適であり得る。特定の決済カードの商業クレデンシャルは、（例えば、直接的又は商業エンティティサブシステム400を介した）販売事業者サブシステム200との商業クレデンシャルデータ通信（例えば、非接触近接型通信及び／又はオンライン型通信）に使用するために発行銀行サブシステム370によってデバイス

40

50

100上に（例えば、後述のNFC構成要素120のクレデンシャル補足的セキュリティドメインのクレデンシャルとして）供給され得る。各クレデンシャルは、決済ネットワークサブシステム360によってブランド付けされ得る特定の決済カードのブランドであってよい。決済ネットワークサブシステム360は、種々の発行銀行370及び／又は、特定のブランドの決済カードの使用（例えば、商業クレデンシャル）を処理することができる種々の取得銀行300のネットワークであってもよい。

【0018】

財務トランザクションがシステム1内で生じるために、少なくとも1つの商業クレデンシャルが電子デバイス100のセキュアエレメント上にセキュアに供給されなければならない。例えば、このような商業クレデンシャルを、（例えば、金融機関サブシステム350とデバイス100との間の通信経路75を介するクレデンシャルデータ654として、そして通信構成要素106を介してセキュアエレメント145に渡されることにより）金融機関サブシステム350から直接デバイス100のセキュアエレメント145に少なくとも部分的に直接供給することができる。追加的に、又は代替的に、このような商業クレデンシャルを、金融機関サブシステム350からデバイス100のセキュアエレメント145に、商業エンティティサブシステム400を介して、少なくとも部分的に直接供給することができる（例えば、このような商業クレデンシャルを金融機関サブシステム350と商業エンティティサブシステム400との間の通信経路55を介するクレデンシャルデータ654として供給し、それを商業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との間の通信経路65を介してクレデンシャルデータ654としてデバイス100に渡し、そして、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）。経路75を介した、かつ／又は経路55／65を介したクレデンシャルデータ654は、セキュアエレメントのクレデンシャル補足的セキュリティドメインの少なくとも一部分又は全部として、デバイス100のセキュアエレメント145に供給することができ、またそれは、決済アプリケーション又はクレデンシャル情報161a及びクレデンシャル鍵155a'を有するクレデンシャルアプレット153aなどの、クレデンシャル情報及び／又はクレデンシャル鍵を有するクレデンシャルアプレットを含むことができる。図1Aに示すように、例えば、金融機関サブシステム350はまた、（例えば、クレデンシャル鍵155a'を用いてデバイス100により暗号化されたデータを解読するために）クレデンシャル鍵155a'へアクセスすることもできる。金融機関サブシステム350は、クレデンシャル鍵155a'の管理を担当することができる、管理は、そのような鍵の生成、交換、記憶、使用、及び置換を含んでもよい。金融機関サブシステム350は、金融機関サブシステム350のセキュアエレメントにクレデンシャル鍵155a'のバージョンを記憶することができる。デバイス100のクレデンシャル鍵155a'及び金融機関サブシステム350のクレデンシャル鍵155a'は、電子デバイス100のセキュアエレメント及び金融機関サブシステム350の両方が利用可能な任意の好適な共有秘密（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）等）とすることができ、（例えば、財務トランザクションの決済データを妥当性検査するため）電子デバイス100と金融機関サブシステム350が独立して任意の好適な暗号データ（例えば、暗号文）又は任意の他の好適なデータを生成することを可能とする機能を持つ。これは、関数の出力が少なくとも部分的に共有秘密によって決定され得る任意の好適な暗号アルゴリズム又は暗号を用い、共有秘密は金融機関サブシステム350によってデバイス100に供給され得ることによって理解されたい。共有秘密は、事前に（例えば、金融機関サブシステム350によるデバイス100へのクレデンシャルの提供の際に）金融機関サブシステム350とデバイス100との間で共有されてもよく（この場合には、このような共有秘密は事前共有鍵と呼ばれる場合がある）、又は、共有秘密は、特定の財務トランザクションに使用する前に、鍵合意プロトコルを用いて（例えば、ディフィー・ヘルマンのような公開鍵暗号法を用いて、又はケルベロスのような対称鍵暗号法を用いて）作成されてもよい。共有秘密及び、関数の出力が共有秘密によって少なくとも部分的に決定

10

20

30

40

50

され得る好適な暗号アルゴリズム又は暗号は、デバイス100のセキュアエレメントによってアクセス可能とすることができる。

【0019】

商業エンティティサブシステム400は、金融機関サブシステム350とデバイス100との間の媒介として提供されてもよく、その場合、商業エンティティサブシステム400は、クレデンシャルがデバイス100のセキュアエレメントに供給される際、及び／又はそのような供給されたクレデンシャルがデバイス100と販売事業者サブシステム200との間の商業クレデンシャルデータ通信の一部として使用される際に、新たなセキュリティ層を提供、かつ／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構成されてもよい。商業エンティティサブシステム400は、特定の商業エンティティによって提供されてもよく、デバイス100のユーザに、ユーザ固有アカウントのユーザ固有のログイン情報を通じて（例えば、ユーザ固有識別及びパスワードの組合せを通じて）種々のサービスを提供し得る。一例として、商業エンティティサブシステム400は、アップル インコーポレイテッド（カリフォルニア州クパチーノ）によって提供されてもよい。同社はまた、デバイス100のユーザへの様々なサービスの提供者（例えば、デバイス100で再生されるメディアを販売／レンタルするiTunes（登録商標）ストア、デバイス100上で使用されるアプリケーションを販売／レンタルするアップルのApp Store（登録商標）、デバイス100からデータを記憶する、かつ／又は複数のユーザデバイス及び／又は複数のユーザプロフィールを互に関連付けるアップルの iCloud（登録商標）サービス、様々なアップル製品をオンラインで購入するためのアップルのオンラインストア、デバイス間でメディアメッセージを通信するためのアップルのiMessage（登録商標）サービス等）であってもよく、また、（例えば、デバイス100がiPod（登録商標）、iPad（登録商標）、iPhone（登録商標）等である場合）デバイス100自身及び／又はデバイス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）の提供者、製造業者及び／又は開発者であってもよい。商業エンティティサブシステム400を提供し得る商業エンティティ（例えば、アップル インコーポレイテッド）は、金融機関サブシステム350のいずれの金融エンティティとも別個で独立したものであってもよい。例えば、商業エンティティサブシステム400を提供し得る商業エンティティは、エンドユーザデバイス100上で提供されるクレジットカード又は他の商業クレデンシャルを供給及び／又は管理し得る、いずれの決済ネットワークサブシステム360又は発行銀行サブシステム370とも別個かつ／又はそれから独立したものであってもよい。追加的に、又は代替的に、商業エンティティサブシステム400を提供し得る商業エンティティ（例えば、アップル インコーポレイテッド）は、販売事業者サブシステム200のいずれの販売事業者とも別個で独立したものであってもよい。例えば、商業エンティティサブシステム400を提供し得る商業エンティティは、非接触近接型通信用の販売事業者端末、オンライン通信用のサードパーティアプリケーション又はオンラインリソース113、及び／又は販売事業者サブシステム200の任意の他の態様を提供し得る販売事業者サブシステム200のいずれの販売事業者とも別個かつ／又はそれから独立したものであってもよい。このような商業エンティティは、自身がデバイス100上で金融機関サブシステム350によって提供されたクレデンシャルを供給したいと望む場合、及び／又は、このような供給されたクレデンシャルが財務トラザクションに資金供給する販売事業者サブシステム200との商業クレデンシャルデータ通信の一部として使用されている場合、デバイス100のユーザに対して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、デバイス100の種々の構成要素（例えば、商業エンティティが少なくとも部分的にデバイス100を製造又は管理することができる場合、例えば、デバイス100のソフトウェア構成要素及び／又はハードウェア構成要素）を構成又は制御する潜在的能力を活用することができる。例えば、いくつかの実施形態では、デバイス100は、（例えば、デバイス100と販売事業者サブシステム200との間のオンライン型セキュアデータ通信の間）より高いレベルのセキュリティを可能にし得る特定のデータの共有及び／又は受信を、デバイス100のユーザにはシームレス

10

20

30

40

50

で透過的に、商業エンティティサブシステム400と（例えば、通信経路65を介して）通信するように構成されてもよい。図示していないが、商業エンティティサブシステム400はまた、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と同一又は同様であり得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と同一又は同様であり得る通信構成要素、図2の電子デバイス100のI/Oインタフェース114と同一又は同様であり得るI/Oインタフェース、図2の電子デバイス100のバス118と同一又は同様であり得るバス、図2の電子デバイス100のメモリ構成要素104と同一又は同様であり得るメモリ構成要素、及び／又は、図2の電子デバイス100の電源構成要素108と同一又は同様であり得る電源構成要素も含むことができ、そのうち1つ、一部又は全部が少なくとも部分的にサーバ410によって提供されてもよい。

10

【0020】

少なくとも1つの商業クレデンシャルが（例えば、クレデンシャル鍵155a'及びクレデンシャル情報161aを有するクレデンシャルSSDの一部分として）デバイス100のセキュアエレメント上に供給されることに加えて、デバイス100が販売事業者サブシステム200と財務トランザクションをよりセキュアに行うことができるように、アクセス鍵155bを有する少なくとも1つのアクセスSSDがデバイス100のセキュアエレメント上に供給されてもよい。例えば、アクセスSSDを少なくとも部分的に、商業エンティティサブシステム400から直接デバイス100のセキュアエレメントに供給することができる（例えば、商業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との間の通信経路65を介してアクセスデータ652として供給でき、そして、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）。経路652を介したアクセスデータ65は、アクセスSSDの少なくとも一部又は全部としてデバイス100のセキュアエレメント上に供給されることができ、アクセス鍵155bを有するアクセスアプレット153bを含むことができる。図1Aに示すように、商業エンティティサブシステム400はまた、（例えば、アクセス鍵155bを用いてデバイス100によって暗号化されたデータを解読するために）アクセス鍵155bにアクセスすることもできる。商業エンティティサブシステム400は、アクセス鍵155b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。商業エンティティサブシステム400は、アクセス鍵155bのそのバージョンを商業エンティティサブシステム400のセキュアエレメント内に記憶することができる。アクセス鍵155bを有するデバイス100のアクセスSSDは、（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のユーザの意図及びローカル認証を判定するように構成されてもよく、また、このような判定に応じて、（例えば、デバイス100のクレデンシャルSSDのクレデンシャルを用いて）決済トランザクションを行うための別の特定のSSDを可能とするように構成されてもよい。このようなアクセスSSDをデバイス100のセキュアエレメント内に記憶することにより、財務トランザクションに対するユーザの意図及び財務トランザクションの認証を確実に判定する能力を向上させることができる。また、デバイス100のこのようなアクセスSSDのアクセス鍵155bは、デバイス100のセキュアエレメントの外部に通信され得るトランザクションデータの暗号化を高めるために活用されてもよい。追加的に又は代替的に、以下に説明するように、アクセスデータ652は、電子デバイス100のセキュアエレメントの発行者セキュリティドメイン（「ISD」）に対するISD鍵156kを含むことができ、そのISD鍵はまた商業エンティティサブシステム400によって維持されてもよく、以下に説明するようにアクセス鍵155bに加えて、又はその代わりに使用されてもよい。

20

30

40

【0021】

販売事業者アプリケーション又はオンラインリソース113は、デバイス100と販売事業者サブシステム200との間でオンライン財務トランザクションを促進することを可能とするために、又は販売事業者サブシステム200によるデバイス100の任意の他の

50

好適なセキュアデバイス機能性へのオンラインアクセスを可能とするために、デバイス100によりアクセスすることができる。最初に、このようなアプリケーション113は、アプリケーション113がデバイス100によって有効に利用される前に、商業エンティティサブシステム400によって承認若しくは登録されてもよいし、又は別の方法で可能にされてもよい。例えば、商業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、通信経路85を介して販売事業者サブシステム200からアプリケーション113を表す少なくとも一部のデータを受信することができる。また、いくつかの実施形態では、商業エンティティサブシステム400は、アプリケーション113のための販売事業者鍵157を生成するか、他の方法で割り当てることができる。また、このような販売事業者鍵157を販売事業者サブシステム200に（例えば、経路85を介して）提供することができる。代替的に、販売事業者サブシステム200は、アプリケーション113のために販売事業者鍵157を生成するか、又は他の方法により割り当てることができる。またこのような販売事業者鍵157を、商業エンティティサブシステム400に（例えば、経路85を介して）提供することができる。販売事業者サブシステム200又は商業エンティティサブシステム400のいずれも、販売事業者鍵157の管理を担当することができる。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。このような販売事業者鍵157がどのように、又はどこで生成及び／又は管理され得るかにかかわらず、販売事業者サブシステム200及び商業エンティティサブシステム400はともに、販売事業者鍵157のバージョンを記憶することができる（例えば、販売事業者サブシステム200及び商業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、その場合、いくつかの実施形態では、（例えば、非対称鍵暗号化／解読プロセスに使用するために）販売事業者サブシステム200によって記憶された販売事業者鍵157は秘密鍵とすることができ、商業エンティティサブシステム400によって記憶された販売事業者鍵157は対応する公開鍵とすることができる）。いくつかの実施形態では、このような販売事業者鍵157を販売事業者アプリケーション113に特に関連付けることができ、他の実施形態では、販売事業者鍵157を販売事業者サブシステム200の販売事業者に特に関連付けることで、販売事業者鍵157は、販売事業者サブシステム200の同じ販売事業者が稼働させる複数のサードパーティアプリケーション又はウェブリソースに関連付けることができる。一意の販売事業者識別子167が、商業エンティティサブシステム400によって、かつ／又は販売事業者サブシステム200によって、生成され、かつ／又は、他の方法でアプリケーション113に割り当てられ、若しくはアプリケーションに関連付けられてもよい。例えば、販売事業者識別子167は、英数字列、ドメイン（例えば、URL、又は、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のための）、又は、販売事業者及び／又は特定の販売事業者オンラインリソースを一意に識別する（例えば、それらを商業エンティティサブシステム400に対して一意に識別する）ことができる他の好適な識別子とすることができる。販売事業者アプリケーション113又は販売事業者エンティティの特定の販売事業者識別子167と販売事業者鍵157を関連付けるために、表430又は商業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得る他の好適なデータ構造若しくは情報源が提供され得る。販売事業者オンラインリソースを、特定の販売事業者識別子167及び特定の販売事業者鍵157と関連付けることができ、それらのそれぞれを、販売事業者サブシステム200と商業エンティティサブシステム400との間でセキュアに共有することができる。表430は、デバイス100が鍵157及び販売事業者識別子167と関連付けられた販売事業者アプリケーション113を介して販売事業者サブシステム200とインタフェースすることを伴い得るトランザクションのために、セキュリティ層を販売事業者サブシステム200に通信される任意のセキュアデバイスデータ（例えば、デバイス100にとってネイティブな決済クレデンシャルデータを含み得る商業クレデンシャルデータ）に提供するために、商業エンティティサブシステム400が適切な販売事業者鍵157を決定及び利用することを可能とすることができる。デバイス100は、アプリケーション113に（例えば、アプリケーションス

10

20

30

40

50

トア420から通信経路65を介して)アクセスし、アプリケーション113を(例えば、プロセッサ102を用いて)実行するように構成することができる。代替的に、又は追加的に、販売事業者鍵157及び販売事業者の識別子167は、販売事業者のサードパーティネイティブアプリではなく、又はそれに加えて、販売事業者のウェブサイト(例えば、いくつかの実施形態において本明細書において販売事業者オンラインリソース又は販売事業者アプリケーションと呼ぶ場合がある、1つ以上のURL又はドメイン)又は販売事業者と一般に関連付けられてもよい。例えば、販売事業者サブシステム200の販売事業者は商業エンティティサブシステム400と協働し、特定の販売事業者ウェブサイト又は販売事業者を一般に表430内の特定の販売事業者鍵157及び販売事業者識別子167と関連付けることができ、それにより、ターゲット又はウェブリソースが販売事業者鍵157及び販売事業者識別子167に関連付けられ得るURL又はドメイン(例えば、そのウェブリソースの一意のドメイン(例えば、store.merchant.com))に向けられ得る、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てトランザクションを行うように、デバイス100が販売事業者サーバ210とインタフェースすることを伴い得るトランザクションのため、セキュリティ層を、販売事業者サブシステム200(例えば、デバイス100にネイティブな決済クレデンシャルデータを含み得る商業クレデンシャルデータ)に通信された任意のセキュアデバイスデータに提供するために、商業エンティティサブシステム400が適切な販売事業者鍵157を決定及び利用することを可能とすることができる。デバイス100は、例えば、販売事業者サーバ210から通信経路15を介して、このようなURLに(例えば、このような販売事業者ウェブリソースをターゲットにする際に販売事業者オンラインリソースとみなすことができるデバイス100上のインターネットアプリケーション113を用いて)アクセスするように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、特定の販売事業者、販売事業者サブシステム200、販売事業者鍵157及び/又は販売事業者識別子167と関連付けられず、代わりに、そのような販売事業者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が利用可能であり、それにより販売事業者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。商業エンティティサブシステム400による販売事業者オンラインリソースのこのような登録(例えば、(例えば、表430に記憶するための)販売事業者サブシステム200と商業エンティティサブシステム400との間での販売事業者鍵157及び販売事業者識別子167の、セキュアかつ妥当性検査された共有)を、販売事業者サブシステム200がオンラインリソースの正当な所有者であることを商業エンティティサブシステム400に対し確実とする任意の好適な方法で実行することができる。上述のように、販売事業者オンラインリソース(例えば、ネイティブアプリ、ドメイン/URL、又は任意の他の好適なウェブリソース、又はおそらく販売事業者端末でも)を、(例えば、図5のステップ501及び/又は図6のステップ606での登録の間)特定の販売事業者識別子167及び特定の販売事業者鍵157と関連付けることができ、それらのそれぞれを、任意の好適な方法で販売事業者サブシステム200と商業エンティティサブシステム400との間でセキュアに共有することができ、そのような関連付けを、(例えば、表430で)商業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。

【0022】

図2の説明

ここで図2を参照すると、図2は図1及び図1Aに関して上記したシステム1の電子デバイス100のより詳細な図を示している。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、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はまた、デバイス100の他の種々の構成要素に、それらから、又はそれらの間で、データ及び/又は電力を転送するための1つ以上の有線若しくは無線通信リンク又は経路を提供し得るバス118を含むことができる。電子デバイス100は、デバイス100の外部のゴミ又は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1つ以上を少なくとも部分的に囲み得る筐体101を備えることもできる。いくつかの実施形態では、電子デバイス100の1つ以上の構成要素を組合せてもよいし、又は省略してもよい。また、電子デバイス100は、図2に組み合わされていない、又は含まれ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、図2に示す構成要素の任意の他の好適な構成要素又はいくつかの実例を含むことができる。簡潔にするために、図2では、それぞれの構成要素のうち1つだけを示している。1つ以上の入力構成要素110を、ユーザに、デバイス100と相互作用(interact)又はインタフェースさせるように設けてもよいし、及び／又は、1つ以上の出力構成要素112を、デバイス100のユーザに情報(例えば、グラフィカル、可聴、及び／又は触覚情報)を提示するように設けてもよい。ここで、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、本明細書では、入出力(「I/O」)構成要素又はI/Oインタフェース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インタフェース114と総称する)場合があることを留意されたい。例えば、入力構成要素110及び出力構成要素112は、表示画面へのユーザのタッチにより入力情報を受信でき、また同一の表示画面を介してユーザに視覚情報を提供し得るタッチスクリーンなど、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性能を制御するように機能し得る任意の処理回路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、かつ／又は出力構成要素112を通し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であってもよく、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であってもよいし、他の好適なオンラインリソース(例えば、販売事業者サブシステム200の販売事業者に関連付けられたアプリケーション)であってもよい。また、図示するように、プロセッサ102は、デバイス100を識別するためにデバイス100のユーザ及び／又は商業エンティティサブシステム400によって利用され得るデバイス識別情報119にアクセスすることができる。

【0023】

NFC構成要素120は、電子デバイス100と販売事業者サブシステム200の販売事業者端末(例えば、販売事業者決済端末220)との間の非接触近接型トランザクション又は通信を可能にし得る任意の好適な近接型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とそのような販売事業者端末との間の非接触近接型通信を可能とする任意の好適な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、NFCブースタ136を含むことができる。NFCデータモジュール132は、非接触近接型通信又はNFC通信の一部としてNFC構成要素120により販売事業者端末に送信され得る好適なデータを収容し、経路設定し、又はその他機能により提供するように構成されてもよい。追加的に、又は代替的に、NFCデータモジュール132は、非接触近接型通信の一部として販売事業者端末からNFC構成要素120により受信され得る好適なデータを収容し、経路設定し、又はその他機能により受信するように構成されてもよい。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、NFCデバイスモジュール130とともに動作し、電子デバイス100と販売事業者端末との間でNFC通信を通信するためにNFC構成要素120を可能とする、アクティブにする、許可する、及び／又は、その他機能により制御することができる。NFCコントローラモジュール140は、NFC構成要素120の働きを決定づけるのを助けるNFC低電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のに使

10

20

30

40

50

用され得る、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、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とともに動作し、電子デバイス100と販売事業者サブシステム200との間のNFC通信を可能とすることができる。NFCメモリモジュール150は、耐タンパ性であってもよく、セキュアエレメント145の少なくとも一部分（例えば、図2A参照）を提供してもよい。例えば、このようなセキュアエレメントは、耐タンパ性プラットフォームを提供するように構成されてよく（例えば、単一チップ又は複数チップセキュアマイクロコントローラとして）、認証され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のような業界標準の権限者）によって定められ得る規則及びセキュリティ要件に従って、アプリケーションならびにそれらの機密データ及び暗号データ（例えば、アプレット153及び鍵155）をセキュアにホスティングし得る。

10

【0024】

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）によって定義及び管理され得る、発行者セキュリティドメイン（「ISD」）152及び補足的セキュリティドメイン（「SSD」）154（例えば、サービスプロバイダセキュリティドメイン（「SPSD」）、信頼されたサービスマネージャセキュリティドメイン（「TSMSSD」）等）のうちの1つ以上を含むことができる。例えば、ISD152は、信頼されたサービスマネージャ（「TSM」）又は発行金融機関（例えば金融機関サブシステム350）が、クレデンシャル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つ以上のクレデンシャル（例えば、各種クレジットカード、銀行カード、ギフトカード、アクセスカード、交通パスなどに関連付けられたクレデンシャル）を形成し、又は他の方法で供給するための鍵及び／又は他の好適な情報を記憶することができる、NFCメモリモジュール150の一部分であり得る。クレデンシャルは、ユーザ／消費者に割り当てられ、かつ電子デバイス100上にセキュアに記憶され得る、クレジットカード決済番号（例えば、デバイス主アカウント番号（「DPAN」）、DPAN有効期限、CVV等（例えば、トークン又はその他として））などの、クレデンシャルデータ（例えば、クレデンシャル情報161a）を含むことができる。NFCメモリモジュール150は、少なくとも2つのSSD154（例えば、少なくとも第1のSSD154a及び第2のSSD154b）を含むことができる。例えば、第1のSSD154a（例えば、クレデンシャルSSD154a）を、特定の特典又は決済権を電子デバイス100に提供し得る特定のクレデンシャル（例えば、金融機関サブシステム350により供給された特定のクレジットカードクレデンシャル又は特定の公衆交通カードクレデンシャル）と関連付けることができる。一方、第2のSSD154b（例えば、アクセスSSD154b）を、別のSSD（例えば、第1のSSD154a）の特定のクレデンシャルに対するデバイス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に提供し得る商業エンティティ（例えば、デバイス100用の制御エンティティとすることができる商業エンティティサブシステム400の商業エンティティ）と関連付けることができる。代替的に、第1のSSD154a及び第2のSSD154bのうちのそれぞれを、電子デバイス100に特定の特典又は決済権を提供し得る各特定のクレデンシャル（例えば、金融機関サブシステム350によって供給された特定のクレジットカードクレデンシャル又は特定の公衆交通カードクレデンシャル）と関連付けることができる。各SSD154は、少なくとも1つのアプレット153を含むことができ、かつ／又はそのアプレットと（例えば、SSD154aはアプレット153aと、SSD154bはアプレット153bと）関連付けられてもよい。例えば、SSD154のアプレット153を、（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され得るアプリケーションとすることができる。クレデンシャルアプレット153は、クレデンシャル情報161を含むことができ、又はクレデンシャル情報161（例えば、アプレット153aの情報161a及び／又はアプレット15

20

30

40

50

3 b の情報 1 6 1 b) と関連付けられることができる。各 S S D 1 5 4 及び／又はアプレット 1 5 3 は、自身の鍵 1 5 5 のうち少なくとも 1 つを含むこともでき、かつ／又はそれ自身の鍵のうち少なくとも 1 つと（例えば、アプレット 1 5 3 a は少なくとも 1 つの鍵 1 5 5 a と、アプレット 1 5 3 b は少なくとも 1 つの鍵 1 5 5 b と）に関連付けられてもよい。

【0025】

S S D 1 5 4 の鍵 1 5 5 は、暗号アルゴリズム又は暗号の関数出力を決定し得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特定の変換を指定することができる、又は解読中はその逆とすることができる。鍵はまた、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で使用されてもよい。S S D の鍵は、好適な共有秘密を別のエンティティに提供することができる。鍵及びアプレットのそれぞれを、T S M 又は許可されたエージェントによってデバイス 1 0 0 のセキュアエレメント上にロードしてもよいし、デバイス 1 0 0 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、クレデンシャル S S D 1 5 4 a を特定のクレジットカードクレデンシャルと関連付けることができる一方、その特定のクレデンシャルは、デバイス 1 0 0 のセキュアエレメントから（例えば、N F C 構成要素 1 2 0 から）販売事業者サブシステム 2 0 0 に対する商業クレデンシャルデータ通信として、クレデンシャル S S D 1 5 4 a のアプレット 1 5 3 a がかかる使用に対して可能にされている、又は他の方法でアクティブにされている、又はロック解除されている場合に行う財務トランザクションのためにのみ、通信可能である。

【0026】

N F C 構成要素 1 2 0 の使用を可能とするため、クレデンシャルのクレジットカード情報又は銀行アカウント情報などの機密決済情報を、電子デバイス 1 0 0 から販売事業者サブシステム 2 0 0 に送信する際に特に有用であり得るセキュリティ特徴を提供してもよい。このようなセキュリティ特徴はまた、アクセスが制限され得るセキュア記憶領域を含むことができる。セキュア記憶領域にアクセスするために、例えば、個人識別番号（「P I N」）の入力を介した、又はバイオメトリックセンサとのユーザ相互作用を介したユーザ認証を提供することが必要とされ得る。例として、アクセス S S D 1 5 4 b は、他の S S D 1 5 4 （例えば、クレデンシャル S S D 1 5 4 a ）をそのクレデンシャル情報 1 6 1 a を通信するために使用することを可能とする前に、このような認証が生じているかどうかを判定するためにアプレット 1 5 3 b を活用することができる。特定の実施形態では、セキュリティ特徴の一部又は全部が N F C メモリモジュール 1 5 0 内に記憶されてもよい。更に、商業クレデンシャルデータを販売事業者サブシステム 2 0 0 と通信するための認証鍵のようなセキュリティ情報を、N F C メモリモジュール 1 5 0 内に記憶してもよい。特定の実施形態では、N F C メモリモジュール 1 5 0 は、電子デバイス 1 0 0 内に埋め込まれたマイクロコントローラを含むことができる。一例としては、アクセス S S D 1 5 4 b のアプレット 1 5 3 b は、（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 1 1 0 を介して）のデバイス 1 0 0 のユーザの意図及びローカル認証を判定するように構成することができ、そのような判定に応じて、（例えば、クレデンシャル S S D 1 5 4 a のクレデンシャルを用いて）決済トランザクションを行うために別の特定の S S D を可能とするように構成することができる。

【0027】

図 2 A の説明

ここで図 2 A を参照すると、図 2 A は、図 1 ～図 2 に関して上記したシステム 1 の電子デバイス 1 0 0 の一部分の別の詳細図を示している。図 2 A に示すように、例えば、デバイス 1 0 0 のセキュアエレメント 1 4 5 は、アプレット 1 5 3 a 、クレデンシャル 1 6 1 a 、アクセス鍵 1 5 5 a 、及び／若しくはクレデンシャル鍵 1 5 5 a ' を含み得る、又は、アプレット 1 5 3 a 、クレデンシャル 1 6 1 a 、アクセス鍵 1 5 5 a 、及び／若しくはクレデンシャル鍵 1 5 5 a ' に関係付けられ得る S S D 1 5 4 a と、アプレット 1 5 3 b 、クレデンシャル 1 6 1 b 、アクセス鍵 1 5 5 b 、及び／若しくはクレデンシャル鍵 1 5

5 b' を含む得る、又は、アプレット 153 b、クレデンシャル 161 b、アクセス鍵 155 b、及び／若しくはクレデンシャル鍵 155 b' に関係付けられ得る SSD 154 b とを含むことができる。いくつかの実施形態において、特定の補足的セキュリティドメイン（「SSD」）154（例えば、SSD 154 a 及び 154 b のうちの 1 つ）を、特定の TSM 及び、電子デバイス 100 に特定の特典又は決済権を提供し得る少なくとも 1 つの特定の商業クレデンシャル（例えば、特定のクレジットカードクレデンシャル又は特定の公衆交通カードクレデンシャル）と関連付けることができる。各 SSD 154 は、NFC デバイスモジュール 130 によって使用される SSD 154 の機能を可能とするために、アクティブ化を必要とすることがある自身のマネージャ鍵 155（例えば、鍵 155 a k 及び 155 b k のそれぞれ 1 つ）を有することができる。追加的に又は代替的に、各 SSD 154 は、特定の商業クレデンシャルと関連付けられ得る、それ自身のクレデンシャルアプリケーション又はクレデンシャルアプレット（例えば、Java（登録商標）カードアプレットインスタンス）（例えば、SSD 154 a のクレデンシャルアプレット 153 a を第 1 の商業クレデンシャルと関連付けることができ、かつ／又は、SSD 154 b のクレデンシャルアプレット 153 b を第 2 の商業クレデンシャルと関連付けることができる）のうち少なくとも 1 つを含むことができ、かつ／又はそれと関連付けられることができ、クレデンシャルアプレットは自身のアクセス鍵（例えば、クレデンシャルアプレット 153 a 用のアクセス鍵 155 a 及び／又はクレデンシャルアプレット 153 b 用のアクセス鍵 155 b）、及び／又は、自身のクレデンシャル鍵（例えば、クレデンシャルアプレット 153 a 用のクレデンシャル鍵 155 a' 及び／又はクレデンシャルアプレット 153 b 用のクレデンシャル鍵 155 b'）を有することができ、クレデンシャルアプレットは、（例えば、販売事業者端末 220 による）NFC 通信として、かつ／又は（例えば、商業エンティティサブシステム 400 を介した）電子デバイス 100 と販売事業者サブシステム 200 との間のオンライン型通信として、NFC デバイスモジュール 130 によって使用される、その関連付けられた商業クレデンシャルを可能とするためにアクティブ化を必要とすることがある。いくつかの実施形態では、クレデンシャルアプレットのクレデンシャル鍵（例えば、クレデンシャルアプレット 153 a 用のクレデンシャル鍵 155 a' 及び／又はクレデンシャルアプレット 153 b 用のクレデンシャル鍵 155 b'）は、（例えば、販売事業者サブシステム 200 を介した）セキュアエレメント 145 と金融機関サブシステム 350 との間の当該アプレットの当該クレデンシャル情報のセキュアな送信を可能とするため、そのようなクレデンシャルを担当することができ、かつ（例えば、図 1 A に示すように）金融機関サブシステム 350 によってアクセス可能とすることができる金融機関サブシステム 350 によって生成されてもよい。追加的に、又は代替的に、クレデンシャルアプレットのアクセス鍵（例えば、クレデンシャルアプレット 153 a 用のアクセス鍵 155 a 及び／又はクレデンシャルアプレット 153 b 用のアクセス鍵 155 b）は、商業エンティティサブシステム 400 によって生成されてもよく、セキュアエレメント 145 と商業エンティティサブシステム 400 との間で当該アプレットの当該クレデンシャル情報のセキュアな送信を可能とするため、（例えば、図 1 A に示すように）商業エンティティサブシステム 400 によってアクセス可能とすることができる。追加的に、又は代替的に、図示するように、各アプレットは、それ自体の一意のアプリケーション識別子（「AID」）、例えば、アプレット 153 a の AID 155 a a 及び／又はアプレット 153 b の AID 155 b a を含むことができる。例えば、AID は、特定のカード方式及び製品、プログラム又はネットワーク（例えば、MasterCard Cirrus、Visa PLUS、Interac など）を識別することができ、AID は、AID に関連付けられたクレデンシャルの決済システム（例えば、カード方式）又はネットワーク（例えば、MasterCard、Visa、Interac など）を識別するのに使用され得る登録されたアプリケーションプロバイダ識別子（「RID」）だけでなく、AID に関連付けられたクレデンシャルのプロバイダ又は決済システムによって提供される製品、プログラム、又はアプリケーション間を区別するのに使用され得る専用アプリケーション識別子拡張（「PIX」）も含むことができる。セキュアエレメント 1

10

20

30

40

50

45のファームウェアを統括するように機能し得る任意の好適な仕様（例えば、Java（登録商標）カード仕様）は、セキュアエレメント145上の各AIDの一意性を確実にするか、又は他の方法で強制するように機能することができる（例えば、セキュアエレメント145上の各クレデンシャルインスタンスをそれ自体の一意のAIDと関連付けることができる）。

【0028】

追加的に、又は代替的に、図2Aに示すように、セキュアエレメント145はISD152を含むことができ、それは、そのセキュリティドメインに関連付けられた信頼されたサービスマネージャ（例えば、図1Aに示す、商業エンティティサブシステム400）にも知られたISD鍵156kを含むことができる。ISD鍵156kは、商業エンティティサブシステム400と電子デバイス100のセキュアエレメント145との間のセキュアな送信を可能とするために、アクセス鍵155a及び／又はアクセス鍵155bと同様に、かつ／又はその代わりに、商業エンティティサブシステム400及び電子デバイス100によって活用されることがある。また、図2Aに示すように、プロセッサ102とセキュアエレメント145との間で各種データを通信してもよい。例えば、デバイス100のプロセッサ102は、プロセッサ102の販売事業者アプリケーション113、ならびに、セキュアエレメント145、（例えば、I/O入力データ115iを受信するための、かつ／又は、I/O出力データ115oを送信するための）I/Oインタフェース構成要素114a及び／又は通信構成要素106と、情報を通信することができるデバイスアプリケーション103を実行するように構成することができる。また、図示するように、プロセッサ102は、デバイス識別情報119にアクセスすることができ、それは、デバイス100とリモートエンティティとの間のセキュアな通信を可能とするために利用され得る。

【0029】

追加的に、又は代替的に、図2Aに示すように、セキュアエレメント145は、制御権限セキュリティドメイン（「CASD」）158を含むことができ、それは、サードパーティオンエレメントの信頼のルート（third-party on-element root of trust）として機能するように構成され得る特定の目的のセキュリティドメインとすることができる。CASD158に関連付けられたアプリケーションは、他のアプリケーション及び／又は特定の管理層（例えば、Global Platform管理層）へのグローバルサービスとして、オンエレメント機密鍵生成を提供するように構成されてもよい。CASD158内で使用され得る機密鍵素材は、セキュアエレメント145の発行者を含むいかなるエンティティによっても検査又は修正されないように構成されてもよい。CASD158は、CASDアクセスキット158k（例えば、CASD秘密鍵（「CASD-SK」）、CASD公開鍵（「CASD-PK」）、CASD証明書（「CASD-Cert.」）及び／又はCASD署名モジュール）を含むように構成されてもよく、かつ／又はそれを生成し、かつ／又は他の方法で、それを含むように構成されてもよい。例えば、CASD158は、デバイス100の別の部分（例えば、システム1の他のサブシステムと共有するための通信構成要素106）に特定のデータを提供する前に、セキュアエレメント145上で特定のデータに（例えば、CASDアクセスキット158kを用いて）署名するように構成することができる。例として、CASD158は、セキュアエレメント145によって提供される任意のデータに署名し、他のサブシステム（例えば、商業エンティティサブシステム400）がそのような署名されたデータが、セキュアエレメント145によって署名されたことを（例えば、商業エンティティサブシステム400において関連付けられたCASDキット158kを用いて）確認することができるよう構成され得る。

【0030】

追加的に、又は代替的に、図2Aに示すように、セキュアエレメント145は、特定のセキュリティドメインエレメントのライフサイクル状態（例えば、アクティブ化され、非アクティブ化された、ロックされた、など）を修正し、特定のライフサイクル状態での特

10

20

30

40

50

定のセキュリティドメインエレメントについての特定の出力情報 115 o を、デバイス 100 のユーザと（例えば、ユーザ I / O インタフェース 114 a を介して）共有するための電子デバイス 100 にローカル機能性を提供するように構成され得る非接触レジストリサービス（「CRS」）アプレット又はアプリケーション 151 を含むことができる。例えば、CRS アプリケーション 151 は、セキュアエレメント 145 上の各セキュリティドメインエレメントの現在のライフサイクル状態のリストを維持し得る CRS リスト 151 t（例えば、SSD 154 a のクレデンシャルアプレット 153 a 及び／又は SSD 154 b のクレデンシャルアプレット 153 b の 1 つ、一部又は全部のライフサイクル状態を含み得るリスト）を含むことができ、CRS アプリケーション 151 は、セキュアエレメント 145 の 1 つ以上のセキュリティドメインエレメントのライフサイクル状態を、（例えば、オペレーティングシステムアプリケーション 103 内のバックグラウンドプロセスとして実行し得るカード管理デーモン（「CMD」）アプリケーション 103 a 及び／又はカード管理アプリケーション 103 b（例えば、アップル インコーポレイテッドによる Passbook（登録商標）又は Wallet（登録商標）アプリケーション）及び／又は販売事業者アプリケーション 113（例えば、販売事業者鍵 157 及び販売事業者識別子 167 と関連付けられ得る販売事業者オンラインリソース）及び／又は識別サービス（「IDS」）アプリケーション 103 c などのデーモンのような任意の好適なアプリケーションタイプであって、必ずしもデバイス 100 のインタラクティブなユーザの制御下にある必要はない）デバイス 100 のアプリケーションと共有するように構成され得、また、それは、特定のライフサイクル状態情報をデバイス 100 のユーザに、出力情報 115 o として、I / O インタフェース 114 a 及びユーザインタフェース（「UI」）アプリケーション（例えば、カード管理アプリケーション 103 b の UI）を介して提供することができ、それにより、（例えば、特定のクレデンシャルアプレットの商業クレデンシャルを財務トランザクションに使用可能とするよう、CRS リスト 151 t 及びセキュリティドメインエレメントのライフサイクル状態を更新するために）ユーザがセキュリティドメインエレメントのライフサイクル状態を変更可能とすることができる。追加的に、又は代替的に、CRS 151 は、CRS 151 に関連付けられた信頼されたサービスマネージャ（例えば、図 1 A に示すような、商業エンティティサブシステム 400）にも知られ得る CRS アクセス鍵 151 k を含むことができる。商業エンティティサブシステム 400 と電子デバイス 100 のセキュアエレメント 145 との間のセキュアな送信を可能とするため、アクセス鍵 155 a 及び／又はアクセス鍵 155 b と同様に、かつ／又はその代わりに、CRS アクセス鍵 151 k を商業エンティティサブシステム 400 及び電子デバイス 100 により活用することができる。

【0031】

IDS アプリケーション 103 c は、オペレーティングシステムアプリケーション 103 及び／又はカード管理アプリケーション 103 b の内部でバックグラウンドプロセスとして実行し得る、かつ／又は CMD アプリケーション 103 a によって提供され得るデーモンのような任意の好適なアプリケーションタイプとすることができ、また、それは、任意の好適な IDS サービス上で送信され得る IDS メッセージをリスニングし、それに応答する IDS マネージャとして動作することができ、IDS マネージャは、アップル インコーポレイテッドによる iMessage（登録商標）など（例えば、アップル インコーポレイテッドによる FaceTime（登録商標）又は Continuity（登録商標））のような任意の好適なメッセージングサービスと同様とすることができ、これにより、ホストデバイス 100 の IDS アプリケーション 103 c と別のデバイス（例えば、クライアントデバイス）同様の IDS アプリケーションとの間のメッセージの一意のエンドツーエンド暗号化を可能とすることができる。そのようなメッセージを、通信デバイスの一方又は両方の、及び／又は通信デバイスの特定のユーザの一方又は両方の一意の識別子を用いて暗号化することもできる。このようなメッセージを、ローカルリンク又は真のデバイスツーデバイス（例えば、ピアツーピア）通信として通信してもよいし、商業エンティティサブシステム 400 を介して（例えば、識別管理システム構成要素 470 を介し

10

20

30

40

50

て) 通信してもよい。このようなメッセージングを、構造化されたフォーマット (例えば、プロトコルバッファ) 及び/又は非構造化フォーマットでデータを交換することを可能にし得る低遅延ソリューションとして可能とすることができる。IDSアプリケーション103cは、IDSメッセージが受信されたとき、実行されていない場合は、自動的に起動され得る。IDSアプリケーション103cは、受信したIDS通信に関するユーザインタフェース表示及び要求されたデータに関する要求デバイスへの応答を見張るよう機能し得る。ホストデバイスのISDアプリケーション103cは、初期要求をクライアントデバイスから検出し得るときに、カード管理アプリケーション103bのカード管理デーモンアプリケーション103aを稼働状態に復帰させるように機能することができ、これにより、ホストデバイスが低電力「スリープ」モードで動作することを可能とすることができる。IDSアプリケーション103cは、追加的に又は代替的に、このような要求の「タイムアウト」を管理するように機能することができ、それにより、クライアントデバイスからの決済の要求がホストデバイス上で一定期間 (例えば、そのような要求に応答するホストデバイスの能動的なユーザ対応がない場合、60秒) アクションがない場合、IDSアプリケーション103cは、要求を終了させてホストデバイスが「キャンセル」状態を生成しクライアントデバイスに配信する結果となり得る判定を行うように機能することができ、それにより、適切なメッセージ (例えば、クライアントデバイスのユーザに対する「タイムアウトエラー」) を表示することができる。

図3及び図3A～図3Dの説明

【0032】

図3に示すように、また以下により詳細に説明するように、電子デバイス100の特定の例としてはiPhone (登録商標) のようなハンドヘルド型電子デバイスとすることができ、筐体101は、デバイス100とユーザならびに/又は周辺環境とが互いにインタフェースし得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とすることができる。例えば、タッチスクリーンI/O構成要素114aは、表示出力構成要素112a及び関連タッチ入力構成要素110fを含むことができ、表示出力構成要素112aは、ユーザが電子デバイス100と相互作用することを可能にし得る視覚又はグラフィックユーザインタフェース (「GUI」) 180を表示するために使用されてもよい。GUI180は、表示出力構成要素112aの領域の全部又は一部に表示され得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) の種々の層、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は、GUI180の1つ以上のグラフィック要素又はアイコン182を有する第1の画面190を表示するように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、デバイス100は、そのアイコン182に関連付けられた新しいアプリケーションを開き、販売事業者オンラインリソースアプリケーションなどの、当該アプリケーションに関連付けられたGUI180の対応する画面を表示するように構成することができる。例えば、「Merchant App」テキストインジケータ181 (すなわち、特定のアイコン183) がラベル付けされた特定のアイコン182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販売事業者アプリケーション (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、又は他の方法で、それにアクセスすることができる。別の例として、「Internet」テキストインジケータ (すなわち、特定のアイコン184) がラベル付けされた特定のアイコン182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、別のタイプの販売事業者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販売事業者のウェブリソースのURLに向けられ得るインターネットブラウザアプリケーションを起動し、又は他の方法でそれにアクセスすることができる。任意の好適な販売事業者オンラインリソースがアクセスされると、デバイス100は、特定の方法 (例えば、デバイス100の任意のセキュア機能を実行するために (例えば

、デバイス100のNFC構成要素120のクレデンシャル（例えば、クレデンシャルSD154aのクレデンシャル）を用いて販売事業者サブシステム200に決済を行うために）、デバイスユーザにより使用され得る任意の好適なアプリケーション（例えば、販売事業者オンラインリソース113）の使用中の、GUI180のこのような表示の特定の例のための図3A～図3D参照）でデバイス100を用いて当該販売事業者オンラインリソースと相互作用するための1つ以上のツール又は特徴を含み得る特定のユーザインタ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。各アプリケーションに対して、画面は表示出力構成要素112a上に表示されてもよく、種々のユーザインタフェース要素を含んでもよい。追加的に、又は代替的に、各アプリケーションに対して、他の種々のタイプの非視覚情報を、デバイス100の種々の他の出力構成要素112を介してユーザに提供してもよい。例えば、いくつかの実施形態では、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フェース構成要素を含まなくてもよいが、代わりに、トランザクションに資金供給するために決済クレデンシャルの使用を選択及び認証するための、又はデバイスの他の好適なセキュアな任意の機能を行うための、オーディオ出力構成要素及び機械的又は他の好適なユーザ入力構成要素を提供してもよい。

【0033】

図4の説明

ここで図4を参照すると、図4は、システム1の商業エンティティサブシステム400の特定の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、商業エンティティサブシステム400は、セキュアプラットフォームシステムとすることができ、セキュア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。商業エンティティサブシステム400の1つ、一部、又は全部の構成要素を、デバイス100のプロセッサ構成要素102と同一又は類似であり得る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と同一又は類似であり得る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と同一又は類似であり得る、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。商業エンティティサブシステム400の1つ、一部又は全部の構成要素は、金融機関サブシステム350及び／又は販売事業者サブシステム200とは別個の独立したものであり得る単一の商業エンティティ（例えば、アップル インコーポレイテッド）によって管理され、所有され、少なくとも部分的に制御され、及び／又は他の方法で提供されてもよい。商業エンティティサブシステム400の構成要素は、新しいセキュリティ層を提供するために、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ために、互いに相互作用することができ、また、任意の好適な金融機関サブシステム350及び／又は電子デバイス100及び／又は販売事業者サブシステム200と集合的に相互作用することができる。

【0034】

商業エンティティサブシステム400のSMPブローカ構成要素440は、商業エンティティユーザアカウントを用いたユーザ認証を管理するように構成することができる。SMPブローカ構成要素440はまた、デバイス100上のクレデンシャルのライフサイクル及び供給を管理するように構成することができる。SMPブローカ構成要素440は、デバイス100上のユーザインタフェース要素（例えば、GUI180の要素）を制御し得る主エンドポイントとすることができる。オペレーティングシステム又はエンドユーザデバイスの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）は、特定のアプリケーションプログラムインタフェース（「API」）を呼び出すように構成することができ、またSMPブローカ440は、これらのAPIの要求を処理し、デバイス100のユーザインタフェースを導き出し得るデータで応答するように、及び／又は、セキュアエレメント

145と（例えば、商業エンティティサブシステム400と電子デバイス100との間の通信経路65を介して）通信し得るアプリケーションプロトコルデータユニット（「APDU」）で応答するように構成することができる。このようなAPDUは、金融機関サブシステム350から、システム1の信頼されたサービスマネージャ（「TSM」）（例えば、商業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との間の通信経路55のTSM）を介して商業エンティティサブシステム400により受信され得る。商業エンティティサブシステム400のSMP TSM構成要素450は、金融機関サブシステム350からのデバイス100へのクレデンシャル供給動作を実行するために使用され得る、Global Platformベースのサービス又は他の好適なサービスを提供するように構成することができる。Global Platform、又は任意の他の好適なセキュアなチャンネルプロトコルは、SMP TSM構成要素450が、商業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との間のセキュアな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との間で、機密なアカウントデータを適正に通信及び／又は供給することを可能とすることができる。

10

【0035】

SMP TSM構成要素450は、HSM構成要素490を使用してその鍵を保護し、新しい鍵を生成するように構成することができる。商業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は、システム1の種々の構成要素間のユーザ認証及び／又は機密データ送信のために提供され得る鍵管理及び暗号化動作を提供するように構成することができる。SMP暗号サービス構成要素460は、セキュアな鍵記憶及び／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。SMP暗号サービス構成要素460の決済暗号サービスは、IDMS構成要素470と相互作用し、ファイル上のクレジットカードに関連付けられた情報又は、商業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業クレデンシャルを取り出すように構成することができる。このような決済暗号サービスは、メモリ内のそのユーザアカウントの商業クレデンシャル（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）情報を有し得る商業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。IDMS構成要素470は、（例えば、商業エンティティ固有サービス（例えば、アップル インコーポレイテッドによるiMessage（登録商標））を用いた）識別サービス（「IDS」）転送のような、デバイス100と別のデバイスとの間の好適な通信を可能とする、かつ／又は管理するように構成することができる。例えば、特定のデバイスを、そのようなサービスに対して自動で又は手動で登録することができる（例えば、商業エンティティ400のエコシステム内のすべてのデバイスを、そのサービスに対して自動で登録することができる）。サービスを使用して（例えば、デバイス100のISDアプリケーション103cを使用して）メッセージが送信可能となる前に、このようなサービスは、アクティブな登録を要求し得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。商業エンティティサブシステム400が、特定のユーザアカウントと関連付けられた特定のクライアントデバイス（例えば、商業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得る1つ以上の非ネイティブ決済クレデンシャルを効率的かつ効果的に識別するように機能することができるように、IDMS構成要素470及び／又は他の好適な任意のサーバ若しくは運用エンティティサブシステム400の一部は、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供給された任意のクレデンシャルの状況を識別するように、又は他の方法で検索するように機能することができる。商業エンティティサブシステム400の商業エンティティ不正システム構成要素480は、商業クレデンシャル及び／又はユーザについて商業エンティティに既知のデータ（例えば、商業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に基づいて（例えば、商業クレデンシャル情報）、及び／又は商業エンティティの制御下にあり得る他の好適な任意のデータ、及び／又は金融機関サブシステム350の制御下にないかも知れない他の好適な任意のデータに基

20

30

40

50

づいて)、商業クレデンシャルに関する商業エンティティ不正検査を実行するように構成することができる。商業エンティティ不正システム構成要素480は、種々の要因又は閾値に基づいて、クレデンシャルに対する商業エンティティ不正スコアを決定するように構成されてもよい。追加的に、又は代替的に、商業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/レンタルする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/レンタルするApple App Store(登録商標)、デバイス100からのデータを記憶しかつ/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。一例として、ストア420は、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65を介して)提供するように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、商業販売事業者アプリケーション、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)商業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/又は商業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55を介した金融エンティティサブシステム350及び/又は図1の通信経路65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商業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。

【0036】

図5の説明

図5は、セキュアデバイス機能へのオンラインアクセスを妥当性検査するための例示的なプロセス500のフローチャートである。プロセス500は、電子デバイス100、商業エンティティサブシステム400、及び販売事業者サブシステム200によって実施するように示されている。しかし、プロセス500は、他の任意の好適な構成要素又はサブシステムを用いて実施され得ることを理解されたい。プロセス500は、販売事業者サブシステム200とのトランザクション(例えば、オンライン決済又は非接触近接型決済)における電子デバイス100でのクレデンシャルのセキュアな使用を可能とするための、又は電子デバイス100の任意の他の好適なデータ(例えば、位置データ、健康データ、又は任意の他のプライベートデータ又は有効に妥当性検査されていないサードパーティサブシステムと共有されるべきではないもの)の販売事業者サブシステム200によるセキュアなアクセスを可能とするための、商業エンティティサブシステム400による販売事業者サブシステム200の妥当性検査などの、販売事業者サブシステム200による電子デバイス100のセキュア機能へのオンラインアクセスを可能とするために、サードパーティ販売事業者サブシステム200をセキュアにかつ効率的に妥当性検査する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る。販売事業者オンラインリソース又は鍵若しくはサーバ若しくは端末若しくは識別子などの販売事業者サブシステム200及び/又はそのいずれかの特徴を記述するために用語「販売事業者(merchant)」を利用することができるが、サブシステム200は、電子デバイス100の所有者又はユーザとは、及び/又は商業(又は運用)エンティティサブシステム400とは別個であり得る、任意の好適なサードパーティエンティティによって動作される任意の好適なサブシステム(例えば、処理サブシステム(例えば、データ処理サブシステム))とすることができることを理解されたい。例えば、販売事業者サブシステム200は、電子デバイス100のセキュアデバイス機能へのアクセス又は他の方法による、受信若しくは相互作用(例えば、販売事業者オンラインリソースを用いた、デバイス100へのデータのロード(例えば、デバイス100への決済クレデンシャルの供給)、デバイス100からのデータの受信(例

10

20

30

40

50

えば、デバイス100の決済クレデンシャルデータ若しくはヘルスケアデータ若しくは位置データ若しくは連絡先データ若しくはプライベートメディアデータへのアクセス)などを試み得る任意の好適なサードパーティサブシステムとすることができる。プロセス500は、デバイス100と任意の好適な販売事業者サブシステムの任意の好適なウェブリソースとの間でよりセキュアで信頼された任意の好適なデータの通信を可能とするように機能することができる。プロセス500は、そのようなデータ通信を可能とする前に、商業エンティティサブシステム400と信頼関係があることを確実にするために、好適なウェブリソース又は他のオンラインリソースを妥当性検査するように機能することができる。

【0037】

プロセス500のステップ501では、販売事業者サブシステム200を商業エンティティサブシステム400に登録することができる。上述のように、販売事業者サブシステム200の販売事業者オンラインリソース113(例えば、ネイティブアプリ、ドメイン/URL、又は任意の他の好適なウェブリソース、又はおそらく販売事業者端末でも)を特定の販売事業者識別子167及び特定の販売事業者鍵157と関連付けることができ、それらのそれぞれを、任意の好適な方法で、販売事業者サブシステム200と商業エンティティサブシステム400の間でセキュアに共有することができ、そのような関連付けは、(例えば、表430内で)商業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。いくつかの実施形態では、ネイティブアプリケーション(例えば、ネイティブアプリケーション販売事業者オンラインリソース113)の開発者は、権利付与のシステムを使用して、アプリケーションを実行する電子デバイス100のセキュアデバイス機能(例えば、プッシュメッセージング、クラウドストレージ、セキュアエレメントクレデンシャル決済等)へのアクセスを可能とすることができ、その権利付与は、(例えば、アプリケーションストア420への配置のため、及び/又は表430内でアプリケーションの販売事業者鍵157及び販売事業者識別子167をセキュアに関連付けるために)アプリケーションが商業エンティティサブシステム400により登録されるのを可能とするのに必要とされ得るコード署名プロセスの一部としてアプリケーションのバイナリに署名されてもよく、例えば、販売事業者識別子167はアプリケーションの権利付与の一部を形成することができる。このようなネイティブアプリケーションとは異なり、ウェブリソース(例えば、ウェブサイト販売事業者オンラインリソース113)は、電子デバイス100上で実行され得るように機能するネイティブアプリケーションに(例えば、商業エンティティサブシステム400によって)提供され得るコード署名又は同様の保護を有し得ない。代わりに、ウェブリソースのドメインの所有権を、当該ウェブリソースを登録し得る前に証明してもよい。販売事業者サブシステム200によって所有、又は、又は他の方法で制御されたウェブサイト販売事業者オンラインリソース113を登録するためには、このような所有権を、商業エンティティサブシステム400による販売事業者オンラインリソース113の登録前に(例えば、特定の販売事業者識別子167及び特定の販売事業者鍵157を当該販売事業者オンラインリソース113に関連付けて、(例えば、表430内の)商業エンティティサブシステム400による将来のアクセスのために販売事業者サブシステム200と商業エンティティサブシステム400との間で共有する前に)、商業エンティティサブシステム400に証明しなければならない。例えば、商業エンティティサブシステム400に登録される販売事業者オンラインリソース113のドメインの所有権を証明するためには、ドメインの識別情報を商業エンティティサブシステム400に提供することができ、商業エンティティサブシステム400は任意の好適なファイル(例えば、JSONファイルなどの静的ファイル)を販売事業者サブシステム200に提供し、販売事業者サブシステム200は(例えば、共有された販売事業者鍵157によって)当該ファイルに署名し、登録されるドメイン上の周知のパスに当該ファイルをホストすることができ、そして、商業エンティティサブシステム400は、ドメインから当該署名されたファイルにアクセスし、(例えば、共有された販売事業者鍵157によって)ファイルの署名を削除し、アクセスしたファイルが販売事業者サブシステム200と共有

10

20

30

40

50

したファイルと一致することを確認することができる。ウェブリソースを登録するためのいくつかの例示的なプロセスは、「Sharing Account Data Between Different Interfaces To A Service」と題された米国特許出願公開第2015/0350106号に記載され、その全体が参照により本明細書に組み込まれる。ステップ502では、商業エンティティサブシステム400に、販売事業者サブシステム200の任意の好適なタイプの販売事業者オンラインリソース113（例えば、デバイス上でローカルに実行しているか、サーバ上でリモートでホストされているか、それとも、デバイスに近接して配置されるかにかかわらず、ネイティブアプリ、ハイブリッドアプリ、ウェブリソース、又は電子デバイスにより利用される販売事業者の販売事業者端末も）の妥当性をセキュアに登録する任意の好適なプロセス又はプロセス（複数可）を利用することができ、それによって、販売事業者オンラインリソース113に関連付けられた少なくとも1つの販売事業者識別子167及び少なくとも1つの販売事業者鍵157（例えば、対称又は非対称鍵ペア）を、販売事業者オンラインリソース113と関連付けることができ、将来の使用のために（例えば、表430内で）販売事業者サブシステム200及び商業エンティティサブシステム400の両方にとってアクセス可能にさせることができ、また任意の好適なデータを、任意の好適な方法（例えば、アプリケーション113、鍵157、識別子167及び／又は任意の好適な通信プロトコル（単数又は複数）を用いた通信経路85を介した任意の他の好適なデータ）でそのようなプロセスの間、販売事業者サブシステム200と商業エンティティサブシステム400との間で通信することができる。1つ以上の販売事業者識別子を特定の販売事業者オンラインリソース113と関連付けることができ、例えば、第1の販売事業者識別子167を特定の販売事業者オンラインリソース113と一意に関連付けて、及び／又は、第2の販売事業者識別子167を特定の販売事業者サブシステム200のそれぞれの販売事業者オンラインリソース113と関連付けることができる。追加的に、又は代替的に、1つ以上の販売事業者鍵を、特定の販売事業者識別子又は特定の販売事業者オンラインリソース113と関連付けてもよい。このような販売事業者鍵及び販売事業者識別子のすべての関連付けを、ステップ501の1つ以上のインスタンスにおいて、商業エンティティサブシステム400（例えば、1つ以上の表430内に）に記憶してもよいし、又は他の方法で、商業エンティティサブシステムにとってアクセス可能としてもよい。

【0038】

プロセス500のステップ502では、登録された販売事業者オンラインリソースを用いて、販売事業者サブシステム200と電子デバイス100との間で潜在的トランザクションデータを通信することができる。例えば、販売事業者オンラインリソースアプリケーション113を実行中の、又は他の方法でそれにアクセス中のデバイス100とユーザが相互作用している間（例えば、ユーザが販売事業者の商品又はサービスをオンラインショッピングしている間、又はユーザがヘルスケアプロフェッショナルと通信している間）のある時点では、潜在的トランザクションデータが、デバイス100に、販売事業者サブシステム200、又は、デバイス100と販売事業者（又は処理）サブシステム200の販売事業者（又はプロセッサ）との間で生じ得る、潜在的なセキュアなデータトランザクションに関する任意の好適なデータを示し得る任意の他の好適なエンティティから通信されることがある。潜在的トランザクションデータは、以下を含むがこれに限られない。（i）販売事業者オンラインリソースアプリケーション113の少なくとも1つの又はそれぞれの販売事業者識別子167などの特定の販売事業者情報、（ii）デバイス100と販売事業者サブシステム200との間で共有される特定のタイプのセキュアなデータの識別情報などの特定のトランザクション情報（例えば、財務トランザクションの通貨及び金額ならびに決済タイプ（例えば、デバイス100上に供給されたVisa決済クレデンシャルを用いた5米ドル）、健康トランザクションのヘルスケアデータのタイプ及び量（例えば、デバイス100により検出された、又は他の方法で取得された過去3日間にわたる特定のユーザの心拍数データ）など）、及び／又は（iii）一意の販売事業者ベースのトランザクション識別子（例えば、行われているトランザクションと関連付けるための販売事業

者サブシステム200によりランダムに又は一意に生成され得る複数文字英数字列などの任意の好適なデータ要素)が挙げられるが、これらに限定されない。このような潜在的トランザクションデータは、関連データの有無にかかわらず、購入を行う顧客の連絡先情報フィールド(例えば、電話番号、電子メールアドレス、送り先住所)などの、セキュアなデータトランザクションを完了するのに必要とされ得る、又は少なくとも使用され得る任意の好適な数及びタイプのデータフィールドを含むことができ、いくつかのフィールドは、そのような潜在的トランザクションデータの一部として取り込まれ、挿入されてもよく、及び/又はいくつかのフィールドは、そのような潜在的トランザクションデータの一部としては取り込まれないが、空になっており、プロセス500の後半部分の間に取り込まれるのを待ち受けてもよい。ステップ502のこのような潜在的トランザクションデータは、本明細書では、(例えば、財務トランザクションのための)PKDataRequest又はPKPaymentRequestと呼ばれる場合がある。いくつかの実施形態では、販売事業者サブシステム200と関連付けられた潜在的トランザクションデータをステップ502でデバイス100にとって利用できるようにさせるために、ユーザはデバイス100とアクティブに相互作用しなくてもよい。代わりに、例として、デバイス100は、すべて自動で、デバイス100のユーザによるいかなるアクティブな相互作用もなしに、特定の製品を購入すべきことを判定し、当該特定の製品の少なくとも1つの特定の販売事業者から関連付けられたトランザクションデータを取得するために1つ以上の販売事業者と相互作用するように構成することができる(例えば、デバイス100は、家電製品を購入しなければならないことを判定する(例えば、洗濯機がより多くの洗濯洗剤を必要とすることを検出する、又は特定の日付により多くの洗剤を購入するように、ユーザが事前に設定したカレンダー行事を検出する)ように構成され得る家電であって、自動で、当該製品の最良の商談を提供する特定の販売事業者を識別することができ、自動で、販売事業者オンラインリソースを用いて当該販売事業者と相互作用し、当該製品を当該販売事業者から購入するために、トランザクションデータを取得し得る家電とすることができる)。ステップ502の潜在的トランザクションデータは、潜在的トランザクションデータと関連付けられたセキュアなデータトランザクションを完了する(例えば、財務トランザクションに資金供給する)ために、デバイス100がセキュアにセキュアデバイスデータ(例えば、適切な決済クレデンシャルデータ)を生成し、かつ/又は、それを販売事業者サブシステム200に提供するのに必要なすべてのデータを含むことができる。このような潜在的トランザクションデータは、ステップ502において、任意の好適な方法で販売事業者サブシステム200によってデバイス100に通信することができる(例えば、このような潜在的トランザクションデータは、任意の好適な通信プロトコルを用いた通信経路15を介して、又は任意の好適な通信プロトコルを用いた端末220とNFC構成要素120との間の非接触近接型通信チャネルを介して、販売事業者サブシステム200のサーバ210からデバイス100の通信構成要素106に送信することができる)。

【0039】

プロセス500のステップ504では、販売事業者オンラインリソース妥当性検査セッションを開始することができる。このことは、電子デバイス100がセキュアなデータトランザクション(例えば、ステップ502の潜在的トランザクションデータによって識別されたセキュアなデータトランザクション)が生じることを示すことに応じて(例えば、デバイス100のユーザが、ステップ502の販売事業者オンラインリソースの潜在的トランザクションデータにより識別されたセキュアなデータトランザクションを行うユーザの願望を伝えるために、販売事業者オンラインリソースのGUIエレメント(例えば、無線ボタン)を選択することに応じて、又は任意の好適な要件が満たされたことに自動的に基づいて(例えば、ステップ502の潜在的トランザクションデータがデバイス100に通信されることに単に応じて))生じ得る。販売事業者オンラインリソースと特定のセキュアなデータトランザクションを実行するような意図が判定されると、デバイス100上の販売事業者オンラインリソース113は、データトランザクション要求を生成してカード管理アプリケーション103b又はデバイス100上の他の好適なデバイスアプリケー

10

20

30

40

50

ションを送信するように機能することができ、当該デバイスアプリケーション103bは、ステップ504において販売事業者妥当性検査セッション開始データを生成し販売事業者サブシステム200に通信するように機能することができる。ステップ504では、実行される特定のセキュアなデータトランザクションに対する販売事業者オンラインリソース妥当性検査セッションを開始するための販売事業者妥当性検査セッション開始データとして、任意の好適なデータが、電子デバイス100により生成され、かつ／又は販売事業者サブシステム200に通信され得る。例えば、ステップ504では、妥当性検査セッション識別子がデバイス100によって生成され、それを販売事業者妥当性検査セッション開始データの少なくとも一部分として販売事業者サブシステム200に通信することができる、そのような妥当性検査セッション識別子は任意の好適な英数字列又は任意の他の好適な識別子とすることができ、それらは、開始されている現在の販売事業者オンラインリソース妥当性検査セッションを一意に識別する（例えば、少なくとも一定期間、セッションが販売事業者サブシステム200及び／又は商業エンティティサブシステム400に対するものであることを一意に識別する）ことができる。デバイス100によって生成されると、妥当性検査セッション識別子は、妥当性検査セッション識別子の生成を助けるように、デバイス100の一意の識別子（例えば、デバイス識別子119又はデバイス100に対して（例えば、商業エンティティサブシステム400に対して）一意となり得るデバイス100のセキュアエレメント145の一意のセキュアエレメント識別子）を利用することで商業エンティティサブシステム400に対して一意とされることができる。追加的に、又は代替的に、ステップ504では、販売事業者妥当性検査セッション開始データの少なくとも一部分として、チャレンジ要求ターゲット識別子（例えば、チャレンジ要求URL）を、デバイス100から販売事業者サブシステム200に通信することができ、このようなチャレンジ要求ターゲット識別子は、販売事業者サブシステム200が、販売事業者を妥当性検査するために通信することとなるエンティティを識別することができる（例えば、実行される特定のセキュアなデータトランザクションの販売事業者オンラインリソースを妥当性検査するために、販売事業者サブシステム200と協働し得る商業エンティティサブシステム400のサーバ410を識別するURL）。デバイスアプリケーション（例えば、カード管理アプリケーション103b（例えば、ウォレットアプリケーション））は、商業エンティティサブシステム400によって制御され得る任意の好適なオペレーティングシステム又はアプリケーション更新の一部としてプログラミングされたこのようなチャレンジ要求ターゲット識別子を有することができるので、チャレンジ要求ターゲット識別子を、デバイス100上で、任意の好適な時間に商業エンティティサブシステム400により更新することができる。追加的に、又は代替的に、このような販売事業者妥当性検査セッション開始データは、自身を妥当性検査するよう販売事業者への要求を示す任意の好適なデータ、デバイス100を示す任意の好適なデータ（例えば、デバイス識別子119）及び／又は実行される特定のセキュアなデータトランザクションを示す任意の好適なデータ（例えば、特定の販売事業者情報（例えば、販売事業者識別子167）、特定のトランザクション情報（例えば、財務トランザクションの通貨及び金額ならびに決済タイプ又は健康トランザクションのヘルスケアデータのタイプ又は量）などのステップ502の潜在的トランザクションデータからの任意の好適なデータ）、及び／又は一意の販売事業者ベースのトランザクション識別子などの、他の任意の好適なデータを含むことができる。ステップ504では、任意の好適な販売事業者妥当性検査セッション開始データを、任意の好適な方法で、デバイス100によって販売事業者サブシステム200に通信することができる（例えば、このような販売事業者妥当性検査セッション開始データを、任意の好適な通信プロトコルを用いた通信経路15を介して、又は任意の好適な通信プロトコルを用いたNFC構成要素120と端末220との間の非接触近接型通信チャネルを介してデバイス100の通信構成要素106から販売事業者サブシステム200のサーバ210に送信することができる）。

【0040】

プロセス500のステップ506では、販売事業者サブシステム200が妥当性検査セ

10

20

30

40

50

セッションを開始するためにステップ504でデバイス100から任意の好適な販売事業者妥当性検査セッション開始データを受信したことに応じて、販売事業者サブシステム200は、販売事業者オンラインリソースを妥当性検査するために商業エンティティサブシステム400と通信するように機能することができる。いくつかの実施形態では、ステップ504の販売事業者妥当性検査セッション開始データが妥当性検査セッション識別子を含まない場合、販売事業者サブシステム200は、開始されている現在の販売事業者オンラインリソース妥当性検査セッションを一意に識別し得るような妥当性検査セッション識別子を生成するように機能することができる。販売事業者サブシステム200により生成されると、販売事業者サブシステム200が同一の妥当性検査セッション識別子を、少なくとも、同一の商業エンティティサブシステムに対して、かつ／又は同一の販売事業者識別子に対して、かつ／又はセッション識別子が商業エンティティサブシステムにおいて任意の特定のプロセスに保留されていないことを確実にするのに十分な一定期間内に、2回使用しないことを確実にすることによって、妥当性検査セッション識別子は商業エンティティサブシステム400に対して一意となり得る。ステップ506は、商業エンティティサブシステム400が、（例えば、ステップ502及び504で識別されるように）実行される特定のセキュアなデータトランザクションのために販売事業者オンラインリソースを妥当性検査することを可能にし得る適切な数のサブプロセスを含むことができる。図6のプロセス600のステップ614～ステップ622に関して詳細に記載するように、ステップ506の妥当性検査は、販売事業者サブシステム200が妥当性検査される販売事業者オンラインリソースと関連付けられた販売事業者識別子（例えば、販売事業者オンラインウェブリソースのドメインであり得るステップ501で登録された販売事業者識別子167）、（例えば、ステップ504でデバイス100により、又はステップ506で販売事業者サブシステム200により生成された）妥当性検査セッション識別子、及び任意の他の好適なデータ（例えば、デバイス100を識別するデータ及び／又は実行される特定のセキュアなデータトランザクションを識別するデータ）を含み得るチャレンジ要求を、（例えば、ステップ504でデバイス100から販売事業者妥当性検査セッション開始データにより識別され得るような）商業エンティティサブシステム400に通信することを含むことができる。このようなチャレンジ要求は、（例えば、HTTPヘッダ又は別の方法で）販売事業者サブシステム200によって、チャレンジ要求の販売事業者識別子と関連付けられた販売事業者鍵（例えば、（例えば、妥当性検査される販売事業者オンラインリソース113のための）ステップ501で販売事業者識別子167に登録された販売事業者鍵157）で署名することができる。商業エンティティサブシステム400は、このようなチャレンジ要求を受信し、（例えば、（例えば、表430内で販売事業者識別子167を識別することによって）販売事業者オンラインリソース113がステップ501で登録されていたこと、かつまだ妥当であることを確認するために）チャレンジ要求の販売事業者識別子167により識別された販売事業者オンラインリソース113を妥当性検査するように機能することができ、そして、（例えば、表430内の当該識別された販売事業者識別子167と関連付けられた販売事業者鍵157を用いて）チャレンジ要求の署名を妥当性検査することができる。チャレンジ要求の要素の妥当性検査に応じて、商業エンティティサブシステム400は、チャレンジデータ（例えば、エンтроピーを介して任意の好適なランダムデータ）を生成し、任意の好適なデータ構造で（例えば、表430等で）識別子データに対してチャレンジデータ（例えば、チャレンジ要求の妥当性検査セッション識別子及び販売事業者の販売事業者識別子の一方又は両方）を記憶し、商業エンティティサブシステム400によりアクセス可能な販売事業者鍵157（例えば、チャレンジ要求の署名を妥当性検査するのに使用される表430からの販売事業者鍵）を用いてチャレンジデータを暗号化し、そして、チャレンジデータを暗号化するのに使用される販売事業者鍵のハッシュ（例えば、複数の登録された販売事業者オンラインリソース及び／又は複数の販売事業者鍵を有し得る販売事業者を支援するために提供され得る、適正な販売事業者鍵157（例えば、チャレンジデータを解読するための販売事業者サブシステム200の秘密鍵157）を識別するために販売事業者サブシステム200によって使用

10

20

30

40

50

され得る表430の公開販売事業者鍵157のハッシュバージョン)、チャレンジ要求の妥当性検査セッション識別子、などの、任意の他の好適なデータとともに暗号化されたチャレンジデータを含み得るチャレンジングデータを、販売事業者サブシステム200に通信することができる。このようなチャレンジングデータの受信に応じて、販売事業者サブシステム200は、適切な販売事業者鍵157(例えば、ステップ501で登録されている販売事業者サブシステム200での秘密販売事業者鍵157)を用いて、暗号化されたチャレンジデータを解読して、そして、チャレンジ要求の妥当性検査セッション識別子及び適切な販売事業者識別子などの任意の他の好適なデータとともに、解読されたチャレンジデータを含むチャレンジレスポンスデータを商業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、当該チャレンジレスポンスは、チャレンジ要求の販売事業者識別子と関連付けられた販売事業者鍵(例えば、(例えば、妥当性検査される販売事業者オンラインリソース113のための)販売事業者識別子167でステップ501で登録された販売事業者鍵157)で(例えば、HTTPヘッダ内に、又は別の方法で)販売事業者サブシステム200によって署名され得る。そのようなチャレンジレスポンスデータの受信に回答して、商業エンティティサブシステム400は、(表430内の識別された販売事業者識別子167と関連付けられた販売事業者鍵157を用いて)チャレンジレスポンスの署名を妥当性検査し、チャレンジレスポンスの解読されたチャレンジデータが、チャレンジレスポンスの妥当性検査セッション識別子に対して、及び/又は(表430内の)販売事業者の識別子に対して記憶されていることを確認するように機能することができる。いくつかの実施形態では、チャレンジデータと妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクを、リンクが自動で削除される前の限られた時間しか維持できないので、販売事業者サブシステム200は、チャレンジングデータを受信し、そして、特定の妥当性検査セッションのための販売事業者オンラインリソースを妥当性検査するために、適切なチャレンジレスポンスデータを商業エンティティサブシステム400に送信しなければならない特定の持続時間に限定されることがあり(例えば、商業エンティティサブシステム400は、特定時間後に商業エンティティサブシステム400で、チャレンジデータと妥当性検査セッション識別子及び/又は販売事業者識別子との間のこのような関連付けを除去する(例えば、リンクが作成された後10分(又は任意の他の好適な時間)以内に表430からのリンクを除去する)ように機能することができる)、それにより、トランザクションのセキュリティを向上させることができる。したがって、(例えば、ステップ501で登録された)商業エンティティサブシステム400における販売事業者鍵と販売事業者識別子との関連付けを用いて、(例えば、ステップ502及びステップ504で識別された)実行される特定のセキュアなデータトランザクションのステップ506における販売事業者オンラインリソースの妥当性検査を完了することができる。ステップ506では、任意の好適なデータを、適切な方法で販売事業者サブシステムと商業エンティティサブシステム400との間で通信することができる(例えば、このようなデータを、好適な通信プロトコルを用いた通信経路85を介して販売事業者サブシステム200のサーバ210と商業エンティティサブシステム400のサーバ410との間で送信することができる)。

【0041】

ステップ508では、ステップ504で開始された妥当性検査セッションに基づいたステップ506での販売事業者オンラインリソースの妥当性検査に応じて、商業エンティティサブシステム400は、妥当性検査データを生成し、妥当性検査セッションの妥当性検査セッション識別子及び/又は販売事業者識別子などの、識別子データに対してそれを記憶することができる。例えば、チャレンジレスポンスの署名の妥当性検査に応じて、かつ、チャレンジレスポンスの当該チャレンジデータ及び妥当性検査セッション識別子及び/又は販売事業者識別子も商業エンティティサブシステム400において(例えば、表430内で)適正にリンクされたことを確認したことに応じて、商業エンティティサブシステム400は、当該リンクを消費し(例えば、商業エンティティサブシステム400においてチャレンジデータと妥当性検査セッション識別子及び/又は販売事業者識別子との間の

10

20

30

40

50

このような関連付けを除去し（例えば、表４３０からリンクを除去し）、妥当性検査データ（例えば、任意の好適なランダムデータ（例えば、暗号ナンス（例えば、エントロピーを介する任意の好適なランダムデータ）））を生成し、そして、ステップ５０８で、妥当性検査データを、チャレンジ要求及び／又はチャレンジレスポンスの妥当性検査セッション識別子に対して、又は他の方法によりそれに関連付けて、及び／又は販売事業者の販売事業者識別子に対して、又は他の方法によりそれに関連付けて、（例えば、表４３０又は別の方法などの任意の好適なデータ構造で）記憶することができる。

【００４２】

ステップ５１０では、ステップ５０６で販売事業者オンラインリソースを妥当性検査し、そして、ステップ５０８で妥当性検査セッション識別子及び／又は販売事業者識別子に対する任意の好適な妥当性検査データを記憶したことに応じて、商業エンティティサブシステム４００は、妥当性検査レスポンスデータを電子デバイス１００に通信することができ、このような妥当性検査レスポンスデータは、限定されることなく、ステップ５０８での妥当性検査データ、ステップ５０８での妥当性検査セッション識別子、ステップ５０６で妥当性検査された販売事業者オンラインリソースを識別するデータ（例えば、販売事業者識別子１６７）及び／又は任意の他の好適なデータを含む、任意の好適なデータを含むことができる。いくつかの実施形態において、図５に示すように、このような妥当性検査レスポンスデータを、商業エンティティサブシステム４００から直接電子デバイス１００に（例えば、任意の好適な通信プロトコルを用いた通信経路６５を介して）通信することができ、商業エンティティサブシステム４００が妥当性検査レスポンスデータを適正な電子デバイス１００に通信することができるように、電子デバイス１００を識別するデータ（例えば、デバイス識別子１１９）を（例えば、ステップ５０２等で）妥当性検査セッション識別子と関連付け、またステップ５０６の妥当性検査と関連付けることができる。代替的に、いくつかの実施形態では、このような妥当性検査レスポンスデータを、商業エンティティサブシステム４００から販売事業者サブシステム２００を介して電子デバイス１００に通信することができ、それによって、販売事業者サブシステム２００は、妥当性検査レスポンスデータを商業エンティティサブシステム４００から（例えば、任意の好適な通信プロトコルを用いた通信経路８５を介して）受信し、そして、妥当性検査レスポンスデータの少なくとも一部分を電子デバイス１００に（例えば、任意の好適な通信プロトコルを用いた通信経路１５を介して、又は非接触近接型通信として）渡すことができる。このような妥当性検査データは、（例えば、ＨＴＴＰヘッダ内で、又は別の方法で）商業エンティティサブシステム４００により、電子デバイス１００にとってアクセス可能であり得る、商業エンティティサブシステム４００に関連付けられたアクセス鍵（例えば、セキュアエレメント１４５のアクセス鍵１５５ａ、アクセス鍵１５５ｂ、ＣＲＳ１５１ｋ及び／若しくはＩＳＤ鍵１５６ｋ又は、デバイスアプリケーション（例えば、カード管理アプリケーション１０３ｂ）に知られ得る任意の鍵）で署名され得るので、デバイス１００は、署名された妥当性検査データを受信するとすぐに署名を妥当性検査し、電子デバイス１００によって信頼されていない別のエンティティサブシステムではなく、商業エンティティサブシステム４００が妥当性検査データを生成したことを確認することができる。

【００４３】

プロセス５００のステップ５１２では、セキュアデバイスデータは、少なくとも部分的にデバイス１００により生成され、アクセスされ得る。そして、ステップ５１４では、このようなセキュアデバイスデータは、ステップ５１０で受信された妥当性検査レスポンスデータの少なくとも一部分及びステップ５０２の潜在的トランザクションデータの少なくとも一部分とともに、デバイストランザクションデータとしてデバイス１００により商業エンティティサブシステム４００に通信され得る。例えば、ステップ５０２の潜在的トランザクションデータに使用されている販売事業者オンラインリソースの妥当性を示し得るステップ５１０での妥当性検査レスポンスデータの受信に応じて、デバイス１００は、特定のセキュアなデータトランザクションを実行するため、ステップ５１２では、販売事業者サブシステム２００と共有されるセキュアなデータを取得するか、他の方法により識別

10

20

30

40

50

する（例えば、財務トランザクションに使用される決済クレデンシャルデータを生成するか、健康トランザクションで共有される特定の健康データを収集する）ように機能することができる。そして、ステップ514では、デバイス100は、ステップ510の妥当性検査レスポンスデータの妥当性検査データ及び妥当性検査セッション識別子及び販売事業者識別子とともに、及び／又は、（例えば、特定の販売事業者情報（例えば、販売事業者識別子167）、特定のトランザクション情報（例えば、財務トランザクションの通貨及び金額ならびに決済タイプ、又は健康トランザクションのヘルスケアデータのタイプ若しくは量）、及び／又は一意の販売事業者ベースのトランザクション識別子など、ステップ502の潜在的トランザクションデータによってデバイス100に提供され得る）実行される潜在的セキュアなデータトランザクションに関する任意の好適なデータとともに、ステップ512のセキュアなデータを、デバイス100のトランザクションデータとして商業エンティティサブシステム400に通信することができる。したがって、ステップ514でデバイス100から商業エンティティサブシステム400に通信されるデバイス100のトランザクションデータは、ステップ502の潜在的トランザクションデータの一部又は全部、ならびにステップ512のセキュアデバイスデータ、ならびにステップ510の妥当性検査レスポンスデータを含むことができる。

10

【0044】

デバイス100は、ステップ514においてデバイス100のトランザクションデータを商業エンティティサブシステム400に通信する前に、ステップ514のデバイス100のトランザクションデータ（例えば、ステップ512のセキュアデバイスデータ）の全部又は少なくとも一部分を商業エンティティ鍵で暗号化することができる。例えば、デバイス100は、セキュアエレメント145のアクセス鍵155a、アクセス鍵155b、CRS151k、CASD158k、及び／若しくはISD鍵156k又は、デバイス100にとって（例えば、デバイス100のアプリケーション103からプロセッサ102にとって等）アクセス可能な任意の他の鍵であって、また商業エンティティサブシステム400にとってもアクセス可能であり得る鍵（例えば、デバイス100と商業エンティティサブシステム400との間の共有秘密）で、デバイス100のトランザクションデータの少なくとも一部分を暗号化することができる。いくつかの実施形態では、このような商業エンティティ鍵又はアクセス鍵は、商業エンティティサブシステム400の方式に関連付けられた商業エンティティ公開鍵とすることができ、商業エンティティサブシステム400は関連付けられた商業エンティティ秘密鍵にアクセスし得る。商業エンティティサブシステム400は、このような商業エンティティ公開鍵を任意の好適な方法で、デバイス100に提供することができる。デバイス100のトランザクションデータは、任意の好適な商業エンティティ鍵による少なくとも部分的な暗号化、及び／又は署名がなされているか否かにかかわらず、ステップ540において、任意の好適な方法で、デバイス100により商業エンティティサブシステム400に通信され得る（例えば、このようなデバイス100のトランザクションデータは、任意の好適な通信プロトコルを用いた通信経路65を介してデバイス100の通信構成要素106から商業エンティティサブシステム400のサーバ410に送信され得る）。

20

30

【0045】

次に、ステップ514で通信されたデバイス100のトランザクションデータを受信した後、プロセス500のステップ516は、商業エンティティサブシステム400がステップ514で受信した受信デバイス100のトランザクションデータの妥当性検査データを妥当性検査することを含むことができる。例えば、このようなデバイス100のトランザクションデータの受信に応じて、商業エンティティサブシステム400は、当該デバイス100のトランザクションデータから妥当性検査レスポンスデータを識別し、ステップ516では、当該受信した妥当性検査レスポンスデータの当該妥当性検査データが、受信したデバイス100のトランザクションデータ（例えば、妥当性検査レスポンスデータ）の妥当性検査セッション識別子に対して、及び／又は受信したデバイス100のトランザクションデータ（例えば、妥当性検査レスポンスデータ）の販売事業者識別子に対して（例えば、表430で）記憶されていることを確認するように機能することができる。いくつかの実施形態においては、妥当性検査データと、妥

40

50

当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクは、リンクが自動的に削除される前の限られた時間しか維持できないので、電子デバイス100は、妥当性検査された販売事業者オンラインリソースとの特定のセキュアなデータランザクションを実行するために、当該デバイストラランザクションデータのセキュアデバイスデータを商業エンティティサブシステム400によりセキュアされるようにするため、ステップ510で妥当性検査レスポンスデータを受信し、そして、ステップ514でデバイストラランザクションデータを商業エンティティサブシステム400に送信しなければならない、特定の持続時間を限定されてもよく（例えば、商業エンティティサブシステム400は、特定の時間後に、商業エンティティサブシステム400において妥当性検査データと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、リンクが作成された後10分（又は任意の他の好適な時間）以内に表430からのリンクを除去する）ように機能することができる）、それにより、ランザクションのセキュリティを向上させることができる。追加的に、又は代替的に、ステップ508では、妥当性検査データと、妥当性検査セッション識別子及び販売事業者識別子のうち一方又は両方との間の記憶されたリンクとの関連付けも行われることができ、ステップ506中に（例えば、チャレンジ要求の一部として）販売事業者サブシステム200により商業エンティティサブシステム400に利用可能とされ得る、特定のタイプのセキュアなデータの識別情報などの任意の好適な特定ランザクション情報は、デバイス100と販売事業者サブシステム200との間で共有される（例えば、財務ランザクションの通貨及び金額ならびに決済タイプ（例えば、デバイス100上に供給されたVisa決済クレデンシャルを用いた5米ドル）、健康ランザクションのヘルスケアデータのタイプ及び量（例えば、デバイス100により検出されるか、他の方法により取得された過去3日間にわたる特定のユーザの心拍数データ）など）。また、同様の特定のランザクション情報もまた、ステップ514のデバイストラランザクションデータの一部分として、電子デバイス100により商業エンティティサブシステム400にとって利用可能とさせることができ、それにより、ステップ516は、商業エンティティサブシステム400がステップ514で受信した（例えば、ステップ508で表430に記憶した）妥当性検査データに対して現在記憶されている特定のランザクション情報が、ステップ514で受信した特定のランザクション情報に少なくとも特定の程度類似していることの確認も含むことができ、それによりランザクションのセキュリティを向上させることができる。例えば、ステップ508では、特定の妥当性検査データが、5米ドルの財務ランザクションを示す潜在的ランザクションと関連付けられた特定のランザクション情報に対して記憶されるが、ステップ514で特定の妥当性検査データとともに商業エンティティサブシステム400により受信した特定のランザクション情報が2,000米ドルの財務ランザクションを示している場合、商業エンティティサブシステム400は、\$5と\$2,000との間のずれの大きさが特定の閾値より大きい（例えば、5%超の相違）ことにより、デバイストラランザクションデータの妥当性検査データを妥当性検査しないように機能することができる。したがって、たとえ妥当性検査データと、ステップ514で受信したデバイストラランザクションデータの妥当性検査セッション識別子及び／又は販売事業者識別子が、商業エンティティサブシステム400で（例えば、表430で）アクティブにリンクされていることが確認されても、そのリンクと関連付けられ得る他のデータにデバイストラランザクションデータが適合しない場合（例えば、妥当性検査ステップ506中に識別されたセキュアなデータランザクションの任意の好適な特徴が、ステップ514のデバイストラランザクションデータで識別されたものと適切な量（例えば、財務ランザクション通貨価値の10%超、健康データの概算時間の10%超、健康データのタイプが異なるなど）異なる場合）、妥当性検査データは妥当性検査されなくてもよい。

【0046】

ステップ500のステップ518では、ステップ516でのデバイストラランザクションデータの妥当性検査データの妥当性検査に応じて、商業エンティティサブシステム400

10

20

30

40

50

は更に、セキュアデバイスデータが販売事業者サブシステム200以外の任意の他のエンティティにより受信及び利用され得ないように、販売事業者サブシステム200との共有秘密を用いてデバイスランザクションデータの少なくともセキュアデバイスデータを暗号化することによって、ステップ514で受信したデバイスランザクションデータのセキュアデバイスデータをセキュアとすることができる。例えば、妥当性検査データ及びデバイスランザクションデータの妥当性検査セッション識別子ならびに／又は販売事業者識別子もステップ516で商業エンティティサブシステム400で（例えば、表430で）適正にリンクされていたことを確認することで、デバイスランザクションデータの妥当性検査データの妥当性検査に応じて、商業エンティティサブシステム400は当該リンクを消費する（例えば、商業エンティティサブシステム400で妥当性検査データと妥当性検査セッション識別子及び／又は販売事業者識別子との間のそのような関連付けを除去する（例えば、表430からリンクを除去する））ことができ、そして、デバイスランザクションデータのセキュアデバイスデータを更にセキュアとするためにステップ518に進むことができる。ステップ514のデバイスランザクションデータがいずれかの商業エンティティ鍵で暗号化される場合、商業エンティティサブシステム400は、ステップ518でそのようなデータを解読するように機能することができる（例えば、商業エンティティサブシステム400のサーバ410は、デバイスランザクションデータを受信し、そして、（例えば、商業エンティティサブシステム400のアクセス鍵155a、アクセス鍵155b、CRS151k、CASD158k及び／又はISD鍵156kで）当該デバイスランザクションデータを解読する／その署名を削除することができる）。デバイス100と商業エンティティサブシステム400の両方に既知の商業エンティティ鍵を用いて暗号化／署名された形式でデバイス100と商業エンティティサブシステム400との間でデバイスランザクションデータを通信することによって、プロセス500は、当該デバイスランザクションデータの通信が、商業エンティティ鍵にアクセスできないエンティティにより傍受され使用されるのを禁止することができる。また、ステップ518では、商業エンティティサブシステム400は、デバイスランザクションデータの少なくとも一部分を、販売事業者鍵（例えば、特定のランザクションへの資金供給が行われている販売事業者サブシステム200に関連付けられ得る販売事業者鍵157）で暗号化する、又は他の方法により再フォーマットするように機能することができる。このような販売事業者鍵は、（例えば、ステップ514のデバイスランザクションデータの販売事業者識別子に関連付けられた販売事業者鍵を識別することによって）、商業エンティティサブシステム430により表400を介して決定されてもよく、商業エンティティサブシステム400にとって表430を介してアクセス可能であり得る。販売事業者識別子は、ステップ518では、商業エンティティサブシステム400により受信及び利用され、商業エンティティサブシステム400によりアクセス可能な、多くの販売事業者鍵のうち特定の1つを（例えば、商業エンティティサブシステム400の表430を活用することによって販売事業者鍵157を）識別することができる、そして、商業エンティティサブシステム400は、デバイスランザクションデータの少なくとも一部分（例えば、デバイスランザクションデータの少なくともセキュアデバイスデータ）を暗号化するための当該識別された販売事業者鍵を使用することができる。このようなセキュアデバイスデータをこのような販売事業者鍵（例えば、商業エンティティサブシステム400及び販売事業者サブシステム200に知られ得るが、電子デバイス100又はシステム1の他のサブシステムには知られ得ない鍵）で暗号化することで、このようなセキュアデバイスデータを、別のエンティティに傍受されず、かつ意図しない目的で使用されずに商業エンティティサブシステム400から販売事業者サブシステム200にセキュアに通信できるようにセキュアとすることができる。デバイスランザクションデータの少なくともセキュアデバイスデータを暗号化するために、ステップ518で商業エンティティサブシステム400により利用された販売事業者鍵は、ステップ506での販売事業者オンラインリソースの妥当性検査中にチャレンジデータを暗号化するために商業エンティティサブシステム400により使用された販売事業者鍵（例えば、デバイス100又は商業エンティティサ

10

20

30

40

50

ブシステム400及び販売事業者サブシステム200以外の任意のサブシステムによる使用に利用することができない鍵)と同一とすることができる。したがって、商業エンティティサブシステム400は、セキュアなデータトランザクションに特有の販売事業者妥当性検査セッション中に商業エンティティサブシステム400によって最近妥当性検査された販売事業者オンラインリソースを用いたデバイス100と販売事業者サブシステム200との間のセキュアなデータトランザクションを促進するように機能することができる(例えば、ステップ504及びステップ506の妥当性検査セッションとステップ516及びステップ518のセキュアなデータトランザクションは、同一の妥当性検査セッション識別子を使用することができ、それは、アクティブであるか、他の方法により限られた時間可能とすることができ(例えば、妥当性検査セッション識別子とチャレンジデータとの間のリンク及び/又は妥当性検査セッション識別子と妥当性検査データとの間のリンクは、限られた時間(例えば、30秒と10分の間のような、任意の好適な時間の量)、商業エンティティサブシステム400で妥当であり得る))、それによりトランザクションのセキュリティを向上させることができる)。

10

【0047】

次に、ステップ520では、プロセス500は、商業エンティティサブシステム400がステップ518のセキュアなセキュアデバイスデータをセキュアなトランザクションデータとしてデバイス100に通信することを含むことができる。例えば、デバイストランザクションデータのこのような販売事業者鍵で暗号化されたセキュアデバイスデータを、ステップ520で、セキュアなトランザクションデータの少なくとも一部分として、適切な通信プロトコルを用いた通信経路65を介して商業エンティティサブシステム400からデバイス100に送信してもよい。このようなセキュアなトランザクションデータは、販売事業者鍵で暗号化されたセキュアデバイスデータに加え、トランザクションに関連付けられたステップ502の任意の好適なデータなど、任意の好適なデータを含むことができ、それは、(i) ステップ502の潜在的トランザクションデータを提供した特定の販売事業者サブシステム200を識別し得る販売事業者識別子の識別などの特定の販売事業者情報、(ii) 財務トランザクションの支払いをするのに使用される特定の通貨又は価値の識別などの特定のトランザクション情報、(iii) (例えば、行われているトランザクションと関連付けるために販売事業者サブシステム200により生成された)一意の販売事業者ベースのトランザクション識別子、(iv) (例えば、行われているトランザクションと関連付けるためにデバイス100により生成された)一意のデバイスベーストランザクション識別子、(v) 妥当性検査セッション識別子などを含むが、これらに限定されるものではない。したがって、ステップ520において商業エンティティサブシステム400からデバイス100に通信されたセキュアなトランザクションデータは、ステップ502の潜在的トランザクションデータの一部又は全部、ならびにセキュアなセキュアデバイスデータを含むことができる。

20

30

【0048】

次に、プロセス500のステップ522では、デバイス100は、ステップ520で商業エンティティサブシステム400から通信されたセキュアなトランザクションデータを受信でき、好適な方法でそのセキュアなトランザクションデータを販売事業者サブシステム200と共有することができる。例えば、このようなセキュアなトランザクションデータは、任意の好適な通信プロトコルを用いた通信経路15を介して、及び/又はNFC構成要素120と販売事業者端末220との間の非接触近接型通信として、デバイス100の通信構成要素106から販売事業者サブシステム200のサーバ210に送信されてもよい。ステップ522でデバイス100により販売事業者サブシステム200に(例えば、販売事業者オンラインリソース113(例えば、ステップ502で使用される同一のリソース)を用いて)通信され得るセキュアなトランザクションデータは、ステップ520の販売事業者鍵で暗号化されたセキュアデバイスデータに加えて、トランザクションに関連付けられた任意の好適なデータなどの任意の好適なデータを含むことができ、それは、(i) ステップ502の潜在的トランザクションデータを提供した特定の販売事業者サブ

40

50

システム200を識別し得る販売事業者識別子の識別などの特定の販売事業者情報、(ii) 財務トランザクションの支払いをするのに使用される特定の通貨又は価値の識別などの特定のトランザクション情報、(iii) (例えば、行われているトランザクションと関連付けるために販売事業者サブシステム200により生成された) 一意の販売事業者ベースのトランザクション識別子、(iv) (例えば、行われているトランザクションと関連付けるためにデバイス100により生成された) 一意のデバイスベーストランザクション識別子、(v) 妥当性検査セッション識別子などを含むが、これらに限定されるものではない。したがって、ステップ522で販売事業者サブシステム200と共有されたセキュアなトランザクションデータは、ステップ502の潜在的トランザクションデータの一部又は全部、ならびにステップ518の少なくとも販売事業者鍵で暗号化されたセキュアデバイスデータを含むことができる。ステップ522で、セキュアなトランザクションデータの、販売事業者鍵で暗号化されたセキュアデバイスデータを通信することにより、プロセス500は、ステップ512でデバイス100により生成された、又は他の方法により識別されたセキュアデバイスデータが販売事業者鍵へのアクセスを有しない販売事業者(又はプロセッサ) エンティティ(例えば、販売事業者サブシステム200以外の販売事業者サブシステム又はシステム1の任意の他のサブシステム) により使用されるのを防止しつつ、特定のセキュアなデータトランザクションを促進するため、このような販売事業者鍵で暗号化されたセキュアデバイスデータの販売事業者サブシステム200への通信を可能とすることができる。代替的に、図示されていないが、このようなセキュアなトランザクションデータは、任意の好適な方法(例えば、任意の好適な通信プロトコルを用いた通信経路85を介して)で、ステップ520及びステップ522デバイス100を介せずに、商業エンティティサブシステム400から販売事業者サブシステム200に直接通信することができ、商業エンティティサブシステム400は、ステップ514のデバイストランザクションデータの任意の販売事業者識別子を活用し、ターゲット販売事業者サブシステム200を識別することができる。セキュアなトランザクションデータの、販売事業者鍵で暗号化されたセキュアデバイスデータが販売事業者サブシステム200により受信された後、プロセス500は、販売事業者サブシステム200がその販売事業者鍵で暗号化されたセキュアデバイスデータを好適な目的(例えば、任意の好適なセキュアデバイスデータの処理又は取扱い)で利用することを含むことができる。

【0049】

図5のプロセス500で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。プロセス500の妥当性検査ステップが失敗した場合、そのような失敗は1つ以上の適切なエンティティに通信され得ることを理解されたい。例えば、ステップ506で販売事業者オンラインリソースの妥当性検査が失敗した場合、及び/又はステップ516で妥当性検査データの妥当性検査が失敗した場合、このような失敗は、デバイス100が販売事業者サブシステム200との潜在的トランザクションを解除し、デバイス100から販売事業者オンラインリソースを潜在的に除去することができるように、商業エンティティサブシステム400により電子デバイス100と共有されてもよい。デバイス100のユーザがステップ512でセキュアなデータトランザクションに使用するために特定のセキュアなデータを選択した後、プロセス500の残りのステップは、そのユーザにとって透過的に発生することがある(例えば、ステップ514～522は、デバイス100に対するユーザによる更なる相互作用なしに発生することがあり、デバイス100のユーザにとって瞬時に行われるもののように見えることがある)。プロセス500は、あたかも、ステップ512の後、セキュアデバイスデータが自動でかつ瞬時に販売事業者サブシステム200に送信されるように、デバイス100のユーザに見えることがあり、トランザクションの状況は(例えば、販売事業者サブシステム200及び/又は商業エンティティサブシステム400により) デバイス100に確認されることができる。追加的に、又は代替的に、販売事業者オンラインリソースの妥当性検査は、デバイス100に対して透過的に発生することができる(例えば、ステップ506～5

10

20

30

40

50

10は、また、場合によりステップ504も、デバイス100に対するユーザによる相互作用なしに発生することができ、ステップ502の後デバイス100のユーザに対して瞬時に行われているように見えることがある）。代替的に、いくつかの実施形態では、プロセス500は、デバイス100のユーザにとって全く透過的に発生することができる（例えば、デバイス100は、セキュアなデバイストランザクションがいつ発生すべきかを判定し、妥当性検査レスポンスデータを自動で受信し、かつ／又はデバイストランザクションデータを自動で送信するように、かつ／又は、デバイス100に対するユーザによるアクティブな相互作用なしにセキュアなデバイストランザクションのセキュアなトランザクションデータを自動で受信及び／又は送信するように構成されてもよい。

【0050】

図6の説明

図6は、財務トランザクションを行うためのセキュアデバイス機能へのオンラインアクセスを妥当性検査にするための例示的なプロセス600のフローチャートである。プロセス600は、電子デバイス100、販売事業者サブシステム200、取得銀行サブシステム300、商業エンティティサブシステム400、及び金融機関サブシステム350によって実施されているように示されている。しかし、プロセス600は、他の任意の好適な構成要素又はサブシステムを用いて実施され得ることを理解されたい。プロセス600は、デバイス100からの決済クレデンシャルを用いて販売事業者サブシステム200との間で財務トランザクションを安全かつ効率的に行う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る。図6のプロセス600に従って財務トランザクションを行うためのシステム1の動作に関する以下の議論を容易にするため、図1～図4の解釈図のシステム1の種々の構成要素、及び、そのようなトランザクション中のデバイス100のグラフィカルユーザインタフェース（例えば、販売事業者オンラインリソース113又はデバイス100の任意の好適なアプリケーションによって提供され得るようなGUI）を表し得る図3～図3Dの画面190～190dの正面図が参照される。説明する動作は、幅広い種類のグラフィカル要素及び視覚的方式により実現されてもよい。したがって、図3～図3Dの実施形態は、本明細書で採用するユーザインタ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、幅広い種類のユーザインタフェーススタイルを含んでもよい。プロセス600は、販売事業者サブシステム200による電子デバイス100のセキュア決済機能へのアクセスを可能とするため販売事業者サブシステム200を妥当性検査するコンテキストにおいて少なくとも部分的に記載されているが、プロセス600のすべてではないにしても多くが、任意の好適なサードパーティサブシステムによるデバイス100の任意のセキュア機能（例えば、位置データ、健康データ、他の任意のプライベートデータ、又は、他の有効に妥当性検査されていないサードパーティサブシステムと共有若しくはそのサードパーティサブシステムから受信されるべきではない機能）へのアクセスを可能とするために当該サードパーティサブシステムを妥当性検査するために利用され得ることを理解されたい。

【0051】

プロセス600は、ステップ602で開始することができ、アクセスデータ652（例えば、図1Aのアクセスデータ652）は、商業エンティティサブシステム400によってデバイス100上に供給され得る。例えば、デバイス100が販売事業者サブシステム200とのトランザクションをよりセキュアに行うことを可能とするために、アクセスSSD（例えば、SSD154b）を、アクセスデータ652として、デバイス100のセキュアエレメント145に商業エンティティサブシステム400のサーバ410から供給することができる。上述のように、アクセスSSD154bを、商業エンティティサブシステム400から直接デバイス100のセキュアエレメント145上に少なくとも部分的に供給することができる（例えば、商業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との間の通信経路65を介してアクセスデータ652として供給でき、それは、そして、（例えば、パス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）。経路65を介したアクセスデ

10

20

30

40

50

ータ652は、アクセスSSD154bの少なくとも一部又は全部としてデバイス100のセキュアエレメント145上に供給することができ、アクセスアプレット153b及び／又はアクセス鍵155bを含むことができる。ステップ602は、デバイス100が（例えば、デバイス100がユーザに販売される前に商業エンティティサブシステム400によって）最初に構成されているとき、少なくとも部分的に実行されてもよい。追加的に、又は代替的に、ステップ602は、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、少なくとも部分的に実行されてもよい。追加的に、又は代替的に、アクセスデータ652は、セキュアエレメント145のISD 152用のISD鍵156kを含むことができ、商業エンティティサブシステム400とデバイス100との間のセキュアな送信を可能とするために、アクセス鍵155bに加えて、又はその代替的に使用することができる。追加的に、又は代替的に、アクセスデータ652は、デバイス100のセキュアエレメント145のCRS151のCRS151k及び／又はCASD158のCASD158kを含むことができ、それは、商業エンティティサブシステム400とデバイス100との間のセキュアな送信を可能とするために（例えば、任意の好適な商業エンティティ鍵として、又は商業エンティティサブシステム400とデバイス100との間の共有秘密として使用されるための）アクセス鍵155b及び／又はアクセス鍵155a及び／又はISD156kに加えて、又はその代替的に使用されてもよい。追加的に、又は代替的に、アクセスデータ652は、デバイス100のセキュアエレメントには記憶されなくてよく、プロセッサ102など、デバイス100の他の部分にとって、メモリ104を介してアクセス可能であり得る、任意の他の好適な商業エンティティ鍵又は商業エンティティサブシステム400とデバイス100との間の共有秘密を含むことができる。

【0052】

プロセス600のステップ604では、金融（又は発行者又はトランザクション）機関サブシステム350は、商業エンティティサブシステム400を介して、いくつかの実施形態におけるデバイス100上にクレデンシャルデータ654（例えば、図1Aのクレデンシャルデータ654）を供給することができる。例えば、このようなクレデンシャルデータ654を、少なくとも部分的に、金融機関サブシステム350から直接デバイス100のセキュアエレメント145上に供給することができる（例えば、金融機関サブシステム350とデバイス100との間の図1Aの通信経路75を介して供給することができ、それを通信構成要素106を介してセキュアエレメント145に渡すことができる）。追加的に、又は代替的に、このようなクレデンシャルデータ654を、商業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からデバイス100のセキュアエレメント145に少なくとも部分的に供給することができる（例えば、金融機関サブシステム350と商業エンティティサブシステム400との間の図1Aの通信経路55を介して供給でき、商業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との間の図1Aの通信経路65を介してクレデンシャルデータ654としてデバイス100に渡すことができ、そして、（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）。経路75及び／又は経路65を介したクレデンシャルデータ654は、クレデンシャルSSD154aの少なくとも一部分又は全部としてデバイス100のセキュアエレメント145上に供給でき、クレデンシャル情報161aを有するクレデンシャルアプレット153a及び／又はクレデンシャル鍵155a'及び／又は鍵155akを含むことができる。ステップ604は、デバイス100のユーザがデバイス100に供給される特定のクレデンシャルを選択するときに少なくとも部分的に実行されてもよい。いくつかの実施形態では、クレデンシャルデータ654は、商業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へ最初に提供され得る、及び／又は、商業エンティティサブシステム400によって追加され得る、アクセス鍵155aも含むことができる。いくつかの実施形態では、このようなクレデンシャルデータ654は、供給されている決済クレデンシャルのクレデンシャル情報の少なくとも一部分として主アカウント番号（例えば、アプレット153aのク

10

20

30

40

50

レデンシャル情報161a)、AID(例えば、SSD154aで供給されている決済クレデンシャルのデータのアップレット153a用のAID155aa)、SSD識別子、及び／又はSSDカウンタを含むことができる。

【0053】

デバイス100に供給されるクレデンシャルデータは、金融又は決済クレデンシャルである場合、そのクレデンシャルで決済を行うのに必要なすべてのデータ、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、カード妥当性検査コード(「CVV」))、PAN有効期限、クレデンシャルと関連付けられた名称、ならびに、デバイス100が適切な暗号データ(例えば、任意の好適な共有秘密及び関数出力が少なくとも部分的に共有秘密によって決定され得る任意の好適な暗号アルゴリズム又は暗号)を生成するように動作し得る、その他のデータを含むことができる。「仮想」クレデンシャル又は仮想PAN又はデバイスPAN(「D-PAN」)を、ユーザの「実際の」クレデンシャル又は実際PAN又は資金供給PAN(「F-PAN」)ではなく、デバイス100上に供給することができる。例えば、クレデンシャルがデバイス100に提供されることが決定されると、実際のクレデンシャルの代わりに仮想クレデンシャルが生成され、実際のクレデンシャルにリンクされ、デバイス100に供給されることが(例えば、金融機関サブシステム350によって、商業エンティティサブシステム400によって、及び／又はデバイス100のユーザによって)要求されてもよい。仮想クレデンシャルと実際のクレデンシャルとのこのような作成及びリンク付けは、金融機関サブシステム350の任意の好適な構成要素によって実行され得る。例えば、決済ネットワークサブシステム360(例えば、実際のクレデンシャルのブランドと関連付けられ得る特定の決済ネットワークサブシステム360)は、(例えば、図1Aに示すように)実際のクレデンシャルと仮想クレデンシャルとの間の関連付けを作成し得る仮想リンク付けテーブル312を規定して記憶することができるので、仮想クレデンシャルが(例えば、デバイス100に供給された後の)販売事業者サブシステム200との財務トランザクションのためにデバイス100により利用されるときはいつでも、決済ネットワークサブシステム360は、許可又は妥当性検査要求を受信し、又は他の方法により、(例えば、ステップ638でのデータ688の受信に応じてステップ640で)その仮想クレデンシャルを示す任意の受信したデータを妥当性検査するように試みることができ、表312によって決定される仮想クレデンシャルと関連付けられた実際のクレデンシャルに照らして、この妥当性検査試行要求の分析を行うことができる。代替的に、このような表は、適切な発行銀行サブシステム370又は金融機関サブシステム350によってアクセス可能な任意の他の好適なサブシステムによってアクセス可能及び／又は同様に活用されてもよい。デバイス100に実際のクレデンシャルではなく、仮想のクレデンシャルを供給することにより、金融機関サブシステム350を仮想のクレデンシャルが無許可のユーザにより傍受された場合に生じ得る不正活動を制限するように構成することができる。これは、決済ネットワークサブシステム360は、特定のトランザクション中に、表312を利用して仮想クレデンシャルを実際のクレデンシャルにリンク付ける構成のみ可能とされることによる。

【0054】

プロセス600のステップ606では、商業エンティティサブシステム400は、販売事業者サブシステム200に登録することができる。例えば、プロセス500のステップ501に関して説明するように、ステップ606では、販売事業者サブシステム200の販売事業者オンラインリソース113(例えば、ネイティブアプリ、ドメイン/URL、又は任意の他の好適なウェブリソース、又はおそらく販売事業者端末でも)を、少なくとも1つの特定の販売事業者識別子167及び少なくとも1つの特定の販売事業者鍵157と関連付けることができ、それらのそれぞれを、任意の好適な方法で、販売事業者サブシステム200と商業エンティティサブシステム400の間でセキュアに共有することができる、また、そのような関連付けは、販売事業者オンラインリソース113を商業エンティティサブシステム400に登録できるように(例えば、表430内で)商業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。いくつかの実施形態では

、オンラインリソース決済プログラムに参加するために、販売事業者は、商業エンティティサブシステム400の商業エンティティによって実行されるプログラムのメンバーとして登録すること、及び／又は販売事業者証明書を取得することが必要とされ得る。販売事業者は、証明書又は他の好適な登録証拠なしに決済データを受け取ることができない。このような販売事業者鍵（単数又は複数）及び／又は販売事業者識別子（単数又は複数）がどのように又はどこで生成され、かつ／又は管理されても、販売事業者サブシステム200及び／又は商業エンティティサブシステム400はともに、販売事業者鍵ペアの販売事業者鍵のバージョンを（例えば、販売事業者サブシステム200及び商業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の中で）記憶することができる。これにより、商業エンティティサブシステム400と販売事業者サブシステム200との間でデータをセキュアに通信するための共有秘密を可能とすることができる。いくつかの実施形態において、デバイス100は、デバイス100上の鍵で決済データをセキュアに暗号化するための販売事業者鍵を備えることができる。

10

【0055】

プロセス600のステップ608では、デバイス100は、販売事業者のオンラインリソース658（例えば、（例えば、ステップ606で登録される）図1Aの販売事業者オンラインリソース113）にアクセスすることができる。図1Aに示すように、販売事業者のリソースアプリケーション113を、商業エンティティサブシステム400（例えば、アプリケーションストア420）からデバイス100にロードすることができる。例えば、図3に示すように、デバイス100のユーザは、I/O構成要素114aのタッチスクリーン入力構成要素110fを用いてGUI180の特定の画面190の「Merchant App」アイコン183を選択することができ、この選択を、デバイス100により、販売事業者のサードパーティアプリケーション113（例えば、（例えば、アプリケーションストア420の登録された販売事業者オンラインリソースアプリケーションとして）商業エンティティサブシステム400を介してデバイス100によりアクセスされ得るデバイス100上で少なくとも部分的に実行中のネイティブアプリケーション）と相互作用する能力をユーザに提供するための開始イベントとして認識することができる。追加的に、又は代替的に、このような販売事業者のリソース658は、（例えば、サーバ210又は端末220を介して）販売事業者サブシステム200から直接デバイス100によってアクセスされ得る。このような販売事業者アプリケーションアイコンの選択に応じて、GUIは、デバイス100により、ユーザがアプリケーション113と相互作用する（例えば、購入のために販売事業者から商業的に入手可能なアイテムを閲覧するか、販売事業者又は他の人と共有する特定の健康データ又は位置データを判定する）ことを可能にし得る相互作用型スクリーンを提供することができる。代替的に、ステップ608は、デバイス100が、「Internet」アイコン（例えば、図3のGUI180の特定の画面190のアイコン184）により選択可能とすることができる、デバイス100のインターネットアプリケーション、又は販売事業者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、販売事業者のウェブページ又は他のウェブリソースと相互作用する能力をユーザに提供するウェブ表示を有するハイブリッドアプリケーションを用いて、（例えば、販売事業者サーバ210又は販売事業者エンティティにより少なくとも部分的に制御される任意のサーバを介して）販売事業者サブシステム200から販売事業者のウェブリソースとして販売事業者のリソース658にアクセスすることを含むことができる。代替的に、ステップ608は、アクティブなユーザ入力なしに販売事業者オンラインリソース113としてのリソース658の任意の好適な自動アクセスを含むことができる（例えば、特定の供給を切らしていることを検出する自律型家電製品デバイス100（例えば、洗剤の供給が少ないことを検出したことに応じる洗濯機デバイス100）のように、デバイス100は、任意の好適なイベントの検出に応じてリソース658と自動で相互作用するように機能することができる）。

20

30

40

【0056】

次に、ステップ610では、デバイス100は、（例えば、プロセス500のステップ

50

502に関して説明するように) アクセスされた販売事業者リソースから潜在的トランザクションデータ660を受信することができる。例えば、図1Aに示すように、デバイス100が販売事業者のリソース113(例えば、販売事業者のサードパーティアプリケーション若しくはウェブサイト又は任意の他の好適なオンラインリソース(例えば、リソース658))と相互作用しているときに、潜在的トランザクションデータ660を、販売事業者サブシステム200(例えば、販売事業者サーバ210)からデバイス100に提供してもよい。追加的に、又は代替的に、潜在的トランザクションデータ660の少なくとも一部分は、ステップ610でデータが販売事業者サーバ210からデバイス100にアクティブに送信されるのではなく、(例えば、アプリケーション113がメモリ構成要素に記憶されている、又はデバイス100のプロセッサ102によって実行されている場合) デバイス100に対してローカルなアプリケーション113を介してデバイス100によってローカルにアクセス可能とすることができる。例えば、アプリケーション113をデバイス100に最初に記憶することができると(例えば、販売事業者のリソース658としてステップ608で(例えば、アプリケーションストア420からロードすることができると))、追加情報が販売事業者サブシステム200によりデバイス100に提供されることなく、潜在的トランザクションデータ660の少なくとも一部は、当該最初に記憶されたアプリケーション113により生成されることができる。潜在的トランザクションデータ660は、デバイス100のユーザと販売事業者サブシステム200の販売事業者との間で生じる潜在的財務トランザクションの任意の好適な特性を示す任意の好適なデータを含むことができ、それは、(i)一意の販売事業者識別子(例えば、取得銀行販売事業者識別子及び/又は商業エンティティ販売事業者識別子(例えば、ステップ610で登録され得る販売事業者識別子167))及び/又は使用されている特定の販売事業者リソース(例えば、特定の販売事業者アプリケーション113)の識別情報)など、特定の販売事業者情報、(ii)トランザクションの支払いをするのに使用される特定の通貨(例えば、円、ポンド、ドルなど)の識別及び/又は、トランザクションに支払われる通貨の特定の量の識別、及び/又は、購入もしくはレンタルされる、他の方法により支払いをされる特定の製品又はサービスの識別、及び/又は、使用される既定若しくは初期の配送先住所の識別など、特定のトランザクション情報、(iii)トランザクションのための販売事業者にアクセス可能な1つ以上のタイプの決済方法を示す情報(例えば、購入に使用され得る決済カードのリスト(例えば、Visaではなく、MasterCard))、及び/又は(iv)一意の販売事業者ベースのトランザクション識別子(例えば、行われているトランザクションと関連付けるために販売事業者サブシステム200によりランダムにかつ一意に生成され得る、3文字又は4文字英数字列など、任意の好適なデータ要素)を含むが、これらに限定されない。このような潜在的トランザクションデータ660は、購入を行う顧客の連絡先情報フィールド(例えば、電話番号、電子メールアドレス、送り先住所)など、関連付けられたデータにかかわらず、財務トランザクションを完了するのに必要とされ、又は少なくとも使用され得る任意の好適な数及びタイプのデータフィールドを含むことができ、いくつかのフィールドは、このような潜在的トランザクションデータ660として取り込まれ挿入されることがあり、及び/又はいくつかのフィールドは、このような潜在的トランザクションデータ660の一部としては取り込まれないが、空とされ、プロセス600の間に取り込みを待ち受けてもよい。ステップ610のこのような潜在的トランザクションデータ660は、本明細書では、(例えば、財務トランザクションのための)PKDataRequest又はPKPaymentRequestと呼ばれる場合がある。代替的に、上述のように、販売事業者サブシステム200と関連付けられた潜在的トランザクションデータ660をステップ610でデバイス100にとって利用できるようにさせるために、ユーザはデバイス100とアクティブに相互作用しなくてもよい。

【0057】

セキュアな決済データの通信のために、潜在的トランザクションデータ660は、商品及び/又はサービスの購入のための決済トークンを生成するためのデバイス100に対す

10

20

30

40

50

る販売事業者リソースの要求を含むことができ、例えば、販売事業者の決済処理能力、支払い額及び通貨コードに関する情報を含む潜在的トランザクションに関する任意の好適な情報をカプセル化することができる。潜在的トランザクションデータ660はまた、販売事業者によってサポートされ得る1つ以上の決済ネットワーク（例えば、決済ネットワーク（単数又は複数）360）のリストも含むことができることで、デバイス100は、このようなリスト化された1つ以上の決済ネットワークのいずれかがデバイス100又はクライアントとしてデバイス100にとって利用可能な任意の好適なホストデバイスに対する許可された決済クレデンシャルを有するかを判定するように構成することができる。いくつかの実施形態では、例えば図3Aに示すように、このような潜在的トランザクションデータ660がデバイス100によりアクセスされると、デバイス100のGUIは、画面190aを提供することができ、販売事業者のリソースはトランザクションデータ660を使用してデバイス100のユーザに、潜在的トランザクションと関連付けられた任意の好適な情報、例えば、情報307aで販売事業者の名称（例えば、「販売事業者A」）、情報307bで製品の名称（例えば、「商品B」）、情報307cで価格（例えば、「価格C」）、及び／又は情報307dで初期の配送先データ（例えば、「住所D」）を示すことができる。販売事業者サブシステム200によりデバイス100に提供され得る潜在的トランザクションデータ660は、このような情報307a、307b、307c及び／又は307dを示すことができる。デバイス100のユーザは、デバイス100及び画面190aと相互作用して、そのような情報（例えば、配送先住所など）の特定の部分を調整することができ、それは、（例えば、ステップ610の別のインスタンスで）更新された潜在的トランザクションデータが販売事業者サブシステム200により生成又は共有されることを必要とし得る。図3Aに示すように、かつ以下により詳細に説明するように、画面190aには、セキュアな支払いプロンプト309も含まれていてもよい。潜在的トランザクションデータ660の少なくとも一部分を、図1Aの通信経路15を介して販売事業者サブシステム200からデバイス100に提供することができ、デバイス100の通信構成要素106により受信することができる。通信構成要素106は、この潜在的トランザクションデータ660を、（例えば、（例えば、情報307a～307d及び309のために）デバイス100上のユーザインタフェースの一部としての画面190a上に表示するための）プロセッサ102及び／又はセキュアエレメント145に渡すことができる。例えば、セキュアエレメント145は、デバイス100と販売事業者サブシステム200との間の財務トランザクションをセキュアに可能とするために、そのような潜在的トランザクションデータ660の少なくとも一部分を利用することができる。いくつかの実施形態では、潜在的トランザクションデータ660は、販売事業者決済要求データ及び／又はユニフォームリソースロケータ（「URL」）又は任意の他の好適な参照文字列及び／又はクエリ文字列と呼ばれる場合がある。

【0058】

プロセス600のステップ612では、販売事業者オンラインリソース妥当性検査セッションを開始することができる。プロセス500のステップ504に関して上述したように、ステップ612は、電子デバイス100がセキュアなデータトランザクション（例えば、ステップ610の潜在的トランザクションデータ660により識別されたセキュアなデータトランザクション（例えば、財務トランザクション））が発生すべきことを示したことに応じて生じることがある。このような指示は、ステップ610の販売事業者オンラインリソースの潜在的トランザクションデータ660によって識別されるセキュアなデータトランザクションを行うユーザの意図を伝えるために、デバイス100のユーザが図3Aのセキュアな支払いプロンプト309などの販売事業者オンラインリソースのGUI要素（例えば無線ボタン）を選択することに応じて生じ得る。代替的に、このような指示は、好適な要件が満たされていることに基づいて（例えば、ステップ610の潜在的トランザクションデータ660がデバイス100に通信されていることに単純に応じて）自動的に生じてよい。例えば、この指示が発生したとき、販売事業者オンラインリソース113（例えば、ウェブリソース用のウェブキット）は、カード管理アプリケーション103

10

20

30

40

50

b（例えば、決済用のセキュアなデータトランザクションのパスキット）にセキュアなデータトランザクション要求を送信するように動作するようにしてもよいし、デバイス100（例えば、カード管理アプリケーション103b又はデバイス100の他の好適なアプリケーション）は、このようなセキュアなデータトランザクション要求を受信かつ処理するように動作し、そして、ステップ612で販売事業者オンラインリソース妥当性検査セッション開始データ662を生成し、販売事業者サブシステム200に通信するように動作するようにしてもよい。

【0059】

ステップ612では、実行される特定のセキュアなデータトランザクション（例えば、図3Aのデータ660及び／又は画面190aにより識別された財務トランザクション）に対する販売事業者オンラインリソース妥当性検査セッションを開始するための販売事業者オンラインリソース妥当性検査セッション開始データ662として、任意の好適なデータを、電子デバイス100により生成し、かつ／又は販売事業者サブシステム200に通信することができる。例えば、妥当性検査セッション識別子はデバイス100により生成され、ステップ612で販売事業者オンラインリソース妥当性検査セッション開始データ662の一部分として販売事業者サブシステム200に通信されてもよく、このような妥当性検査セッション識別子は、任意の好適な英数字列又は、開始されている現在の販売事業者オンラインリソース妥当性検査セッションを一意に識別し得る（例えば、少なくとも特定の期間に、販売事業者サブシステム200及び／又は商業エンティティサブシステム400に対してそのようなセッションを一意に識別する）任意の他の好適な識別子とすることができる。追加的に、又は代替的に、ステップ612では、販売事業者オンラインリソース妥当性検査セッション開始データ662の少なくとも一部分として、チャレンジ要求ターゲット識別子（例えば、チャレンジ要求URL）を、デバイス100から販売事業者サブシステム200に通信することができ、このようなチャレンジ要求ターゲット識別子は、販売事業者サブシステム200が、販売事業者を妥当性検査するために通信することとなるエンティティを識別することができる（例えば、実行される特定のセキュアなデータトランザクションの販売事業者オンラインリソースを妥当性検査するために、販売事業者サブシステム200と協働することとなる商業エンティティサブシステム400のサーバ410を識別するURL）。デバイスアプリケーション（例えば、カード管理アプリケーション103b）は、商業エンティティサブシステム400により制御され得る任意の好適なオペレーティングシステム又はアプリケーション更新の一部としてプログラミングされたこのようなチャレンジ要求ターゲット識別子を有することができるので、チャレンジ要求ターゲット識別子は、デバイス100上で、任意の好適な時間に商業エンティティサブシステム400により更新することができる。追加的に、又は代替的に、このような販売事業者オンラインリソース妥当性検査セッション開始データ662は、自身を妥当性検査する販売事業者及び／又はステップ608でアクセスされ、ステップ610で潜在的トランザクションデータ660を受信するために利用された特定の販売事業者オンラインリソースへの要求を示す任意の好適なデータ、デバイス100を示す任意の好適なデータ（例えば、デバイス識別子119）、及び／又は実行される特定のセキュアなデータトランザクションを示す任意の好適なデータ（例えば、特定の販売事業者情報（例えば、販売事業者オンラインリソースの販売事業者識別子167）、特定のトランザクション情報（例えば、財務トランザクションの通貨及び金額ならびに決済タイプ）などのステップ610の潜在的トランザクションデータ660からの任意の好適なデータ）、及び／又は一意の販売事業者ベースのトランザクション識別子などの、他の任意の好適なデータを含むことができる。任意の好適な販売事業者オンラインリソース妥当性検査セッション開始データ662を、ステップ612で、任意の好適な方法で、デバイス100によって販売事業者サブシステム200に通信することができる（例えば、このような販売事業者オンラインリソース妥当性検査セッション開始データ662を、任意の好適な通信プロトコルを用いた通信経路15を介して、又は任意の好適な通信プロトコルを用いた、端末220とNFC構成要素120との間の非接触近接型通信チャネルを介してデバイス100の通信

10

20

30

40

50

構成要素１０６から販売事業者サブシステム２００のサーバ２１０に送信することができる）。

【００６０】

ステップ６００でプロセス６１４では、販売事業者サブシステム２００が、販売事業者オンラインリソース１１３の妥当性検査セッションを開始するため、ステップ６１２でデバイス１００からいずれかの好適な販売事業者オンラインリソース妥当性検査セッション開始データ６６２を受信したことに応じて、販売事業者サブシステム２００は、実行される特定のセキュアなデータランザクション（例えば、ステップ６１０及び／又はステップ６１２で識別された金融決済ランザクション）のための販売事業者オンラインリソースを妥当性検査するために、任意の好適なチャレンジ要求データ６６４を商業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る。ステップ６１４で販売事業者サブシステム２００から商業エンティティサブシステム４００に通信されるチャレンジ要求データ６６４は、販売事業者サブシステム２００（例えば、販売事業者リソース１１３）の妥当性を商業エンティティサブシステム４００に証明しようとするための任意の好適なデータを含むことができ、それは、妥当性検査される販売事業者オンラインリソースと関連付けられた販売事業者識別子（例えば、販売事業者オンラインウェブリソースのドメインであり得るステップ６０６で登録された少なくとも１つの販売事業者識別子１６７）、（例えば、ステップ５０４でデバイス１００により、又はステップ５０６で販売事業者サブシステム２００により生成された）妥当性検査セッション識別子及び／又は任意の他の好適なデータ（例えば、デバイス１００を識別するデータ及び／又は実行される特定のセキュアなデータランザクションを識別するデータ）を含むことができるが、これらに限定されない。例えば、チャレンジ要求データ６６４の販売事業者識別子は、現在の販売事業者オンラインリソース妥当性検査セッションを開始したステップ６１０で使用される販売事業者オンラインリソースに関連付けられた任意の好適な販売事業者識別子１６７とすることができる。ステップ６１２の販売事業者オンラインリソース妥当性検査セッション開始データ６６２が、（例えばデバイス１００によって生成される）妥当性検査セッション識別子を含む場合、当該妥当性検査セッション識別子を、ステップ６１４でチャレンジ要求データ６６４の少なくとも一部分として販売事業者サブシステムにより提供することができる。しかし、ステップ６１２の販売事業者オンラインリソース妥当性検査セッション開始データ６６２が妥当性検査セッション識別子を含んでいない場合、又は販売事業者オンラインリソース妥当性検査セッションを、販売事業者サブシステム２００により自動で（例えば、ステップ６１０の潜在的ランザクションデータ６６０の通信に応じて）、かつステップ６１２の販売事業者オンラインリソース妥当性検査セッション開始データ６６２に応じずに開始することができる場合、販売事業者サブシステム２００は、開始されている現在の販売事業者オンラインリソース妥当性検査セッションを一意に識別し得るそのような妥当性検査セッション識別子を生成するように機能することができ、そして、ステップ６１４でチャレンジ要求データ６６４の少なくとも一部分としてその妥当性検査セッション識別子を含むように動作することができる。いくつかの実施形態では、実行される特定のセキュアなデータランザクション（例えば、ステップ６１０及び／又はステップ６１２で識別される金融決済ランザクション）に特有であり得る任意の好適な追加情報が、ステップ６１４でチャレンジ要求データ６６４の少なくとも一部分として提供され得、それは、潜在的ランザクションデータの情報３０７ｂの「製品Ｂ」、潜在的ランザクションデータの情報３０７ｃの「価格Ｃ」、潜在的ランザクションデータの情報３０７ｄの配送先データ「宛先Ｄ」、潜在的ランザクションデータの決済クレデンシャル識別「クレデンシャルＸ」情報３１３を示す情報及び／又は、（例えば、データのいずれかについての任意のプライバシーに対する懸念に照らして）実行されるセキュアなデータランザクションが健康データランザクションである場合、実際の心拍数情報ではなく、「過去３日間の心拍数情報」のような、商業エンティティサブシステム４００と共有するのに適切であり得る実行されるセキュアなデータランザクションに関連付けられた任意の他の好適な情報を含むが、これらに限定されない。本明細書では潜在的ラン

10

20

30

40

50

ザクション識別情報と呼ばれ得るセキュアなデータトランザクションに特定のもので特有であり得るこのような情報は、セキュリティの追加層（単数又は複数）を現在のデータトランザクションプロセスに提供し、及び／又は将来のデータトランザクションに対する追加のセキュリティ（例えば、不正検出）サービスを提供するためのプロセス600の好適な部分の間に使用され得る。チャレンジ要求データ664は、販売事業者サブシステム200により（例えば、HTTPヘッダにおいて、又は別の方法で）販売事業者サブシステム200にとって利用可能で、かつチャレンジ要求の販売事業者識別子に関連付けられた販売事業者鍵（例えば、（例えば、販売事業者オンラインリソース113を妥当性検査するために）ステップ606において販売事業者識別子167で登録された販売事業者鍵157）で署名することができ、それにより、チャレンジ要求データ664を、販売事業者オンラインリソース113を妥当性検査するために商業エンティティサブシステム400により効率的に利用することができる。ステップ614では、任意の好適なチャレンジ要求データ664を、適切な方法で販売事業者サブシステム200により商業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、このようなチャレンジ要求データ664を、好適な通信プロトコルを用いた通信経路85を介して販売事業者サブシステム200のサーバ210から商業エンティティサブシステム400のサーバ410に送信することができる）。このようなチャレンジ要求データ664の通信は、販売事業者オンラインリソース妥当性検査セッション開始データ662の少なくとも一部分として、ステップ612でデバイス100から販売事業者サブシステム200に通信され得るチャレンジ要求ターゲット識別子（例えば、チャレンジ要求URL）に基づいて商業エンティティサブシステム400に適切にアドレス指定され得る。追加的に、又は代替的に、このようなチャレンジ要求データ664の通信は、販売事業者サブシステム200にとって利用可能とすることができ、かつステップ610の潜在的トランザクションデータ660と関連付けられ得るチャレンジ要求ターゲット識別子（例えば、チャレンジ要求URL）に基づいて商業エンティティサブシステム400に適切にアドレス指定され得る（例えば、商業エンティティサブシステム400を識別する識別子を、任意のコード（例えば、ウェブリソース用のJava（登録商標）スクリプトコード）と関連付けることができ、又は他の方法により、販売事業者オンラインリソース内に任意の好適な「セキュアなトランザクション」プロンプト（例えば、図3Aのセキュアな支払いプロンプト309）を提供するために、販売事業者サブシステム200にとって利用可能とさせることができる）。

【0061】

プロセス600のステップ616では、商業エンティティサブシステム400がステップ614で販売事業者サブシステム200から好適なチャレンジ要求データ664を受信したことに応じて、商業エンティティサブシステム400は、チャレンジ要求の販売事業者識別子167によって識別される販売事業者オンラインリソース113を妥当性検査するように機能することができる。例えば、ステップ616では、商業エンティティサブシステム400は、受信したチャレンジ要求データ664の販売事業者識別子167により識別された販売事業者オンラインリソース113が商業エンティティサブシステム400において妥当で、かつ登録された販売事業者オンラインリソースであることの確認を試みるように機能することができ、それは、（例えば、（例えば、ステップ606で）販売事業者識別子167が商業エンティティサブシステム400に登録されており、かつそのような登録が依然として妥当であること（例えば、商業エンティティサブシステム400が表430から販売事業者識別子167を除去しておらず、又は疑わしいか、又は他の理由で、もはや信頼されていないとして表430内のその販売事業者識別子167にフラグをたてていないこと、及び／又は（例えば、表430内の）販売事業者識別子167と関連付けられた証明書が依然として妥当であること）を判定するため）表430内のその販売事業者識別子167を識別することによって、及び／又は、その販売事業者識別子167と関連付けられ、又はそれにより識別されたドメインを識別し、（例えば、ステップ501及び／又はステップ606に関して説明するように）そのドメイン上にホストされ得るファイルを再検証することでそのドメインを再検証することによって、確認することがで

き、そのような再検証を、代替的に又は追加的に、必ずしもデータ664の受信に応じたステップ616ではなく、任意の好適な時（例えば、定期的に又は別の方法で）に商業エンティティサブシステム400により実行することができる。追加的に、又は代替的に、ステップ616では、商業エンティティサブシステム400は、受信したチャレンジ要求データ664の署名の妥当性検査を試みるよう動作することができ、それは、表430内、又はその他商業エンティティサブシステム400内における受信したチャレンジ要求データ664の販売事業者識別子167と関連付けられ得る販売事業者鍵157（例えば、ステップ606の登録の間に行われていることがある関連付け）を識別し、そして、受信したチャレンジ要求データ664の署名を妥当性検査するために（例えば、商業エンティティサブシステム400にとってアクセス可能な販売事業者鍵157が、ステップ614でチャレンジ要求データ664を商業エンティティサブシステム400に通信する前にチャレンジ要求データ664に署名するために販売事業者サブシステム200により使用されていた、販売事業者サブシステム200にとってアクセス可能な販売事業者鍵157とともに設定されたペアの鍵（例えば、鍵のうち一方を公開鍵とすることができ、他方をペアの鍵セットの秘密鍵とすることができ）のうちの1つであることを確認するため）、その識別された販売事業者鍵157を利用することによって行うことができ、それは、プロセス600の後半部（単数又は複数）で（例えば、販売事業者サブシステム200が商業エンティティサブシステム400により事前に暗号化されたデータを解読し得るステップ636で）販売事業者サブシステム200の使用に必要とされ得る販売事業者サブシステム200による販売事業者鍵157の所持を確実にすることができる。商業エンティティサブシステム400による受信したチャレンジ要求データ664の好適な妥当性検査後（例えば、受信したチャレンジ要求データ664の販売事業者識別子及び／又は署名の妥当性検査後）、商業エンティティサブシステム400はまた、ステップ616で、好適なチャレンジデータを生成し、受信したチャレンジ要求データ664の好適な識別子データに対してそのチャレンジデータを記憶するように機能することができる。例えば、受信したチャレンジ要求データ664の好適な妥当性検査後、商業エンティティサブシステム400は、好適なチャレンジデータ（例えば、エントローピーを介した好適なランダムデータ）を生成し、そして、商業エンティティサブシステム400にとってアクセス可能な任意のデータ構造で（例えば、表430で、又は別の方法で）、チャレンジ要求データ664の妥当性検査セッション識別子及びチャレンジ要求データ664の販売事業者識別子の一方又は両方に対してそのチャレンジデータを記憶するように機能することができる。妥当性検査セッションのこのようなチャレンジデータと識別子データ（例えば、妥当性検査セッション識別子及び／又はチャレンジ要求データ664の販売事業者識別子）との間の記憶されたリンク又は関連付けは、（例えば、ステップ622で）妥当性検査セッションの販売事業者オンラインリソースを更に妥当性検査するために、かつ／又は（例えば、ステップ630で）実行されるセキュアなデータトランザクションを更にセキュアとするために、商業エンティティサブシステム400により、後で使用され得る。また、いくつかの実施形態では、チャレンジ要求データ664の潜在的トランザクション識別情報のいずれか又はすべてが、チャレンジデータ及び識別子データに対して記憶され、又は他の方法によりそれらと関連付けられてもよい。

【0062】

プロセス600のステップ618では、商業エンティティサブシステム400が受信したチャレンジ要求データ664を妥当性検査し、ステップ616で妥当性検査セッションの識別子データに対してチャレンジデータを生成したことに応じて、商業エンティティサブシステム400は、任意の好適な鍵又は別の方法を用いてステップ616のチャレンジデータを暗号化するように機能することができ、そして、任意の他の好適なデータとともにその暗号化されたチャレンジデータを、チャレンジングデータ668として販売事業者サブシステム200に通信するように機能することができる。例えば、商業エンティティサブシステム400は、商業エンティティサブシステム400にとってアクセス可能で、（例えば、表430内の、又は、その他商業エンティティサブシステム400内における

(例えば、ステップ606の登録の間に行われた関連付け)受信したチャレンジ要求データ664の販売事業者識別子167に関連付けられ得る任意の好適な販売事業者鍵157を用いてチャレンジデータを暗号化することができ、ステップ618でのチャレンジデータの暗号化のため商業エンティティサブシステム400により使用されるそのような販売事業者鍵157は、ステップ616でチャレンジ要求データ664を妥当性検査するために、商業エンティティサブシステム400により使用された販売事業者鍵157と同一であってもよいし、又は販売事業者鍵157とは異なる販売事業者鍵157であってもよい。このような暗号化されたチャレンジデータに加えて、任意の他の好適なデータを、ステップ618で商業エンティティサブシステム400により販売事業者サブシステム200に通信されるチャレンジングデータ668の一部分として含むことができ、それは、
10 複数の登録された販売事業者オンラインリソース及び／又は複数の販売事業者鍵を有し得る販売事業者を支援するために提供され得る、チャレンジデータを暗号化するために商業エンティティサブシステム400により使用される販売事業者鍵157のハッシュ(例えば、適当な販売事業者鍵157(例えば、チャレンジデータを解読するための販売事業者サブシステム200の秘密鍵157)を識別するために販売事業者サブシステム200により受信及び使用され得る表430の公開販売事業者鍵157のハッシュバージョン)、
20 チャレンジ要求データ664の妥当性検査セッション識別子、チャレンジ要求データ664の販売事業者識別子、チャレンジデータの暗号化のために商業エンティティサブシステム400により使用される販売事業者鍵157と商業エンティティサブシステム400において(例えば、表430で)関連付けられた販売事業者識別子などを含むが、これらに
限定されない。好適なチャレンジングデータ668を、ステップ618で任意の好適な方法で商業エンティティサブシステム400により販売事業者サブシステム200に通信することができる(例えば、このようなチャレンジングデータ668を、好適な通信プロトコルを用いた通信経路85を介して商業エンティティサブシステム400のサーバ410から販売事業者サブシステム200のサーバ210に送信することができる)。

【0063】

プロセス600のステップ620では、販売事業者サブシステム200がステップ618でそのようなチャレンジングデータ668を受信したことに応じて、販売事業者サブシステム200は、受信したチャレンジングデータ668を処理し、そして、現在の妥当性検査セッション中に販売事業者サブシステム200を更に妥当性検査するためにチャレン
30 ジレスポンスデータ670を生成し、商業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る。例えば、ステップ620では、販売事業者サブシステム200は、販売事業者サブシステム200にとって利用可能な任意の好適な販売事業者鍵157(例えば、(例えば、現在の妥当性検査セッション中に妥当性検査されている販売事業者オンラインリソース113のための)ステップ606で販売事業者識別子167に登録された販売事業者鍵157)を用いて、受信したチャレンジングデータ668の暗号化されたチャレンジデータを解読するように機能することができる。ステップ620での暗号化されたチャレンジデータの解読のために販売事業者サブシステム200により使用される
40 このような販売事業者鍵157は、(例えば、データ664及びデータ668の共通のセッション識別子と関連付けられ得るように)チャレンジングデータ668の任意のハッシュ鍵情報を用いて、及び／又は、チャレンジングデータ668の販売事業者識別子を用いて、及び／又は、チャレンジ要求データ664の販売事業者識別子を用いて販売事業者サブシステム200により識別され得る。ステップ620での暗号化されたチャレンジデータの解読のために販売事業者サブシステム200により使用されるこのような販売事業者鍵157は、ステップ614でチャレンジ要求データ664に署名するのに販売事業者サブシステム200により使用された販売事業者鍵157と同一であってもよいし、又は販売事業者鍵157とは異なる販売事業者鍵157であってもよい。受信したチャレンジングデータ668の暗号化されたチャレンジデータを解読した後、販売事業者サブシステム200はまた、ステップ620でチャレンジレスポンスデータ670を生成し、それを
50 販売事業者サブシステム200から商業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、チャレンジレスポンスデータ670は、他の任意の好適なデータとともに商業エンティティサブシステム400に対して販売事業者サブシステム200（例えば、販売事業者リソース113）の妥当性を更に証明しようとするために販売事業者サブシステム200により解読されるチャレンジデータを含むことができ、この他の任意の好適なデータは、現在の妥当性検査セッションの妥当性検査セッション識別子（例えば、チャレンジ要求データ664及び／又は受信したチャレンジングデータ668の妥当性セッション識別子）、現在の妥当性検査セッションによって妥当性検査されている販売事業者オンラインリソースと関連付けられた販売事業者識別子（例えば、チャレンジ要求データ664の販売事業者識別子、チャレンジデータの暗号化のために商業エンティティサブシステム400により使用される販売事業者鍵157と商業エンティティサブシステム400で（例えば、表430で）関連付けられた販売事業者識別子など）、ステップ614のチャレンジ要求データ664に含まれてもよいし、含まれなくてもよいセキュアなデータトランザクションが実行されるための任意の好適な潜在的トランザクション識別情報のいずれか、又はすべてを含むが、これらに限定されない。チャレンジレスポンスデータ670を、販売事業者サブシステム200により（例えば、HTTPヘッダで、又は別の方法で）、販売事業者サブシステム200にとって利用可能な販売事業者鍵（例えば、（例えば、現在妥当性検査されている販売事業者オンラインリソース113のための）販売事業者識別子167にステップ606で登録される販売事業者鍵157）で署名することができ、それにより、販売事業者オンラインリソース113を更に妥当性検査するために、チャレンジレスポンスデータ670を、商業エンティティサブシステム400により効率的に利用することができる。ステップ620でチャレンジレスポンスデータ670に署名するために販売事業者サブシステム200によって使用され得るこのような販売事業者鍵157は、ステップ614でチャレンジ要求データ664に署名するために販売事業者サブシステム200によって使用され得る販売事業者鍵157と同一の販売事業者鍵157であってもよいし、又は異なる販売事業者鍵157であってもよい。追加的に、又は代替的に、ステップ620でチャレンジレスポンスデータ670に署名するために販売事業者サブシステム200によって使用され得るこのような販売事業者鍵157は、ステップ620で暗号化されたチャレンジデータを解読するために販売事業者サブシステム200によって使用され得る販売事業者鍵157と同一の販売事業者鍵157であってもよいし、又は異なる販売事業者鍵157であってもよい。ステップ620では、任意の好適なチャレンジレスポンスデータ670を、適切な方法で販売事業者サブシステム200により商業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、このようなチャレンジレスポンスデータ670を、好適な通信プロトコルを用いた通信経路85を介して販売事業者サブシステム200のサーバ210から商業エンティティサブシステム400のサーバ410に送信することができる）。

【0064】

プロセス600のステップ622では、商業エンティティサブシステム400がステップ620で販売事業者サブシステム200から好適なチャレンジレスポンスデータ670を受信したことに応じて、商業エンティティサブシステム400は、現在の妥当性検査セッションで更なる販売事業者サブシステム200及び対象となるその販売事業者オンラインリソースを妥当性検査するように機能することができる。例えば、ステップ622では、商業エンティティサブシステム400は、受信したチャレンジレスポンスデータ670の署名の妥当性検査を試みようとして動作することができ、それは、表430内の受信したチャレンジレスポンスデータ670の妥当性検査セッション識別子と関連付けられ得る、かつ表430内の、又は商業エンティティサブシステム400における別の方法（例えば、ステップ606の登録の間に行われていることがある関連付け）の、受信したチャレンジレスポンスデータ670の販売事業者識別子167と関連付けられ得る販売事業者鍵157を識別し、そして、受信したチャレンジ要求データ670の署名を妥当性検査するために（例えば、商業エンティティサブシステム400にとってアクセス可能な販売事業者鍵157が、ステップ620でチャレンジレスポンスデータ670を商業エンティティサブ

10

20

30

40

50

システム４００に通信する前にチャレンジレスポンスデータ６７０に署名するために販売事業者サブシステム２００により使用されていた、販売事業者サブシステム２００にとってアクセス可能な販売事業者鍵１５７とともに設定されたペアの鍵（例えば、鍵のうち一方を公開鍵とすることができ、他方をペアの鍵セットの秘密鍵とすることができる）のうちの１つであることを確認するため）、その識別された販売事業者鍵１５７を利用することによって行うことができる。ステップ６２２でチャレンジレスポンスデータ６７０の署名を妥当性検査するために商業エンティティサブシステム４００により使用され得る、そのような販売事業者鍵１５７は、ステップ６１６でチャレンジレスポンスデータ６６４の署名を妥当性検査するために商業エンティティサブシステム４００によって使用され得る販売事業者鍵１５７と同一の販売事業者鍵１５７であってもよいし、又はそれとは異なる販売事業者鍵１５７であってもよく、及び／又は、ステップ６２２でチャレンジレスポンスデータ６７０の署名を妥当性検査するために商業エンティティサブシステム４００によって使用され得る、そのような販売事業者鍵１５７は、ステップ６１８でチャレンジデータを暗号化するために商業エンティティサブシステム４００によって使用され得る販売事業者鍵１５７と同一の販売事業者鍵１５７であってもよいし、又はそれとは異なる販売事業者鍵１５７であってもよい。追加的に、又は代替的に、ステップ６２２では、商業エンティティサブシステム４００は、受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータが妥当なチャレンジデータであることの確認を試みるように機能することができる。例えば、商業エンティティサブシステム４００は、受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータが現在記憶されているか、又は他の方法により、商業エンティティサブシステム４００にとって独立して（例えば、表４３０で）アクセス可能であることを確認しようとするように機能することができる。いくつかの実施形態では、商業エンティティサブシステム４００は、同一のチャレンジデータが表４３０に現在記憶されていることを識別することによって、受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータの妥当性を判定することができる。代替的に、商業エンティティサブシステム４００は、ステップ６１６で表４３０に記憶されているような、受信したチャレンジレスポンスデータ６７０の任意の好適な識別子データに対して（例えば、妥当性検査セッション識別子又は販売事業者識別子に対して）同一のチャレンジデータが現在表４３０に記憶されていることを識別することによって、受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータの妥当性を判定することができる。いくつかの実施形態において、チャレンジデータと妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクを、又はこのような記憶されたチャレンジデータ自体を、商業エンティティサブシステム４００は、リンク又は記憶されたデータが自動で削除される前の限られた時間量の間だけしか維持できないので、販売事業者サブシステム２００は、チャレンジングデータ６６８を受信し、その後、特定の妥当性検査セッションのための販売事業者オンラインリソースを妥当性検査するために、適切なチャレンジレスポンスデータ６７０を商業エンティティサブシステム４００に送信しなければならない特定の持続時間に限定されることがある（例えば、商業エンティティサブシステム４００は、特定時間後の商業エンティティサブシステム４００におけるチャレンジデータと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、リンク又はチャレンジデータが作成された後１０分以内に表４３０からリンク又はチャレンジデータを除去する）ように動作することができ、それにより、トランザクションのセキュリティを向上させることができる）。したがって、（例えば、ステップ６０８で登録するように）商業エンティティサブシステム４００における販売事業者鍵と販売事業者識別子との１つ以上の関連付けを用いて、（例えば、ステップ６１０及び／又はステップ６１２で識別されるように）実行される特定のセキュアなデータトランザクションのステップ６１４～ステップ６２２のいずれか又はすべてにおける販売事業者オンラインリソースの妥当性検査を完了することができる。

【００６５】

商業エンティティサブシステム４００による受信したチャレンジレスポンスデータ６７

10

20

30

40

50

0の好適な妥当性検査後（例えば、受信したチャレンジレスポンスデータ670の署名の妥当性検査後及び／又は受信したチャレンジレスポンスデータ670の解読済のチャレンジデータの妥当性検査後）、商業エンティティサブシステム400はまた、ステップ622で、好適な妥当性検査データを生成し、受信したチャレンジ要求データ664及び／又は受信したチャレンジレスポンスデータ670の好適な識別子データに対してその妥当性検査データを記憶するように機能することができる。例えば、受信したチャレンジ要求データ664及び／又は受信したチャレンジレスポンスデータ670の好適な妥当性検査後、商業エンティティサブシステム400は、好適な妥当性検査データ（例えば、エントロピーを介した任意の好適なランダムデータ及び／又は任意の好適な暗号ナンス）を生成し、そして、商業エンティティサブシステム400にとってアクセス可能な任意のデータ構造で（例えば、表430で、又は別の方法で）、チャレンジ要求データ664及びチャレンジレスポンスデータ670の妥当性検査セッション識別子及び販売事業者識別子の一方又は両方に対してその妥当性検査データを記憶するように機能することができる。妥当性検査セッションのこのような妥当性検査データと識別子データ（例えば、妥当性検査セッション識別子ならびに／又はチャレンジ要求データ664及び／若しくはチャレンジレスポンスデータ670の販売事業者識別子）との間の記憶されたリンク又は関連付けは、（例えば、ステップ630で）実行されるセキュアなデータトランザクションを更にセキュアとするために、商業エンティティサブシステム400により、後で使用され得る。また、いくつかの実施形態では、チャレンジ要求データ664及び／又はチャレンジレスポンスデータ670の潜在的トランザクション識別情報のいずれか又はすべてが、妥当性検査データ及び識別子データに対して記憶され、又は他の方法によりそれらと関連付けられてもよい。

【0066】

商業エンティティサブシステム400において（例えば、表430内で）、受領したチャレンジレスポンスデータ670が復号されたチャレンジデータを、チャレンジデータが識別子情報（妥当性検査セッション識別子及び／又は販売事業者識別子）にリンクされていることの確認によって妥当性検査したことに応じて、商業エンティティサブシステム400は、ステップ622においてそのリンクを消費し（例えば、チャレンジデータと商業エンティティサブシステム400での妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、表430からリンクを除去する））、妥当性検査データ（例えば、任意の好適なランダムデータ（例えば、暗号ナンス（例えば、エントロピーを介した任意の好適なランダムデータ）））を生成し、そして、妥当性検査データを任意の好適な識別子情報（例えば、例えば、チャレンジ要求及び／若しくはチャレンジレスポンスの妥当性検査セッション識別子、かつ／又はチャレンジ要求及び／若しくはチャレンジレスポンスの販売事業者識別子に対する）に対し、又は他の方法によりそれに関連付けて、商業エンティティサブシステム400において（例えば、表430又は別の方法などの任意の好適なデータ構造で）記憶することができる。代替的に、商業エンティティサブシステム400（例えば、表430内）において、チャレンジデータが識別子情報（例えば、妥当性検査セッション識別子及び／又は販売事業者識別子情報）にリンクされていることを確認することによって、受信したチャレンジレスポンスデータ670の解読済のチャレンジデータの妥当性検査に応じて、商業エンティティサブシステム400は、ステップ622で、そのリンクを維持するか、又は他の方法により商業エンティティサブシステム400（例えば、表430内）でそのリンクを更新し（例えば、そのリンクと関連付けられ得るタイマーをリセットするか、又はそのリンクと関連付けるために任意の追加潜在的トランザクション識別情報を追加する）、そして、（例えば、ステップ616で生成された）そのリンクのチャレンジデータを、ステップ622で本来生成され得る妥当性検査データとして利用するように機能することができる。いくつかの実施形態では、ステップ618～ステップ622でのチャレンジデータの使用は、ステップ624～ステップ630での妥当性検査データの使用とは異なり得るため、チャレンジデータと妥当性検査データはサイズ又は任意の他の好適なプロパティ（単数又は複数）に関

10

20

30

40

50

して、異なっているもよい。

【0067】

プロセス600のステップ624では、商業エンティティサブシステム400が受信したチャレンジ要求データ664を妥当性検査し、及び／又は受信したチャレンジレスポンスデータ670を妥当性検査し、ステップ622で妥当性検査セッションの識別子データに対して妥当性検査データを生成し、又は他の方法によりそれを定義することに応じて、商業エンティティサブシステム400は、任意の好適な妥当性検査レスポンスデータ674を生成し通信するように機能することができる。例えば、妥当性検査レスポンスデータ674は、任意の他の好適なデータとともにステップ622の妥当性検査データを含むことができ、この任意の他の好適なデータは、妥当性検査セッション識別子（例えば、チャレンジ要求データ664及び／又はチャレンジレスポンスデータ670の、及び／又は、妥当性検査セッションと関連付けられ得る、妥当性検査セッション識別子）、販売事業者識別子（例えば、チャレンジ要求データ664及び／又はチャレンジレスポンスデータ670の、及び／又は、商業エンティティサブシステム400（例えば、表430内）において妥当性検査セッション中に妥当性検査されている販売事業者オンラインリソースと関連付けられ得る販売事業者識別子）などを含むが、これらに限定されない。いくつかの実施形態において、図6に示すように、このような妥当性検査レスポンスデータ674を、商業エンティティサブシステム400から直接電子デバイス100に（例えば、任意の好適な通信プロトコルを用いた通信経路65を介して）通信することができ、商業エンティティサブシステム400が妥当性検査レスポンスデータ674を適正な電子デバイス100に通信することができるように、電子デバイス100を識別するデータ（例えば、デバイス識別子119）は、妥当性検査セッション開始データ662及び／又はチャレンジ要求データ664及び／又はチャレンジレスポンスデータ670などと関連付けられてもよいし、又は他の方法により、それに含まれてもよい。代替的に、いくつかの実施形態では、このような妥当性検査レスポンスデータ674を、商業エンティティサブシステム400から販売事業者サブシステム200を介して電子デバイス100に通信することができ、それによって、販売事業者サブシステム200は、妥当性検査レスポンスデータ674を商業エンティティサブシステム400から（例えば、任意の好適な通信プロトコルを用いた通信経路85を介して）受信し、そして、妥当性検査レスポンスデータ674の少なくとも一部分を電子デバイス100に（例えば、任意の好適な通信プロトコルを用いた通信経路15を介して、又は非接触近接型通信として）渡すことができるので、妥当性検査レスポンスデータ400は、ステップ624で直接デバイス100とのセキュアな通信チャネルを確立する必要はなくてもよい。妥当性検査レスポンスデータ674は、（例えば、HTTPヘッダ内で、又は別の方法で）商業エンティティサブシステム400により、電子デバイス100にとってもアクセス可能であり得る商業エンティティサブシステム400に関連付けられたアクセス鍵（例えば、セキュアエレメント145のアクセス鍵155a、アクセス鍵155b、CRS151k及び／若しくはISD鍵156k又は、デバイスアプリケーション（例えば、カード管理アプリケーション103b）に知られ得る任意の鍵）で署名されることがあるので、デバイス100は、署名された妥当性検査データを受信するとすぐに署名を妥当性検査し、電子デバイス100によって信頼され得ない別のエンティティサブシステムではなく、商業エンティティサブシステム400が妥当性検査レスポンスデータ674を生成したことを確認することができ、及び／又は、署名された妥当性検査データは、そのようなアクセス鍵へのアクセスを有し得ないエンティティ（例えば、署名された妥当性検査データを商業エンティティサブシステム400からデバイス100に渡すのに使用され得る販売事業者サブシステム200）により利用され得る。

【0068】

上述のように、ステップ610の販売事業者オンラインリソースの潜在的トランザクションデータ660によって識別されるセキュアなデータトランザクションを行うユーザの意図を伝えるために、デバイス100のユーザは図3Aのセキュアな支払いプロンプト309などの販売事業者オンラインリソースのGUI要素（例えば無線ボタン）を選択する

ことができる。

図3Bに示すように、デバイス100及び／又は販売事業者オンラインリソース113は、以下の場合に応じて画面190bを提供するように構成され得る。

図3Aの画面190aにおいて、セキュアな支払いプロンプト309の選択を単体で、又は、デバイス100がステップ624で、妥当性検査セッションエラーがなかったことを示す、妥当性検査レスポンスデータ674を受信したことに加えて受けた場合、及び／又は、

デバイス100が（例えば、ステップ625で）、ステップ612における妥当性検査セッション開始データ662の一部としてデバイス100により生成されたかも知れないセッション識別子と、受信した妥当性検査レスポンスデータ674の一部として提供され得るセッション識別子との一致を検証した場合。

これにより、デバイス100は、レスポンスデータ674が、プロセス600の同一の妥当性検査セッションの一部として、妥当性検査セッション開始データ662と関連付けられていることを確認できる（例えば、デバイス100は（例えば、ステップ612で）販売事業者サブシステム200の販売事業者識別子と組合せて妥当性検査セッション開始データ662のセッション識別子を記憶することができ、そして、記憶されたデータの組合せをセッション識別子及び妥当性検査レスポンスデータ674の販売事業者識別子と比較し（例えば、ステップ625で）、プロセス600の残りの部分を可能とする前に適切な一致を確認することができ、デバイス100は、ステップ612でデバイス100により生成された任意のセッション識別子がステップ612で開始されたセッション中、妥当性検査される特定の販売事業者サブシステム又は販売事業者オンラインリソースに対して一意であることを確実にするように機能することができる）。いずれの場合も、図3Bに示すように、画面190bは、購入を行うためデバイス100にとって利用可能であり得る特定の決済元又はクレデンシャルを選択するために1つ以上の方法でユーザにデバイス100と相互作用するようプロンプトを表示することができる。例えば、画面190bは、ユーザがデバイス100にとって利用可能であり得る複数の決済元のうちの1つを選択することを可能とする決済元選択プロンプト311を含むことができる。決済元選択プロンプト311は、（例えば、上述したように、潜在的トランザクションデータ660により決定され得る）販売事業者によってサポートされた決済ネットワークに関連付けられたクレデンシャルを有する決済元のみ含めることもできず、又は、デバイス100にとって利用可能なすべての決済元を表示するが、許容される決済ネットワークと関連付けられたもののみ選択可能とすることもできる。決済元選択プロンプト311は、任意の好適な決済元（例えば、プロンプト311の決済オプション識別子311aに示され得る「クレデンシャルX」を用いた決済方法、プロンプト311の決済オプション識別子311bに示され得る「クレデンシャルY」を用いた決済方法など）を含むことができ、それは、デバイス100のセキュアエレメントにとってネイティブな任意の好適な決済クレデンシャル及び／又は、デバイス100にとってアクセス可能な任意の利用可能な決済元の任意の好適な非ネイティブ決済クレデンシャル（例えば、クライアントデバイスとしてのデバイス100に対してホストデバイスの役割を果たし得る別のデバイス）を含むが、これらに限定されない。一特定実施例では、図3Cに示すように、デバイス100は、図3Bの決済元選択プロンプト311の識別子311aの「クレデンシャルX」のユーザ選択の受信に応じて、画面190cを提供するように構成されてもよい。図3Cの画面190cは、選択された又は自動的に識別されたデフォルトのクレデンシャルをクレデンシャル識別子情報313で識別することができ、また、選択されたクレデンシャルを利用するユーザ及びその意図を認証するため、1つ以上の方法でデバイス100と相互作用するようデバイス100のユーザにプロンプトを表示することができる。これは、デバイス100のセキュアエレメントに、したがって、購入に使用されるクレデンシャルにアクセスするために、個人識別番号（「PIN」）入力を介して、又はバイオメトリックセンサによるユーザの相互作用を介してユーザ認証を入力するよう（例えば、図3Cの認証プロンプト315で）ユーザにプロンプトを表示することを含むことができる。販売事業者オンラインリソー

10

20

30

40

50

ス妥当性検査セッションは、潜在的トランザクションデータ660が通信されることに
応じて、及び／又は画面190aが提示されることに応じて、及び／又は図3Aの画面19
0aのセキュアな支払いプロンプト309のユーザ選択に応じて、図3Bの決済元選択プ
ロンプト311の特定のクレデンシャルのユーザ選択に応じて、及び／又は、図3Cの画
面190cの提示に応じて、などの任意の好適なイベントに基づいて（例えば、ステップ
612及び／又はステップ614で）開始され得る。図3Bの決済元選択プロンプト31
1は、ステップ612～ステップ624（例えば、ステップ612～ステップ614のい
ずれか1つの前又はその間）で発生し得る妥当性検査セッションの状況にかかわらず、図
3Aの画面190aのセキュアな支払いプロンプト309のユーザ選択に応じて、及び／
又は図3Aの画面190aのセキュアな支払いプロンプト309のユーザ選択だけでなく
、妥当性検査セッションの失敗を示すものではないステップ624での妥当性検査レスポ
ンスデータ674の受け入れにも応じて、などの、任意の好適な瞬間に提示されてもよい
。図3Cの認証プロンプト315は、ステップ612～ステップ624（例えば、ステッ
プ612～ステップ614の前、その間、又はいずれかのステップ）で発生し得る妥当性
検査セッションの状況にかかわらず、決済元選択プロンプト311の決済識別子のユーザ
選択の受信に応じて、及び／又は、決済元選択プロンプト311の決済識別子のユーザ選
択の受信だけでなく、妥当性検査セッションの失敗を示すものではないステップ624で
の妥当性検査レスポンスデータ674の受け入れにも応じてなどの、任意の好適な瞬間に
提示されてもよく、及び／又は画面190cは、ステップ624での妥当性検査レスポ
ンスデータ674の受け入れ前に提示されてもよいが、図3Cの認証プロンプト315は、
ステップ624での妥当性検査レスポンスデータ674の受け入れ後までは使用を可能に
されることができない。

【0069】

デバイス100のユーザが、ステップ610で受信した潜在的トランザクションデータ
660（例えば、決済要求データ）に応じて、潜在的トランザクションへの資金供給に使用
する特定の決済クレデンシャルを選択又は確認する意思及び能力があり、かつ、妥当性
検査レスポンスデータ674がステップ624で電子デバイス100によって受信されて
いる（例えば、ステップ612～ステップ622の販売事業者オンラインリソース妥当性
検査セッションの成功を示し得るデータ）場合、プロセス600は、ステップ625に進
むことができ、プロセス600は、いずれのセッション識別子も一致が（例えば、上述の
ステップ625で）識別された後、（例えば、図3Cの認証プロンプト315のユーザの
選択により）潜在的トランザクションデータ660に基づいて特定の販売事業者、製品、
価格又は配送先に対して潜在的トランザクションを実行するための特定のクレデンシャル
を利用するデバイス100のユーザによる意図及び許可を受信することを含むことができ
る。アクセスSSD154bは、デバイス100のアプレット153bを活用して、その
クレデンシャル情報を商業クレデンシャルデータ通信内で可能とするために他のSSD1
54（例えば、クレデンシャルSSD154a）を使用することが可能になる前にそのよう
な認証が発生したかどうかを判定することができる。ステップ625の一例としては、
アクセスSSD154bのアプレット153bは、（例えば、ユーザがデバイス100の
任意のアプリケーション（例えば、デバイス100の販売事業者リソース113及び／又
はカード管理アプリケーション103b）と相互作用することで使用され得る、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のユーザの意図又はローカル認証を判定するように構成することができ、ま
た、そのような判定に応じて、（例えば、クレデンシャルSSD154aのクレデンシャル
を用いて）決済トランザクションを行うために別の特定のSSDを可能とするように構
成することができる。いくつかの実施形態では、このような判定の後でこのように可能と
する前に、デバイス100のGUIは、選択及び認証されたクレデンシャルを用いて最終
的に決済を開始するよう、1つ以上の方法でデバイス100と相互作用するように（例え
ば、図3Cのプロンプト315と同様のプロンプトで）デバイス100のユーザにプロン
プトを表示することができる別の画面（図示せず）を提供するように構成することができ

る。デバイス100のユーザは、（例えば、画面190a～190cの「販売事業者A」及び「製品B」及び「価格C」及び「配送先D」に対する）ステップ610の潜在的トランザクションデータ660により識別された潜在的トランザクションに資金供給するために、デバイス100にとってネイティブな特定の決済クレデンシャルの使用のためのステップ625で意図及び認証を提供することができる。しかし、代替的に、プロセス600は、ステップ625で意図及び認証が提供され得る前に、デバイス100のユーザが潜在的トランザクションの1つ以上の特性を調整するのを可能とすることができる（例えば、配送先住所情報は、画面190a及び／又は画面190b上で、又は他の方法により、販売事業者サブシステム200とデバイス100との間で通信される追加の更新された潜在的トランザクションデータ660を通して更新され得る）。

10

【0070】

次に、潜在的トランザクションデータ660の特定の決済要求データの受信に応じて、ステップ625で特定の決済クレデンシャルのために意図及び認証が受信されると、プロセス600のステップ626～628は、デバイス100が、（例えば、プロセス500のステップ512及びステップ514に関して説明したように）商業エンティティサブシステム400による使用のためのデバイストランザクションデータ678を生成し、暗号化し、かつ送信することを含むことができる。デバイス100のセキュアエレメント145上のクレデンシャルSSD154aのクレデンシャルが、財務トランザクション（例えば、ステップ625）での使用のために選択され、認証され、及び／又は可能にされると、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、商業エンティティサブシステム400によって使用される、その選択されたクレデンシャルの特定のクレデンシャルデータを生成及び暗号化することができる。例えばトークンデータ及び暗号データなどの、クレデンシャルSSD154a（例えば、（例えば、選択された「クレデンシャルX」と関連付けられ得る）SSD154aの決済カードデータ）のデバイス決済クレデンシャルデータ675は、ステップ626で少なくともトークンデータ及び暗号データを含むデバイス決済クレデンシャルデータ676として生成され、及び／又はクレデンシャル鍵155a'で少なくとも部分的に暗号化され得ることで、このような暗号化されたデバイス決済クレデンシャルデータ676は、デバイス決済クレデンシャルデータ675にアクセスするためのそのクレデンシャル鍵155a'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）により解読されてもよい。このような決済クレデンシャルデータ675は、デバイス100の特定のセキュアエレメントクレデンシャル（例えば、SSD154aのクレデンシャル）の適切な所有をセキュアに証明するように動作し得る任意の好適なデータを含むことができ、この好適なデータは、（i）トークンデータ（例えば、SSD154aのクレデンシャル情報161aのDPAN、DPAN満了日、及び／又はCVV）及び（ii）暗号データ（例えば、SSD154a及び金融機関サブシステム350の共有秘密（例えば、鍵155a'））ならびに、デバイス100にとって利用可能とすることができ、共有秘密を用いて暗号データを独立して生成する金融機関サブシステム350にとって利用可能とさせ得る任意の他の好適な情報（例えば、トークンデータの一部又は全部、デバイス100を識別する情報、コスト及び／又は通貨などのステップ610の潜在的トランザクションデータ660の一部又は全部を識別する情報、任意の好適なカウンタ値、ナンス（例えば、妥当性検査レスポンスデータ674の妥当性検査データのナンス）など）を用いてセキュアエレメント145により生成され得る暗号）を含むが、これらに限定されない。したがって、決済クレデンシャルデータ675は、例えば、主アカウント番号（例えば、実際のF-PAN又は仮想D-PAN）、カードセキュリティコード（例えば、カード妥当性検査コード（「CVV」））、有効期限、クレデンシャルに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との間の共有秘密及び任意の他の好適な情報を用いて生成される暗号）などの、そのクレデンシャルで決済を行うのに必要なすべてのデータを含むことができる。いくつかの実施形態では、クレデンシャルSSD154aの決済クレデンシャルデータ675の一部

20

30

40

50

又は全部がステップ626で暗号化された決済クレデンシャルデータ676としてクレデンシャル鍵155a'で暗号化されると、その暗号化された決済クレデンシャルデータ676は、単独で、又は適用できる潜在的トランザクションデータ660の全部ではないが少なくとも第1の部分（例えば、販売事業者の識別、代金額の識別、通貨及び／又は配送先及び／又は製品の識別、及び一意の販売事業者型トランザクション識別子及び／又は一意のユーザデバイススペースのトランザクション識別子などを含み得る潜在的トランザクションデータ660の一部分又は全部）、妥当性検査レスポンスデータ674の一部又は全部、及び／又は任意の他の好適な情報（例えば、デバイス100自体を識別する情報（例えば、デバイス識別子119）、任意の特有のデバイススペーストランザクション識別子及び／又は同様のもの）とともに、セキュアデバイスデータ677としてステップ627でアクセス情報によって暗号化されてもよい（例えば、SSD154aのアクセス鍵155a、アクセスSSD154bのアクセス鍵155b、ISD鍵156k及び／又はCRS151kによって暗号化されてもよく、及び／又はCASD158kによって署名されてもよい）。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、アクセス情報を使用して、データ660及び／又はデータ674からの販売事業者の識別（例えば、販売事業者又は、アプリケーション113などの購入に使用されるそのリソースの識別）だけでなく、データ660、ならびに、SSD154aの暗号化された決済クレデンシャルデータ675（例えば、暗号化された決済クレデンシャルデータ676）からの購入額及び／又は通貨コードの識別を、セキュアデバイスデータ677に暗号化することができる。いくつかの実施形態では、クレデンシャルSSD154aの決済クレデンシャルデータ675（例えば、トークンデータ及び暗号データなどのSSD154aの決済カードデータ）を生成することができるが、（例えば、ステップ627でデータ677として）商業エンティティ鍵又はアクセス鍵で暗号化する前に、（例えば、ステップ626でデータ676として）クレデンシャル鍵で暗号化することはできない。その代わりに、このような決済クレデンシャルデータ675を（例えば、ステップ627でデータ677として）商業エンティティ鍵又はアクセス鍵で暗号化することができ、それによって、このような実施形態では、今後のデータ676に対する言及又はまた、クレデンシャル鍵で暗号化されていないデータ675に対する言及とすることもできる。いくつかの実施形態では、このような商業エンティティ鍵又はアクセス鍵は、商業エンティティサブシステム400の方式に関連付けられた商業エンティティ公開鍵とすることができ、商業エンティティサブシステム400は関連付けられた商業エンティティ秘密鍵にアクセスし得る。商業エンティティサブシステム400は、このような商業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、そして、（例えば、（例えば、プロセス600のステップ654で）クレデンシャルデータをデバイス100に供給するときに）その商業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。

【0071】

次に、潜在的トランザクションデータ660又は潜在的トランザクション識別情報（例えば、販売事業者の識別、代金額の識別、通貨の識別、一意の販売事業者ベースのトランザクション識別子、製品／サービスの識別及び／又は同様のもの）の少なくとも一部及び／又は、妥当性検査レスポンスデータ674の少なくとも一部分又は全部及び／又は任意の他の好適な情報（例えば、デバイス100自体を識別する情報、一意のデバイススペースのトランザクション識別子及び／又は同様のもの）などの、任意の追加情報とともに、セキュアデバイスデータ677を、（例えば、プロセス500のステップ514に関して説明するように）ステップ628でデバイストランザクションデータ678としてデバイス100から商業エンティティサブシステム400に送信することができる。したがって、デバイストランザクションデータ678（例えば、妥当性検査レスポンスデータ674を有する又は有しないセキュアデバイスデータ677）の少なくとも一部を、デバイストランザクションデータ678のセキュアデバイスデータ677を生成した暗号化に使用されるそのアクセス情報（例えば、アクセス鍵155a、アクセス鍵155b、ISD鍵15

10

20

30

40

50

6 k、CRS 151 k 及び／又は CASD 158 k) へのアクセスを有するエンティティ (例えば、商業エンティティサブシステム 400) により解読することができる。このようなデバイストランザクションデータ 678 を、ステップ 626～ステップ 628 で生成し、そして、ステップ 628 で (例えば、セキュアエレメント 145 から、又は他の方法により通信構成要素 106 及び通信経路 65 を介して) 商業エンティティサブシステム 400 に送信することができる。ステップ 626、627、及び 628 は、デバイストランザクションデータ 678 の一部としてデバイス 100 のセキュアエレメント 145 から生成され送信されるクレデンシャルデータが最初に、デバイス 100 の別の部分 (例えばプロセッサ 102) により解読できないように暗号化されていることを確実にすることができる。すなわち、デバイストランザクションデータ 678 の決済クレデンシャルデータ 675 を、そのセキュアエレメントの外部のデバイス 100 のどの部分にも露出され得ない、又はそれによりアクセスできないクレデンシャル鍵 155 a' で、暗号化されたデバイス決済クレデンシャルデータ 676 として暗号化することができる。また、このようなトランザクションデータ 678 のデバイス決済クレデンシャルデータ 676 を、そのセキュアエレメントの外部のデバイス 100 のどの部分にも露出され得ない、又はそれによりアクセスできないアクセス鍵 (例えば、アクセス鍵 155 a、155 b、156 k、151 k、及び／又は 158 k (例えば、本明細書では「アクセス情報」とも呼ばれる)) でセキュアデバイスデータ 677 として暗号化することができる。

【0072】

次に、ステップ 629 では、プロセス 600 は、商業エンティティサブシステム 400 がデバイストランザクションデータ 678 の少なくとも一部分を受信及び復号することを含むことができる。例えば、商業エンティティサブシステム 400 は、デバイストランザクションデータ 678 を受信することができ、そして、商業エンティティサブシステム 400 で利用可能なアクセス情報 (例えば、155 a、155 b、156 k、151 k、及び／又は 158 k) を用いて、デバイストランザクションデータ 678 のセキュアデバイスデータ 677 を解読することができる。これにより、商業エンティティサブシステム 400 は、決済クレデンシャルデータ 675 を暗号化状態に (例えば、暗号化されたデバイス決済クレデンシャルデータ 676 として) 維持しつつ、(例えば、解読済のセキュアデバイスデータ 677 から) 販売事業者の暗号化されていない識別を判定できるようになる。これは、商業エンティティサブシステム 400 は、ステップ 626 で暗号化されたデバイス決済クレデンシャルデータ 676 として、そのようなデバイス決済クレデンシャルデータ 675 をデバイス 100 のセキュアエレメント 145 により暗号化し得るクレデンシャル鍵 155 a' へアクセスできないからである。追加的に、又は代替的に、販売事業者は、セキュアデバイスデータ 677 とともにデバイストランザクションデータ 678 に含まれ得る追加データによって識別されてもよい。デバイストランザクションデータ 678 は、デバイス 100 又は少なくともそのセキュアエレメントを識別する情報を含むことができるので、デバイストランザクションデータ 678 が商業エンティティサブシステム 400 により受信されると、商業エンティティサブシステム 400 はステップ 629 で使用するべきアクセス情報はどれかを (例えば、アクセス情報 155 a、155 b、156 k、151 k 及び／又は 158 k のどれを) 知ることができる。例えば、商業エンティティサブシステム 400 は、複数のアクセス鍵 155 a／155 b 及び／又は複数の ISD 鍵 156 k にアクセスすることができ、それぞれの鍵は、特定のデバイス 100 又は特定のセキュアエレメントに特有とすることができる。

【0073】

また、ステップ 629 の前又は後に、ステップ 628 で通信されたデバイストランザクションデータ 678 を受信した後、プロセス 600 のステップ 629 は、商業エンティティサブシステム 400 が、デバイストランザクションデータ 678 に含まれるデバイス 100 が有し得る妥当性検査レスポンスデータ 674 の妥当性検査データを妥当性検査することを含むことができる。例えば、このようなデバイストランザクションデータ 678 の受信に応じて、商業エンティティサブシステム 400 は、そのデバイストランザクション

データ678から妥当性検査レスポンスデータ674の少なくとも一部分又は全部を識別し、かつ受信したデバイストラランザクションデータ678の妥当性検査データが商業エンティティサブシステム400に現在記憶されていることを確認する、又は、より具体的には、一部の実施形態では、受信したデバイストラランザクションデータ678の妥当性検査データが、（例えば、プロセス500のステップ516と同様に）ステップ630で（例えば、表430内の）受信したデバイストラランザクションデータ678の妥当性検査セッション識別子に対して、及び／又は受信したデバイストラランザクションデータ678の販売事業者識別子に対して商業エンティティサブシステム400に現在記憶されていることを確認するように機能することができる。いくつかの実施形態において、妥当性検査データと妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクを、リンクが自動的に削除される前の限られた時間量の間だけしか維持できないので、電子デバイス100は、妥当性検査された販売事業者オンラインリソースとの特定のセキュアデータランザクションを実行するため、そのデバイストラランザクションデータ678のセキュアデバイスデータ677を商業エンティティサブシステム400によりセキュアとできるようにするために、ステップ624で妥当性検査レスポンスデータ674を受信し、そして、ステップ628でデバイストラランザクションデータ678を、商業エンティティサブシステム400に送信しなければならない特定の持続時間に限定されることがある（例えば、商業エンティティサブシステム400は、特定時間後の商業エンティティサブシステム400におけるチャレンジデータと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、リンクが作成された後10分以内に表430からのリンクを除去する）ように動作することができる、それにより、ランザクションのセキュリティを向上させることができる）。追加的に、又は代替的に、妥当性検査データと、妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間の記憶されたリンクも、ステップ622で、ステップ614及びステップ620の1つ以上の間に販売事業者サブシステム200により商業エンティティサブシステム400にとって利用できるようにした、デバイス100と販売事業者サブシステム200との間で共有される特定のタイプのセキュアなデータ（例えば、財務ランザクション用の通貨及び金額ならびに決済タイプ）の識別などの、好適な特定の潜在的ランザクション識別情報と（例えば、チャレンジ要求データ664及び／又はチャレンジレスポンスデータ670の一部分として）関連付けることができ、また、同様の特定の潜在的ランザクション識別情報も、ステップ628のデバイストラランザクションデータ678の一部分として電子デバイス100により商業エンティティサブシステム400にとって利用できるようにすることができるので、ステップ630はまた、商業エンティティサブシステム400が（例えば、ステップ616及び／又はステップ622で表430に記憶されているように）ステップ614及び／又はステップ620で受信した妥当性検査データに対して現在記憶されている特定の潜在的ランザクション識別情報がステップ628で受信された特定の潜在的ランザクション識別情報少なくとも同様であることを確認することも含むことができる。例えば、ステップ622では、特定の妥当性検査データが、5米ドルの財務ランザクションを示す潜在的ランザクションと関連付けられた特定の潜在的ランザクション識別情報に対して記憶されるが、ステップ628で特定の妥当性検査データとともに商業エンティティサブシステム400により受信された特定の潜在的ランザクション識別情報が2,000米ドルの財務ランザクションを示している場合、商業エンティティサブシステム400は、\$5と\$2,000との間のずれの大きさにより、デバイストラランザクションデータ678の妥当性検査データを妥当性検査しないように動作することができる。したがって、妥当性検査データとステップ628で受信したデバイストラランザクションデータ678の妥当性検査セッション識別子及び／又は販売事業者識別子とが、商業エンティティサブシステム400で（例えば、表430で）アクティブにリンクされていると確認できる場合、そのリンクと関連付けられ得る他のデータがデバイストラランザクションデータ678により満たされていない場合、妥当性検査データを妥当性検査しなくてもよい（例えば、ステップ616～ステップ622中に

10

20

30

40

50

識別されたセキュアなデータトランザクションのいずれの好適な特性が、好適な量だけ（例えば、財務トランザクション通貨値の10%超だけ、又は健康データのタイムフレームの10%超などの、特定のデータタイプのパーセンテージ偏差）又は、特定のタイプだけ異なる（例えば、健康データのタイプは識別されたデータの2つのインスタンス間（例えば、心拍数データ対マイルウォークデータ、又はバイオメトリックデータ対決済データなど）で異なる、及び／又はトランザクションに使用される通貨タイプは識別されたデータの2つのインスタンス間（例えば、ドル対円など）で異なるといった識別されたデータの異なるタイプ及び／又は商品の配送のための決済トランザクションの配送先住所の場所）ステップ628のデバイストランザクションデータ678とは異なる）。データ比較は、特定のトランザクションのために実際に受信されたデータと、特定の販売事業者が予想基準からずれた特定のインスタンスを検出する（例えば、そのときまでに決済クレデンシャルデータ等処理しただけの販売事業者によるバイオデータの第1のトランザクションを検出する）ための過去の集計データとの間で行うことができ、潜在的トランザクション識別情報は、妥当性検査又は販売事業者によるかつ必ずしもユーザデバイスに関しない不正を検出するのに使用されてもよい（例えば、エンドユーザのプライバシー問題を尊重する特定のインスタンスにおいてデバイスのためではなく販売事業者のために集計データをトラックしてもよい）。

【0074】

次に、ステップ631では、プロセス600は、商業エンティティサブシステム400が決済要求データ610及び／又は妥当性検査セッションにより、したがって、デバイストランザクションデータ678により識別され得る販売事業者と関連付けられた販売事業者鍵（例えば、販売事業者鍵157）を識別し、そして、その販売事業者鍵を用いてデバイストランザクションデータ678の少なくとも一部分を再暗号化することを含むことができる。すなわち、ステップ629で好適なアクセス情報を用いてデバイストランザクションデータ678の少なくとも一部分を解読した後（例えば、セキュアデバイスデータ677を解読し、デバイス決済クレデンシャルデータ676及び、セキュアデバイスデータ677内に暗号化され得る任意の他の情報（例えば、妥当性検査レスポンスデータ674）を達成した後）、商業エンティティサブシステム400は、ステップ631で、デバイストランザクションデータ678の少なくとも一部分（例えば、デバイス決済クレデンシャルデータ676のトークンデータ及び／又は暗号データ）を、デバイストランザクションデータ678内で識別された販売事業者情報と関連付けられ得る、又はステップ630で妥当性検査されたリンクされた妥当性検査データと関連付けられる表430で識別され得る適切な販売事業者鍵で再暗号化することができる。例えば、このような販売事業者鍵（例えば、販売事業者鍵157）を、デバイストランザクションデータ678を用いて識別された商業エンティティ販売事業者情報と、図1Aの表430でのデータとを比較することによって決定することができる。この決定された適切な販売事業者鍵により、商業エンティティサブシステム400は、その販売事業者鍵（例えば、販売事業者鍵157）で、デバイストランザクションデータ678の少なくとも一部分（例えば、デバイス決済クレデンシャルデータ676のトークンデータ及び／又は暗号データ）を暗号化された販売事業者クレデンシャルデータ681として再暗号化することができる。例えば、暗号化された販売事業者クレデンシャルデータ681は、デバイストランザクションデータ678からの少なくとも暗号化されたデバイス決済クレデンシャルデータ676、ならびに、デバイストランザクションデータ678及び／又は潜在的トランザクションデータ660からの、又はそれに基づいた購入額データ又は他の好適なトランザクションデータなどの好適なトランザクションデータを含むことができる。デバイストランザクションデータ678からの販売事業者識別情報は、その販売事業者識別が既に、暗号化された販売事業者クレデンシャルデータ681がステップ631で暗号化され得る販売事業者鍵を決定するのに使用されているので、暗号化された販売事業者クレデンシャルデータ681の中に含まれる必要はない。暗号化された販売事業者クレデンシャルデータ681は、販売事業者サブシステム200により受信されると、販売事業者サブシステム200がこのような暗号

10

20

30

40

50

化された販売事業者クレデンシャルデータ681の作成者として商業エンティティサブシステム400を確立できるように、及び／又は販売事業者サブシステム200がこのよう暗号化された販売事業者クレデンシャルデータ681が署名後修正されていないことを確実にすることができるように商業エンティティサブシステム400により署名され得る。このような暗号化された販売事業者クレデンシャルデータ681は、ステップ631で生成され、そして、ステップ632で、セキュアなトランザクションデータ682として他の好適なデータとともにデバイス100に（例えば、図1Aの経路65を介して商業エンティティサブシステム400のサーバ410からデバイス100の通信構成要素106に）送信されてもよい。

【0075】

ステップ631及びステップ632は、図1Aのセキュアなトランザクションデータ682の一部として商業エンティティサブシステム400から送信されたクレデンシャルデータ（例えば、暗号化された販売事業者クレデンシャルデータ681のトークンデータ及び／又は暗号データ）が、セキュアエレメント145以外のデバイス100の一部分により解読できないように暗号化されてもよいことを確実にするように機能することができる。すなわち、セキュアなトランザクションデータ682のクレデンシャルデータ（例えば、暗号化された販売事業者クレデンシャルデータ681のトークンデータ及び／又は暗号データ）を、いくつかの実施形態では、セキュアエレメント145を含む、デバイス100のいかなる部分にも露出されていない、又は他の方法により、それによりアクセスできない販売事業者鍵（例えば、販売事業者鍵157）で暗号化することができる。また、セキュアなトランザクションデータ682のクレデンシャルデータ（例えば、暗号化された販売事業者クレデンシャルデータ681のトークンデータ及び／又は暗号データ）を、（例えば、ステップ626で）セキュアエレメント145の外部のデバイス100のいかなる部分にも露出していない、又はアクセスできないクレデンシャル鍵155a'で暗号化することができる。

【0076】

そして、ステップ634で、セキュアなトランザクションデータ682を、セキュアなトランザクションデータ684として（例えば、通信経路15を介して、又は非接触近接型通信5として）販売事業者サブシステム200に転送することができる。代替的に、販売事業者クレデンシャルデータ681を、デバイス100（図示せず）を介して通信することなく、商業エンティティサブシステム400から販売事業者サブシステム200に通信することができる。潜在的トランザクションデータ660の1つ、一部、又はすべての部分を、デバイス100及び／又は商業エンティティサブシステム400を通してセキュアなトランザクションデータ682及び／又はセキュアなトランザクションデータ684に運ぶことができるので、潜在的トランザクションの特定の識別子を、プロセス600の間、エンティティのそれぞれにより識別することができ、その識別子は、（i）販売事業者（例えば、「販売事業者A」）の一意の販売事業者識別子及び／又は使用されている特定の販売事業者リソース（例えば、特定の販売事業者アプリケーション113'）の識別などの特定の販売事業者情報、（ii）トランザクションに支払うのに使用される特定の通貨（例えば、円、ポンド、ドルなど）の識別及び／又はトランザクションに支払われる特定の通貨額（例えば、「価格C」）の識別及び／又は購入され、又はレンタルされ、又は他の方法により、支払われる特定の製品又はサービス（すなわち、「製品B」）の識別及び／又は使用されるデフォルトの又は初期の配送先住所（すなわち、「配送D」）の識別などの特定のトランザクション情報、（iii）トランザクションに対する販売事業者にとって許容できる1つ以上のタイプの決済方法（例えば、購入に使用され得る決済カードのリスト（例えば、VisaではなくMasterCard））又はデバイス100により選択され得る決済方法（すなわち、「クレデンシャルX」）を示す情報、（iv）一意の販売事業者ベースのトランザクション識別子（例えば、行われているトランザクションと関連付けるための販売事業者サブシステム200によりランダムに又は一意に生成され得る3又は4文字の英数字列などの任意の好適なデータ要素）、（v）一意のユーザデバイス

10

20

30

40

50

ベースのトランザクション識別子（例えば、行われるトランザクションと関連付けるためのデバイス100によりランダムに又は一意に生成され得る3又は4文字の英数字列などの任意の好適なデータ要素）、(vi) 一意の販売事業者オンラインリソース妥当性検査セッション識別子などを含むが、これらに限定されない。

【0077】

決済クレデンシャルデータ675/676を含む販売事業者クレデンシャルデータ681が販売事業者サブシステム200により（例えば、ステップ634でセキュアなトランザクションデータ684として）受信されると、プロセス600はまた、販売事業者サブシステム200が決済データ686を生成し、取得銀行サブシステム300に（例えば、図1Aの販売事業者サブシステム200と取得銀行サブシステム300との間の通信経路25を介して）送信するように構成され得るステップ636も含むことができ、データ686は、（例えば、セキュアなトランザクションデータ684に含まれ得る、又は他の方法により、それに関連付けられ得るように、又は他の方法により、販売事業者サブシステム200により（例えば、一意のトランザクション識別子に基づいた）潜在的トランザクションデータ660により）既知のトランザクションと関連付けられ得るように）デバイス100のセキュアなデバイス決済クレデンシャルデータ及び製品又はサービスに対する販売事業者の購入価格を示し得る、決済情報と許可要求とを含むことができる。例えば、ステップ636では、販売事業者サブシステム200は、その既知の販売事業者鍵157を活用して、セキュアなトランザクションデータ684の販売事業者クレデンシャルデータ681を少なくとも部分的に解読することができるので、決済データ686は、金融機関サブシステム350にとって利用可能ではない鍵ではなく、そのクレデンシャル鍵155a'（例えば、データ676）で暗号化されたクレデンシャルSSD154aのセキュアな決済クレデンシャルデータを含むことができる。

【0078】

ステップ636で決済データ686が取得銀行サブシステム300に送信されると、ステップ638では、取得銀行サブシステム300は、許可要求データ688として決済データ686からの許可要求情報を金融機関サブシステム350に（例えば、図1Aの取得銀行サブシステム300と金融機関サブシステム350との間の通信経路35を介して）転送することができる。次に、ステップ640では、金融機関サブシステム350の発行銀行サブシステム370が許可要求を（例えば、ステップ640でデータ688として取得銀行サブシステム300から直接に、又はデータ405として決済ネットワークサブシステム360を介して間接に）受信するとき、決済情報（例えば、デバイス100のセキュアエレメント145によるクレデンシャル鍵155a'によって暗号化されたデバイス100の決済クレデンシャルデータ675（例えば、データ676））及び決済額は、そのそれぞれは許可要求データ688ならびにデータ682、684、及び/又は686に含まれ得るが、（例えば、金融機関サブシステム350でクレデンシャル鍵155a'を用いて）解読され、商業クレデンシャルと関連付けられたアカウントは、購入額をカバーするには十分なクレジットを有するかを判定するように分析され得る。十分な資金が存在しない場合、発行銀行サブシステム370は、取得銀行サブシステム300に否定的許可レスポンスを送信することにより、要求されたトランザクションを断ることができる。しかし、十分な資金が存在する場合、発行銀行サブシステム370は、取得銀行サブシステム300に肯定的許可レスポンスを送信することにより、要求されたトランザクションを承認することができ、財務トランザクションを完了することができる。いずれかのタイプの許可レスポンスを、プロセス600のステップ640で許可レスポンストランザクション状況データ690としてユーザ金融サブシステム350により取得銀行サブシステム300に（例えば、図1Aの通信経路45を介して発行銀行サブシステム370から決済ネットワークサブシステム360に提供され得る許可レスポンスデータ415に基づいて通信経路35を介して発行銀行サブシステム370から直接取得銀行サブシステム300に、又は決済ネットワークサブシステム360から取得銀行サブシステム300に）提供することができる。次に、ステップ640で、許可レスポンストランザクション状況データ

690の受信に応じて、プロセス600はまた、取得銀行サブシステム300又は任意の他の好適なサブシステムがステップ642で許可レスポンストランザクション状況データ692として、このような許可レスポンストランザクション状況データを販売事業者サブシステム200と共有することも含むことができ、そして、許可レスポンストランザクション状況データを、ステップ644で確認されたトランザクション状況データ694として（例えば、販売事業者リソースを用いて、又は別の方法で）デバイス100と共有することができる。このような確認されたトランザクション状況データは、図3Dの画面190dの確認データ317などの好適な確認データをデバイス100に提供するように構成されてもよい。トランザクションが成功した場合、確認されたトランザクション状況データは、ステップ644でデバイス100でトランザクションを終了するように機能することができる。追加的に、又は代替的に、トランザクションが成功しなかった場合、確認されたトランザクション状況データは、トランザクションを終了する（例えば、有効な資金が利用可能でなければ、又はデバイスが不正であると識別された場合は、トランザクションを終了するが、有効でない配送先住所が判定された場合は、トランザクションを継続し更新を可能とする）ように動作してもよいし、動作しなくしてもよい。トランザクションを終了させないあらゆるトランザクション状況データは、その処理がアプリケーションによりキャンセルされる、その処理がユーザによりキャンセルされる、又は処理が完了するまで決済処理を継続させることができる。

【0079】

したがって、販売事業者サブシステム200は、セキュアなトランザクションデータ684又は販売事業者クレデンシャルデータ681の他のキャリアを好適な方法で処理するように構成することができる。例えば、販売事業者クレデンシャルデータ681からデバイス決済クレデンシャルデータを得るために、販売事業者サブシステム200は、受信した販売事業者クレデンシャルデータ681の署名性が有効であり、その商業エンティティサブシステム400がその署名の署名者であることを検証することができる。販売事業者サブシステム200は、商業エンティティサブシステム400がどの販売事業者鍵（例えば、どの販売事業者公開鍵157）を使用してもよいかを決定して販売事業者クレデンシャルデータ681を構築する任意の好適な技法を使用することができる。そして、販売事業者サブシステム200は、対応する販売事業者秘密鍵（例えば、販売事業者サブシステム200での販売事業者秘密鍵157）を検索し、その検索された鍵を用いて暗号化された販売事業者クレデンシャルデータ681をカプセル化解除及び／又は解読して暗号化データ676を復元することができる。そして、このようなデータ676を、適切な決済ネットワーク360に提供することができ、それは、金融機関サブシステム350の適切なクレデンシャル鍵155a'を活用して暗号化されたデバイス決済クレデンシャルデータ676をカプセル化解除及び／又は解読し、デバイス決済クレデンシャルデータ675を復元する（例えば、デバイス決済クレデンシャルデータ675を妥当性検査するためデバイス決済クレデンシャルデータ675のトークンデータ及び／又は暗号データを復元する（例えば、受信したデバイス決済クレデンシャルデータ675のトークンデータに基づいて暗号データを独立して生成し、生成された暗号データを、受信したデバイス決済クレデンシャルデータ675の暗号データを比較し、その比較に基づいてトランザクションを妥当性検査するか、又は拒絶する））ことができる。

【0080】

図6のプロセス600で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。図示しないが、セキュアなトランザクションデータを、商業エンティティサブシステム400から直接販売事業者サブシステム200に（例えば、ステップ632及びステップ634でデバイス100を介さず、通信経路85を介して）通信してもよいし、又は（例えば、ステップ632～ステップ638でデバイス100を介さず、及び／又は販売事業者サブシステム200を介さず、及び／又は取得銀行300を介さず、通信経路55を介して）直接金融機関サブシステム350に通信して

もよい。追加的に、又は代替的に、図示しないが、セキュアなトランザクションデータを、デバイス100から直接金融機関サブシステム350に（例えば、販売事業者サブシステム200を介さずに）通信してもよい。プロセス600の妥当性検査ステップが失敗した場合は、そのような失敗を1つ以上の好適なエンティティに通信することができることを理解されたい。例えば、ステップ616でチャレンジ要求データ664の妥当性検査が失敗した場合、及び／又はステップ622でチャレンジレスポンスデータ670の妥当性検査が失敗した場合、及び／又はステップ630でデバイストランザクションデータ678の妥当性検査レスポンスデータ674の妥当性検査データの妥当性検査が失敗した場合、このような失敗は、デバイス100が販売事業者サブシステム200との潜在的トランザクションを解除し、デバイス100から販売事業者オンラインリソースを潜在的に除去することができるように、商業エンティティサブシステム400により、販売事業者サブシステム200及び／又は電子デバイス100と共有されてもよい。デバイス100のユーザがステップ625でセキュアなデータトランザクションに使用するために特定のセキュアなデータ（例えば、特定の決済クレデンシャルの特定の決済クレデンシャルデータ）を選択した後、プロセス600の残りのステップは、そのユーザにとって透過的に発生することがある（例えば、ステップ626～644は、デバイス100に対するユーザによる更なる相互作用なしに発生することがあり、デバイス100のユーザにとって瞬時に行われるもののように見えることがある）。プロセス600は、あたかも、ステップ625の後、セキュアデバイスデータが自動でかつ瞬時に販売事業者サブシステム200に送信されるように、デバイス100のユーザに見えることがあり、トランザクションの状況は（例えば、販売事業者サブシステム200及び／又は商業エンティティサブシステム400により）デバイス100に確認されることができる。追加的に、又は代替的に、販売事業者オンラインリソースの妥当性検査は、デバイス100に対して透過的に発生することができる（例えば、ステップ614～624は、もしステップ612でなければ、デバイス100に対するユーザによる相互作用なしに発生することができ、ステップ610の後デバイス100のユーザに対して瞬時に行われているように見えることがある）。代替的に、いくつかの実施形態では、プロセス600は、デバイス100のユーザにとって透過的に一緒に発生することができる（例えば、デバイス100は、セキュアなデバイストランザクションがいつ発生すべきかを判定し、妥当性検査レスポンスデータを自動で受信し、かつ／又はデバイストランザクションデータを自動で送信するように、かつ／又は、デバイス100に対するユーザによるアクティブな相互作用なしにセキュアなデバイストランザクションのセキュアなトランザクションデータを自動で受信及び／又は送信するように構成されてもよく、販売事業者オンラインリソースは、その特定のセキュアなデバイストランザクションのために開始され、実行される妥当性検査セッションの間、依然として妥当性検査されてもよい）。例えば、上述のように、デバイス100は、すべて自動で、デバイス100のユーザによるアクティブな相互作用なしで、特定の製品を購入すべきことを決定し、その特定の製品の少なくとも1つの特定の販売事業者から関連付けられた潜在的トランザクションデータを取得するために1つ以上の販売事業者と相互作用するように構成することができる（例えば、デバイス100は、家電製品を購入しなければならないことを決定する（例えば、洗濯機がより多くの洗濯洗剤を必要とすることを検出する、又は特定の日より多くの洗剤を購入するための、ユーザが事前に設定したカレンダー行事を検出する）ように構成され得る家電製品であって、自動で、その製品の最良の商談を提供する特定の販売事業者を識別でき、自動で、その販売事業者と相互作用し、その製品をその販売事業者から購入するためにトランザクションデータを取得し得る家電製品とすることができる）。そして、デバイス100及び／又は特定の販売事業者は、ステップ612の妥当性検査セッションを自動的に開始するように機能することができる。

【0081】

いくつかの実施形態では、ステップ618～ステップ622を、ステップ616でチャレンジ要求が妥当性検査された後にスキップしてもよく、代わりに、ステップ616で、チャレンジデータではなく妥当性検査データを生成して記憶してもよい。したがって、い

10

20

30

40

50

くつかの実施形態では、ステップ614及びステップ616は、特定の妥当性検査セッションのための販売事業者オンラインリソースを妥当性検査するのに適切であり得る。いくつかの実施形態では、ステップ616で生成されたチャレンジデータは、ステップ622で生成された妥当性検査データとは異なってもよい。例えば、チャレンジデータは、著しく堅牢なチャレンジを可能とする十分なランダム性を、チャレンジングデータ668とともに販売事業者サブシステム200に提供するのに十分な長さ（例えば、10文字以上などの好適な長さのデータ列）とすることができるが、妥当性検査データは、セッション妥当性検査の証拠を可能とする十分なランダム性を提供するために、及び／又は妥当性検査レスポンスデータデータ674で任意の好適な規格を満たすために（例えば、EMV（Europay MasterCard Visa）規格のデータ長要件を満たすために）10
、チャレンジングデータより短くてもよい（例えば、妥当性検査データは、6文字などの、チャレンジデータのデータ列より短い長さのデータ列としてもよい）。代替的に、チャレンジデータと妥当性検査データは同じであってもよく、ステップ616とステップ622の両方で再利用されてもよい。妥当性検査レスポンスデータ674の妥当性検査データ（例えば、ナンス）は、決済トランザクションがデバイス100と販売事業者との間で発生するという判定に基づくだけではなく、ステップ624で販売事業者サブシステム200のチャレンジの成功した妥当性検査に基づいて、商業エンティティサブシステム400によって生成され、デバイス100に提供されてもよい。デバイス100が販売事業者20
に特有であり得るデバイス100上のネイティブアプリケーションを介して販売事業者サブシステム200と通信することができる場合、販売事業者アプリケーション113はそのようなアプリケーションによって提供されてもよい。しかし、デバイス100が、販売事業者200に特有であってもよいし、特有でなくてもよいが、（例えば、販売事業者の制御下にあるサーバ上の）販売事業者によって管理されたウェブサイトに向けられ得るインターネットブラウザ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介して販売事業者サブシステム200と通信することができる場合、販売事業者アプリケーション113は、通信を販売事業者のウェブサイト（例えば、通信構成要素106を介して）転送し得るレイアウトエンジンソフトウェア構成要素（例えば、WebKit）とすることができる。例えば、デバイス100のこのようなアプリケーション113は、任意のデバイス30
トランザクションデータを販売事業者サブシステム200に提供するためのコンジットとすることができる。

【0082】

ここで、プロセス600の特定の部分の代替的な実施形態を、異なる販売事業者構成に関して記載してもよい。販売事業者サブシステム200は、制御の程度がさまざまであるプロセス600のセキュアなトランザクションに対応するように装備されてもよい。販売事業者サブシステム200がプロセス全体の制御を保持し得る第1の販売事業者構成では、販売事業者サブシステム200は、販売事業者オンラインリソースの妥当性検査（例えば、ステップ614及びステップ616で、及び／又はステップ618及びステップ620で、販売事業者サブシステム200自体が、販売事業者オンラインリソースを妥当性検査するために商業エンティティサブシステム400と通信することができる）だけでなく、商業エンティティサブシステム400により暗号化されたセキュアなデータの解読（例えば、ステップ636で、販売事業者サブシステム200は、販売事業者鍵157を活用して、少なくとも部分的に、セキュアなトランザクションデータ684の販売事業者クレデンシャルデータ681を解読することができる）に対応するように機能することができる。このような第1の販売事業者構成では、販売事業者サブシステム200は、それ自身の決済サービスプロバイダ（「PSP」）の役割を果たすことができ、大容量をもつ巨大販売事業者（例えば、Amazon.com）が典型であり得るような、プロセス600においてオンラインリソースを登録及び妥当性検査するための商業エンティティサブシステム400と通信する唯一のサブシステムとすることができる。代替的に、第2の販売事業者構成では、販売事業者サブシステム200は、図1A及び図6に取得銀行300の一部40
分として示され得る、PSPサブシステム310のような好適な販売事業者パートナサ

10

20

30

40

50

ブシステムに対する決済に関する暗号解読責任を放棄してもよい。このような第2の販売事業者構成では、販売事業者サブシステム200は、販売事業者オンラインリソースの妥当性検査に対応する（例えば、ステップ614で、及び／又はステップ618及びステップ620で、販売事業者サブシステム200自体が、販売事業者オンラインリソースを妥当性検査するために商業エンティティサブシステム400と通信することができる）ように動作することができるが、PSPサブシステム310は、商業エンティティサブシステム400により暗号化されたセキュアなデータの解読に対応する（例えば、ステップ638で、PSPサブシステム310は、販売事業者鍵157を活用して、少なくとも部分的に、決済データ686の販売事業者クレデンシャルデータ681を解読することができる）ように動作することができる。このような第2の販売事業者構成では、販売事業者サブシステム200は、その決済解読のために別個のサードパーティバックエンドPSPを使用することができるので、販売事業者サブシステム200とPSPサブシステム310はともに、プロセス600でオンラインリソースを登録するために商業エンティティサブシステム400と通信することができ、これは、決済サービスプロバイダを活用しうる、より小規模な販売事業者（例えば、取得銀行（例えば、Chase Paymentech）又は小規模PSP（例えば、Stripe、Braintree、First Data）であり、複数の取得銀行、カード及び決済ネットワークと通信し、及び／又は、販売事業者サブシステム200に代わって外部ネットワーク及び銀行口座との技術的接続及び関係を管理し、それによって、販売事業者サブシステム200の金融機関への依存を少なくするように動作し得る）に典型的である。このような第2の販売事業者構成のPSPサブシステム310はデバイス100のユーザから隠されることができ、ユーザは、（例えば、図3A～図3Dの画面190a～190dにより）販売事業者サブシステム200のオンラインリソースとのインタフェースのみ行ってよい。代替的に、第3の販売事業者構成では、販売事業者サブシステム200は、PSPサブシステム310などの、任意の好適な販売事業者パートナーサブシステムに対するオンラインリソース妥当性検査責任及び決済解読責任を委ねることができる。このような第3の販売事業者構成では、PSPサブシステム310は、販売事業者オンラインリソースの妥当性検査（例えば、ステップ614で、PSPサブシステム310自体が、（例えば、PSPサブシステム310が販売事業者サブシステム200からセッション開始データ662を受信することに応じて）販売事業者オンラインリソースを妥当性検査するために商業エンティティサブシステム400とチャレンジ要求データ664を通信することができる）だけでなく、商業エンティティサブシステム400により暗号化されたセキュアなデータの解読にも対応する（例えば、ステップ638で、PSPサブシステム310は、販売事業者鍵157を活用して、少なくとも部分的に決済データ686の販売事業者クレデンシャルデータ681を解読することができる）ように動作することができる。このような第3の販売事業者構成では、販売事業者サブシステム200は、妥当性検査及び決済解読のために別個のサードパーティフロントエンドPSPを使用することができる。そのため、販売事業者サブシステム200とPSPサブシステム310はともに、プロセス600でオンラインリソースを登録し妥当性検査するために商業エンティティサブシステム400と通信することができる。これは、勘定精算（checkout）及び決済プロセス全体のプロセスをサードパーティ決済サービスマークプロバイダによる代行に依存し得る「ロングテール」販売事業者に典型（例えば、StripeのレジはStripeインコーポレイテッドのPSPによって提供され得る）であり得る。別個のサードパーティフロントエンドPSPサブシステム310は、（例えば、販売事業者サブシステム200の販売事業者リソースに埋め込まれたPSPサブシステム310のJavaScript（登録商標）などのPSPサブシステム310のサーバ上でホストされ得る）埋め込み可能な決済フォームをデスクトップ、タブレット及びモバイルデバイスに提供でき、これが販売事業者サブシステム200のウェブリソース内で働くことにより、顧客は（例えばデバイス100のユーザ）トランザクションを完了するのに販売事業者サブシステム200のウェブリソースから離れてリダイレクトされることなく決済を行うこともでき、又は、顧客は販売事業者サブシステム200のウェブリソ

10

20

30

40

50

ースから離れてP S Pサブシステム310のウェブリソースにリダイレクトされて、P S Pサブシステム310のウェブリソース内で決済を完了することもできる（例えば、PayPal.com）。このような第3の販売事業者構成のP S Pサブシステム310は、P S Pオンラインリソースを管理し動作させるように動作することができ、これは販売事業者オンラインリソースと同様であり得るが、例えば、決済自体を処理するように備えられていない販売事業者オンラインリソースによって利用され得る。これにより、例えば、ウェブサイト販売事業者オンラインリソース113は、そのウェブサイト販売事業者オンラインリソース113とインタフェースするデバイス100のユーザを、ウェブサイト販売事業者オンラインリソース113の任意の部分に埋め込まれ得る、ウェブサイトP S Pオンラインリソース113のインタフェースにリダイレクトするか、又はユーザは、ウェブサイト販売事業者オンラインリソース113の任意の好適な部分からリダイレクトされ得る（例えば、図3A～図3Dの画面190a～190dの1つ以上の任意の好適な部分は、ウェブサイト販売事業者オンラインリソースではなく、ウェブサイトP S Pオンラインリソースによって提供され得る）。したがって、販売事業者サブシステム200及びP S Pサブシステム310（例えば、取得者サブシステム300）は、合わせて、システム1の単一で堅牢な処理サブシステム299を提供してもよいし、又はシステム1の構成及び販売事業者サブシステム200の能力に応じてシステム1の別個のエンティティとして使用されてもよい。

【0083】

販売事業者オンラインリソースを商業エンティティサブシステム400に登録することは、販売事業者サブシステム200が、（例えば、3つの販売事業者構成のうちいずれが採用されるかに応じて）単独で又はP S Pサブシステム310と組合せて、商業エンティティサブシステム400でオンラインリソースを妥当性検査し、また商業エンティティサブシステム400により暗号化されるクレデンシャルデータを解読するように動作するように商業エンティティサブシステム400に加入登録することを含むことができる。例えば、ステップ606は、オンラインリソースと関連付けられた1つ以上の販売事業者識別子167に対して商業エンティティサブシステム400と販売事業者サブシステム200又はP S Pサブシステム310との間で共有されている販売事業者鍵157であって、（例えば、ステップ631で）商業エンティティサブシステム400でデータを暗号化するとともに、（例えば、ステップ636又はステップ638で）販売事業者サブシステム200又はP S Pサブシステム310でそのデータを解読するために使用され得るこのような鍵157を含むことができるだけでなく、オンラインリソースと関連付けられた1つ以上の販売事業者識別子167に対して商業エンティティサブシステム400と販売事業者サブシステム200又はP S Pサブシステム310との間で共有されている証明書177であって、（例えば、ステップ614及びステップ616で）オンラインリソースを妥当性検査するのに使用され得る証明書177も含むことができる。

【0084】

一例として、ステップ606では、オンラインリソース（例えば、ウェブサイト販売事業者オンラインリソース113）の共有鍵用の第1の証明書署名要求（「CSR」）を生成し、商業エンティティサブシステム400に通信することができる。共有鍵用のこの第1のCSRは、オンラインリソースのFQDN（fully qualified domain name：完全修飾ドメイン名）（例えば、ルート及びサブドメイン（例えば、DNSホスト名）及び／又は、オンラインリソースのドメインにリンクされ得る任意の好適な販売事業者識別子、及び／又は、オンラインリソースと関連付けられ得る任意の好適な販売事業者パートナーの任意の他の好適な識別子（例えば、販売事業者サブシステム200が商業エンティティサブシステム400により暗号化されたクレデンシャルデータを解読するためにP S Pを使用することができる場合、P S P識別子）を含む、その正確な位置を特定し得るウェブドメイン）などの、オンラインリソースに関連付けられた少なくとも1つの販売事業者識別子167を含むことができる。商業エンティティサブシステム400は、第1のCSRの1つ以上の販売事業者識別子167と関連付けられ得る商業エ

ンティティサブシステム400と販売事業者サブシステム200又はPSPサブシステム310との間で鍵ペア（例えば、公開販売事業者鍵及び秘密販売事業者鍵157）の共有秘密化を促進することによって、ステップ606で共有鍵用の第1のCSRに応答することができる。例えば、鍵ペアのうち第1の販売事業者鍵157を、販売事業者オンラインリソース用の第1のCSRの販売事業者識別子の1つ、一部又はそれぞれに対して、又は他の方法によりそれに関連付けて商業エンティティサブシステム400の表430に記憶することができ、鍵ペアのうち第2の販売事業者鍵157を、販売事業者オンラインリソース用の第1のCSRの販売事業者識別子の1つ、一部又はそれぞれに対して、又は他の方法によりそれに関連付けて、販売事業者サブシステム200及び／又はPSPサブシステム310に記憶することができる。1つ以上の販売事業者識別子を、特定の販売事業者オンラインリソース113と一意に関連付けられた第1の販売事業者識別子167（例えば、ウェブリソース販売事業者オンラインリソース113の場合、FQDB）及び／又は特定の販売事業者サブシステム200の各販売事業者オンラインリソース113と関連付けられた第2の販売事業者識別子167などの、特定の販売事業者オンラインリソース113と関連付けることができる。追加的に、又は代替的に、1つ以上の販売事業者鍵を、特定の販売事業者識別子又は特定の販売事業者オンラインリソース113と関連付けることができる。このような販売事業者鍵及び販売事業者識別子のすべての関連付けを、ステップ606の1つ以上のインスタンスにおいて、商業エンティティサブシステム400（例えば、1つ以上の表430内に）に記憶してもよいし、又は他の方法により、それによってアクセス可能としてもよい。第1の販売事業者構成では、販売事業者サブシステム200は、このような第1のCSRを生成し商業エンティティサブシステム400に提供することができるが、また販売事業者サブシステム200は、オンラインリソース用の第1のCSRの販売事業者識別子167の1つ、一部又はそれぞれに対して、又は他の方法により、それと関連付けて販売事業者鍵157を記憶することができる。第2及び第3の販売事業者構成では、PSPサブシステム310又は販売事業者サブシステム200は、このような第1のCSRを生成し、PSPサブシステム310又は販売事業者サブシステム200のいずれかは、このような第1のCSRを商業エンティティサブシステム400に提供することができるが、またPSPサブシステム310は、商業エンティティサブシステム400から（例えば、直接又は販売事業者サブシステム200を介して）販売事業者鍵157を受信し、オンラインリソース用の第1のCSRの販売事業者識別子167の1つ、一部又はそれぞれに対して、又は他の方法により、それと関連付けて、販売事業者鍵157を記憶することができる。

【0085】

更に、ステップ606では、オンラインリソース（例えば、ウェブサイト販売事業者オンラインリソース113）用の証明書の第2のCSRを生成し、商業エンティティサブシステム400に通信することができる。証明書用のこの第2のCSRは、第1のCSR等の少なくとも1つの販売事業者識別子167（例えば、オンラインリソースのFQDN又は、オンラインリソースのドメインとリンクされ得る任意の他の好適な販売事業者識別子）、及び／又は、オンラインリソースと関連付けられ得る任意の好適な販売事業者パーティナの任意の他の好適な識別子（例えば、販売事業者サブシステム200がオンラインリソースを妥当性検査するためにPSPサブシステムを使用することができる場合、PSP識別子）などの、オンラインリソースに関連付けられた少なくとも1つの販売事業者識別子167を含むことができる。商業エンティティサブシステム400は、商業エンティティサブシステム400と販売事業者サブシステム200又はPSPサブシステム310との間で生成され、共有されている証明書177を促進することによって、ステップ606で証明書用の第2のCSRに応答することができ、証明書177は、第2のCSRの販売事業者識別子167の1つ、一部又は全部を含むことができ、（例えば、第2のCSRの販売事業者識別子のうち1つ以上によって識別され得る）販売事業者オンラインリソース用の第1のCSRの販売事業者鍵を用いて（例えば、商業エンティティサブシステム400により）生成され得る。例えば、第2のCSRのオンラインリソース用の証明書177を

、オンラインリソース用の第2のCSRの販売事業者識別子の1つ、一部、又はそれぞれに対して、又は他の方法により、それと関連付けて、商業エンティティサブシステム400の表430に記憶することができ、証明書177も、オンラインリソース用の第2のCSRの販売事業者識別子の1つ、一部、又はそれぞれに対して、又は他の方法により、それと関連付けて、販売事業者サブシステム200及び／又はそのPSPサブシステム310にも記憶することができる。証明書177は、TLS (transport layer security) 証明書又はSSL (secure sockets layer) 証明書などの好適なデジタル証明書とすることができる。第1の販売事業者構成及び第2の販売事業者構成の両方では、販売事業者サブシステム200は、このような第2のCSRを生成し、商業エンティティサブシステム400に提供することができ、また販売事業者サブシステム200は、オンラインリソース用の第2のCSRの販売事業者識別子167の1つ、一部又はそれぞれに対して、又は他の方法によりそれと関連付けて証明書177を記憶することができる。第3の販売事業者構成では、PSPサブシステム310及び／又は販売事業者サブシステム200は、そのような第2のCSRを生成することができるとともに、このような第2のCSRを商業エンティティサブシステム400に提供することができ、またPSPサブシステム310は、オンラインリソース用の第2のCSRの販売事業者識別子167の1つ、一部又はそれぞれに対して、又は他の方法により、それと関連付けて証明書177を記憶することができ、PSPサブシステム310に証明書177を提供するこのプロセスは、販売事業者サブシステム200に関わりなく行われてもよく、販売事業者サブシステム200がPSPサブシステム310とパートナーシップを形成する前に行われてもよい（例えば、PSPサブシステム310は商業エンティティサブシステム400の信頼されたPSPとすることができ、決済がPSPサブシステム310及びPSPサブシステム310のドメインを介して発生しているフロントエンドPSPモデルを提供するため販売事業者サブシステム200がPSPサブシステム310とパートナーシップを形成する前に証明書177を備えてもよい）。販売事業者サブシステム200は、PSPが提供したドメインと、PSPサブシステム310が信頼しており、そのドメインに対する証明書177を有する商業エンティティサブシステム400からの要求確認を商業エンティティサブシステム400に提供することができる。

【0086】

更に、ステップ606では、第1のCSR及び第2のCSRのいずれか又は両方に対応する前、対応中又は対応した後に、販売事業者サブシステム200による又は販売事業者パートナーPSPサブシステム310によるウェブサイトオンラインリソースのドメイン（例えばFQDN）の所有権を検証する、又は他の方法により、（例えば、ステップ501に関して説明するように）商業エンティティサブシステム400に証明することができる。鍵用の第1のCSR、証明書用の第2のCSR、及びドメイン妥当性検査のいずれか1つは、鍵用の第1のCSR、証明書用の第2のCSR、及びオンラインリソースの登録時のドメイン妥当性検査のいずれか1つの前又は後に生じてよい。しかし、いくつかの実施形態では、証明書用の第2のCSRを処理する前にドメインを検証することは、より容易かつ／又はより効率的な登録プロセスを可能とすることができる。第1の販売事業者構成及び第2の販売事業者構成の両方では、販売事業者サブシステム200は、商業エンティティサブシステム400に加入・登録されているウェブサイト販売事業者オンラインリソースのFQDNを共有することができ、商業エンティティサブシステム400は、（例えば、JSONファイルなどの）好適なファイルを販売事業者サブシステム200に提供することができ、販売事業者サブシステム200は、（例えば、共有販売事業者鍵157で）そのファイルに署名し、そのファイルをFQDN上にホストすることができ、そして、商業エンティティサブシステム400は、FQDNからその署名されたファイルにアクセスし、（例えば、共有販売事業者鍵157で）そのファイルの署名を削除し、アクセスされたファイルが販売事業者サブシステム200と共有されたファイルと一致すること、及び任意の関連付けられた閾値が満たされていること（例えば、持続時間など）を確認することができる。第3の販売事業者構成では、PSPサブシステム310は、商業エンテ

ィティサブシステム400に加入・登録されているウェブサイトオンラインリソースのFQDNを共有することができ、商業エンティティサブシステム400は、（例えば、JSONファイルなどの）好適なファイルをPSPサブシステム310に提供することができ、PSPサブシステム310は、（例えば、共有販売事業者鍵157で）そのファイルに署名し、そのファイルをFQDN上にホストすることができ、そして、商業エンティティサブシステム400は、FQDNからその署名されたファイルにアクセスし、（例えば、共有販売事業者鍵157で）そのファイルの署名を削除し、アクセスされたファイルがPSPサブシステム310と共有されたファイルと一致すること、及び任意の関連付けられた閾値が満たされていること（例えば、持続時間など）を確認することができる。第3の販売事業者構成では、販売事業者サブシステム200は、販売事業者サブシステム200とPSPサブシステム310との間のパートナーシップを示す商業エンティティサブシステム400にデータを通信するように機能することができるので、商業エンティティサブシステム400は、PSPサブシステム310の妥当性検査を販売事業者サブシステム200に確認し、プロセス600の他の部分の間における任意の好適な使用のために（例えば、表430で）販売事業者サブシステム200の販売事業者識別子167とPSPサブシステム310のFQDN及び／又は証明書177との間の関連付けを記憶するように機能することができる。いくつかの実施形態では、第2及び第3の販売事業者構成のPSPサブシステム310に提供される販売事業者鍵（単数又は複数）157は、いずれかのパートナー販売事業者サブシステム200に対してデータを解読するためにPSPサブシステム310によってグローバルに使用されてもよい。代替的に、第2及び第3の販売事業者構成のPSPサブシステム310に提供される販売事業者鍵（単数又は複数）157は、特定のパートナー販売事業者サブシステム200に特有とすることができ、それによって、販売事業者サブシステム200は、（例えば、鍵用の第1のCSRで）商業エンティティサブシステム400と通信することができ、そして、PSPサブシステム310がその販売事業者サブシステム200に特有のそのような販売事業者鍵（単数又は複数）157を（例えば、商業エンティティサブシステム400から直接、又は販売事業者サブシステム200から）受信できるようにすることができ、このような販売事業者鍵（単数又は複数）157を、商業エンティティサブシステム400（例えば、表430で）及び／又はPSPサブシステム310において記憶する、又は他の方法により、販売事業者サブシステム200の好適な販売事業者識別子167と関連付けることができる。これにより、PSPサブシステム310の他の販売事業者特有の鍵を他の販売事業者サブシステムに対して使用できるようにしながら、特定の販売事業者サブシステムがもはや商業エンティティサブシステム400により信頼されない場合、販売事業者特有の販売事業者鍵157を商業エンティティサブシステム400で無効化することができる。いくつかの実施形態では、（例えば、PSPサブシステム310が商業エンティティサブシステム400を販売事業者のプロキシとして販売事業者に実装されるように）販売事業者サブシステム200が直接そのプロセスに関わることなく、PSPサブシステム310が商業エンティティサブシステム400と、PSPサブシステム310の特定のパートナー販売事業者サブシステム200に特有であり得る任意の販売事業者鍵157及び証明書177を共有することを可能とするため、PSPサブシステム310が直接商業エンティティサブシステム400とインタフェースできるようにするための1つ以上のAPIを提供することができる。証明書177はまた、PSPサブシステム310にとってグローバルであってもよいし、又は特定のパートナー販売事業者サブシステム200に特有であってもよい。

【0087】

したがって、ステップ606及び／又はステップ501は、商業エンティティサブシステム400によって検証されるオンラインリソースのドメインだけでなく、商業エンティティサブシステム400でオンラインリソースを加入・登録させるために、商業エンティティサブシステム400ならびに、販売事業者サブシステム200及び／又は販売事業者パートナーPSPサブシステム310で販売事業者鍵157及び証明書177の両方に対して記憶されるオンラインリソースのドメインと関連付けられるか、又は同じである販売事

10

20

30

40

50

業者識別子167も含むことができる。これにより、オンラインリソースの検証されたFQDN及び／又は任意の他の好適な販売事業者識別子167を、販売事業者鍵157及び証明書177に対して、（例えば、プロセス600のステップ614、616及び／又はプロセス500のステップ506における）妥当性検査セッション中のオンラインリソースのFQDNの妥当性検査を可能とするためだけでなく、（例えば、プロセス600のステップ631及び／又はプロセス500のステップ518における）商業エンティティサブシステム400によるセキュアなデータの暗号化、及び、（例えば、プロセス600のステップ636又は638及び／又はプロセス500のステップ522における）販売事業者サブシステム200又はPSPサブシステム310による当該暗号化されたセキュアなデータのカウンターパート復号を可能とするためにも、商業エンティティサブシステム400及び販売事業者サブシステム200及び／又はPSPサブシステム310（例えば、プロセス600のステップ606及び／又はプロセス500のステップ501における）において記憶することができる。例えば、第1の販売事業者構成及び第2の販売事業者構成の両方では、販売事業者オンラインリソース113の妥当性検査セッションを開始するため、販売事業者サブシステム200がステップ612で任意の好適な販売事業者オンラインリソース妥当性検査セッション開始データ662をデバイス100から受信することに応じて、このような妥当性検査セッション開始データ662がオンラインリソースの識別子（例えば、デバイス100によりアクセスされる販売事業者オンラインリソースのFQDN）を含むことができる場合、販売事業者サブシステム200は、実行される特定のセキュアなデータトランザクション（例えば、ステップ610及び／又はステップ612での金融決済トランザクション）のための販売事業者オンラインリソースを妥当性検査するため、販売事業者サブシステム200がステップ606で受信し、妥当性検査セッション開始データ662のFQDNに対して記憶された証明書177を含む任意の好適なチャレンジ要求データ664を、ステップ614で商業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る。代替的に、第3の販売事業者構成では、PSPオンラインリソース113の妥当性検査セッションを開始するため、PSPサブシステム310がステップ612で任意の好適なオンラインリソース妥当性検査セッション開始データ662をデバイス100から受信することに応じて、このような妥当性検査セッション開始データ662がオンラインリソースの識別子（例えば、デバイス100によりアクセスされるPSPオンラインリソースのFQDN）を含むことができる場合、PSPサブシステム310は、実行される特定のセキュアなデータトランザクション（例えば、ステップ610及び／又はステップ612での金融決済トランザクション）のためのPSPオンラインリソースを妥当性検査するため、PSPサブシステム310がステップ606で受信し、妥当性検査セッション開始データ662のFQDNに対して記憶された証明書177を含む任意の好適なチャレンジ要求データ664を、ステップ614で商業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る。ステップ614で販売事業者サブシステム200又はPSPサブシステム310から商業エンティティサブシステム400に通信された、このようなチャレンジ要求データ664は、商業エンティティサブシステム400に対してオンラインリソースの妥当性を証明しようとするための任意の好適なデータを含むことができ、これには、限定されることなく、証明書177が含まれ、この証明書は、FQDN及び／又は、ステップ606で商業エンティティサブシステム400により生成されるオンラインリソースと関連付けられた任意の他の好適な識別子、及び、任意の他の好適なデータ（例えば、デバイス100を識別するデータ及び／又は、実行される特定のセキュアなデータトランザクションを識別するデータ（例えば、本明細書では、潜在的トランザクション識別情報と呼ばれる場合もあるステップ610及び／又はステップ612で識別される金融決済トランザクションであって、それは、追加のセキュリティ層（単数又は複数）を現在のデータトランザクションプロセスに提供するための、及び／又は将来のデータトランザクションのための追加のセキュリティ（例えば、不正検出）サービスを提供するためのプロセス600の任意の好適な部分の間に使用され得る））を含むことができる。

10

20

30

40

50

【0088】

プロセス600のステップ616では、商業エンティティサブシステム400がステップ614で証明書177を有する任意の好適なチャレンジ要求データ664を販売事業者サブシステム200又はPSPサブシステム310から受信することに応じて、商業エンティティサブシステム400は、チャレンジ要求の販売事業者識別子167により識別されるオンラインリソース113を妥当性検査するように機能することができる。例えば、第1の販売事業者構成及び第2の販売事業者構成の両方では、商業エンティティサブシステム400がステップ614で証明書177を有する任意の好適なチャレンジ要求データ664を販売事業者サブシステム200から受信することに応じて、商業エンティティサブシステム400は、受信したチャレンジ要求データ664の証明書177を検証及びチェックし、その信頼が依然として妥当であり、任意の好適なプロセス（単数又は複数）を通じて満了していないことを確実にするように機能することができる（例えば、証明書177は、データ664中で商業エンティティサブシステム400により受信され得、そして、商業エンティティサブシステム400は、その証明書177が商業エンティティサブシステム400に知られている（例えば、表430に記憶されている）か否か、及びその証明書177が依然として信頼されるものか、及び／又はその証明書177が満了していないかを判定するように機能することができる）。次に、受信した証明書177が検証されると、受信した証明書177からFQDN及び／又は別の販売事業者識別子167を抽出し、商業エンティティサブシステム400の表430に記憶されているFQDN及び証明書177の関連付けと照合して、受信した証明書177のFQDNが登録されることを確実にすることができる。例えば、ステップ616では、商業エンティティサブシステム400は受信したチャレンジ要求データ664の販売事業者識別子167によって識別されたオンラインリソース113が商業エンティティサブシステム400において妥当でかつ登録されたオンラインリソースであることを確認しようとするように機能することができる。そのことは、（例えば、（例えば、ステップ606で）販売事業者識別子167が商業エンティティサブシステム400に登録されていること、及びそのような登録が依然として妥当であること（例えば、商業エンティティサブシステム400が販売事業者識別子167を表430から除去していないか、又は疑わしいもの又は他の方法により、もはや信頼されていないものとして、表430で販売事業者識別子167にフラグを立てていないこと）を判定するために）表430のその販売事業者識別子167を識別することによって確認することができる。同様に、第3の販売事業者構成では、商業エンティティサブシステム400がステップ614で証明書177を有する任意の好適なチャレンジ要求データ664をPSPサブシステム310から受信したことに応じて、商業エンティティサブシステム400は、受信したチャレンジ要求データ664の証明書177を検証及びチェックし、その信頼が依然として妥当であり、満了していないことを確実にように機能することができ、受信した証明書177が検証されると、FQDN及び別の販売事業者識別子167及びPSP識別子を、受信した証明書177から抽出できるので、そして、識別されたPSPが識別された販売事業者に代わってトランザクションを行うように許可されているか、ならびに、抽出されたFQDNがステップ614の要求を完全に妥当性検査するために商業エンティティサブシステム400における他の抽出された販売事業者識別子に登録されているかを判定することができる。販売事業者識別子167は、特定の販売事業者サブシステム200のグローバル販売事業者識別子とすることができる（例えば、単一の販売事業者識別子167を、ネイティブアプリの販売事業者オンラインリソース及び販売事業者サブシステム200のウェブサイト販売事業者オンラインリソースを識別するのに使用することができ、及び／又は単一のFQDNを、複数の販売事業者サブシステムと関連付けることができる（例えば、PSPのFQDNは複数の販売事業者サブシステムにより使用され得る））。FQDN及び、特定の販売事業者サブシステム200及び特定のPSPサブシステム310の一意の識別子などの少なくとも1つの他の識別子とともに、証明書177から抽出され、ステップ606で行われ得たように、これらの2つが商業エンティティサブシステム400において（例えば、表430で）既に互いに関連付

10

20

30

40

50

けられていることが確認できる。商業エンティティサブシステム400による受信したチャレンジ要求データ664の好適な妥当性検査後（例えば、受信した証明書177の妥当性検査後及び／又は受信した証明書177のFQDNの妥当性検査後及び識別されたPSPと受信した証明書177の識別された販売事業者との間の許可された関係を確認後）、商業エンティティサブシステム400はまた、ステップ616で、好適な妥当性検査データを生成し、受信したチャレンジ要求データ664の好適な識別子データに対してその妥当性検査データを記憶するように機能することができる。例えば、ステップ616での受信したチャレンジ要求データ664の好適な妥当性検査後、商業エンティティサブシステム400はまた、ステップ616で、好適な妥当性検査データ（例えば、（例えば、上述のステップ622の妥当性検査データと同様の）エントロピーを介した好適なランダムデータ及び／又は好適な暗号ナンス）及び妥当性検査セッション識別子（例えば、好適な英数字列又は（例えば、ステップ612でデバイス100によって、又はステップ614で販売事業者サブシステム200若しくはPSPサブシステム310によって、又はステップ616で商業エンティティサブシステム400によって生成され得る）商業エンティティサブシステム400に対して現在のオンラインリソースを一意に識別し得る他の好適な識別子）を生成するように機能することができ、そして、商業エンティティサブシステム400は、ステップ616で、商業エンティティサブシステム400にとってアクセス可能な好適なデータ構造で（例えば、表430で、又は別の方法で）その妥当性検査データを、妥当性検査セッション識別子及びチャレンジ要求データ664の販売事業者識別子の一方又は両方に対して記憶することができる。したがって、特定の実施形態では、妥当性検査セッション識別子が、少なくとも特定の販売事業者識別子に対して、商業エンティティサブシステム400により実行されている特定の妥当性検査プロセスに対して一意であることを商業エンティティサブシステム400が確実とすることができるように、妥当性検査セッション識別子は商業エンティティサブシステム400により生成されてもよい。しかし、妥当性検査セッション識別子が販売事業者サブシステム200又はPSPサブシステム310によって生成されると、商業エンティティサブシステム400は、そのような妥当性検査セッション識別子が、その妥当性検査セッション識別子とその特定の妥当性検査セッションに使用できるようにする前の妥当性検査セッションの販売事業者識別子に一意であることを確認することができる。そうでなければ、商業エンティティサブシステム400は、妥当性検査セッション識別子を拒絶し、新しい識別子が販売事業者サブシステム200又はPSPサブシステム310によって生成されることを要求することができる。そのような妥当性検査データと妥当性検査セッションの識別子データ（例えば、妥当性検査セッション識別子及び／又はチャレンジ要求データ664の販売事業者識別子）とのこのような記憶されたリンク又は関連付けは、（例えば、ステップ630で）実行されるセキュアなデータトランザクションを更にセキュアとするために、後に商業エンティティサブシステム400によって使用され得る。また、いくつかの実施形態では、チャレンジ要求データ664の潜在的トランザクション識別情報のいずれか又はすべてが、ステップ616で妥当性検査データ及び識別子データに対して記憶され、又は他の方法によりそれらと関連付けられてもよい。

【0089】

第1、第2及び第3の販売事業者構成のうちいずれか1つの構成では、このようなステップ616の後、オンラインリソースをステップ614及び616の単一のセットで妥当性検査することができるので、ステップ618、620及び622をスキップすることができ、そして、プロセス600は、商業エンティティサブシステム400が好適な妥当性検査レスポンスデータ674を生成かつ通信するように機能し得るステップ624を含むことができる。例えば、妥当性検査レスポンスデータ674は、限定されることなく、妥当性検査セッション識別子（例えば、ステップ616で生成された妥当性検査セッション識別子）、1つ以上の販売事業者識別子（例えば、チャレンジ要求データ664（例えば、FQDN、他の販売事業者識別子、PSP識別子など）のいずれかの、若しくはそれぞれの販売事業者識別子、及び／又は、他の方法により、商業エンティティサブシステム4

00で（例えば、表430で）妥当性検査セッション中に妥当性検査されているオンラインリソースと関連付けられ得るいずれかの、若しくはそれぞれの販売事業者識別子）、チャレンジ要求データ664の証明書177、又は同様のものを含み得る他の好適なデータとともにステップ616の妥当性検査データを含み得るセッションオブジェクトとすることができる。いくつかの実施形態において、図6に示すように、このような妥当性検査レスポンスデータ674を、商業エンティティサブシステム400から直接電子デバイス100に（例えば、任意の好適な通信プロトコルを用いた通信経路65を介して）通信することができ、商業エンティティサブシステム400が妥当性検査レスポンスデータ674を適正な電子デバイス100に通信することができるように、電子デバイス100を識別するデータ（例えば、デバイス識別子119）は、妥当性検査セッション開始データ662及び／又はチャレンジ要求データ664などに関連付けられてもよいし、又は他の方法により、それに含まれてもよい。代替的に、いくつかの実施形態（図示せず）では、妥当性検査レスポンスデータ674を、（例えば、第1又は第2の販売事業者構成の）販売事業者サブシステム200を介して、及び／又は、（例えば、第3の販売事業者構成の）PSPサブシステム310を介して商業エンティティサブシステム400から電子デバイス100に通信することができることによって、販売事業者サブシステム200及び／又はPSPサブシステム310は妥当性検査レスポンスデータ674を商業エンティティサブシステム400から受信し、そして、妥当性検査レスポンスデータ674の少なくとも一部分を電子デバイス100に渡すことができる。妥当性検査レスポンスデータ674のセッションオブジェクトは、（例えば、HTTPヘッダ内で、又は別の方法で）商業エンティティサブシステム400により、電子デバイス100がアクセス可能であり得る商業エンティティサブシステム400に関連付けられたアクセス鍵（例えば、セキュアエレメント145のアクセス鍵155a、アクセス鍵155b、CRS151k及び／若しくはISD鍵156k又は、デバイスアプリケーション（例えば、カード管理アプリケーション103b）に知られ得る任意の鍵）で署名されることがあるので、デバイス100は、署名された妥当性検査データを受信するとすぐに署名を妥当性検査し、電子デバイス100により信頼され得ない別のエンティティサブシステムではなく、商業エンティティサブシステム400が妥当性検査レスポンスデータ674を生成したことを確認する、及び／又はそのようなアクセス鍵へのアクセスを有しない別のエンティティ（例えば、販売事業者サブシステム200及び／又はPSPサブシステム310）が、その他のエンティティがそのような署名された妥当性検査データを受信し、それをデバイス100に転送することを依然として可能にしながら、署名された妥当性検査データを使用するのを防止することができる。

【0090】

第1、第2及び第3の販売事業者構成のいずれか1つの構成では、デバイス100のユーザが、ステップ610で受信した潜在的トランザクションデータ660（例えば、決済要求データ）に応じて、潜在的トランザクションに資金供給するのに使用される特定の決済クレデンシャルを選択又は確認する意思と能力があり、また、妥当性検査レスポンスデータ674がステップ624で電子デバイス100によって受信されている（例えば、ステップ612～ステップ616の販売事業者オンラインリソース妥当性検査セッションの成功を示し得るデータ）場合、プロセス600は、ステップ625に進むことができ、この場合、プロセス600は、セッション識別子の一致が（例えば、上述のステップ625で）識別された後、（例えば、図3Cの認証プロンプト315のユーザの選択により）潜在的トランザクションデータ660に基づいて特定の販売事業者、製品、価格又は配送先に対して潜在的トランザクションを実行するための特定のクレデンシャルを利用するデバイス100のユーザによる意図及び認証を受信することを含むことができる。いくつかの実施形態では、セッション識別子整合性がこのような意図及び認証に先立って検証されることを含むステップ625に加えて、又は代替的に、ステップ625は、ドメイン整合性がこのような意図及び認証に先立って検証されることを含むことができる。例えば、ステップ624でデバイス100が妥当性検査レスポンスデータ674を受信したことに応答

10

20

30

40

50

して、デバイス100は、そのような妥当性検査レスポンスデータ674のドメイン識別子（例えば、妥当性検査レスポンスデータ674のFQDN）を現在デバイス100のオンラインリソースのアドレスバー内にあるドメイン識別子と比較するように機能することができる。例えば、デバイス100のウェブキット（例えば、オンラインリソースアプリケーション113）は、妥当性検査レスポンスデータ674を受信し、その妥当性検査レスポンスデータ674を、そのウェブキットが現在ターゲットとしているドメイン識別子（例えば、FQDN）とともにデバイス100のパスキット（例えば、カード管理アプリケーション103b）に中継することができる。そして、パスキットは、（もしあれば）受信した妥当性検査レスポンスデータ674の署名を（例えば、デバイス100のアクセス鍵を用いて）妥当性検査し、ドメイン識別子（例えば、FQDN）を妥当性検査レスポンスデータ674から抽出し、そして、その抽出されたドメイン識別子をウェブキット（例えば、デバイス100のウェブキットによって現在ホストされているJavaScript（登録商標）のFQDN（例えば、第1及び第2の販売事業者構成の販売事業者オンラインリソースのFQDN及び第3の販売事業者構成のPSPオンラインリソースのFQDN）によって識別され、かつ提供されたドメイン識別子と比較することができ、それにより、（例えば、リプレイ攻撃を回避するため）デバイス100がレスポンスデータ674がデバイス100により現在アクセスされている同一のオンラインリソースに関連付けられていることを確認するのを可能とすることができる。ステップ625で好適なセッション識別子整合性及び／又は好適なドメイン識別子整合性が検証された後、ステップ625で特定の決済クレデンシャルのための意図及び認証を受信することができる。そして、第1、第2及び第3の販売事業者構成のそれぞれの構成について、ステップ626～629が上述のように発生することができ、妥当性検査レスポンスデータ674のいずれかの又はすべての好適な部分（例えば、セッション識別子、妥当性検査データ（例えば、ナンス）、FQDN及び／又は任意の他の好適な販売事業者識別子又はPSP識別子、及び／又は他のデータ（例えば、証明書177の少なくとも一部分））は、デバイストランザクションデータ678として、セキュアデバイスデータ677及びトランザクションデータ660とともに含まれ得る。

【0091】

第1、第2及び第3の販売事業者構成のうちいずれか1つの構成では、商業エンティティサブシステム400は、ステップ630で、デバイス100がデバイストランザクションデータ678の中に含み得た妥当性検査レスポンスデータ674の妥当性検査データを妥当性検査するように機能することができる。例えば、このようなデバイストランザクションデータ678の受信に応じて、商業エンティティサブシステム400は、そのデバイストランザクションデータ678から妥当性検査レスポンスデータ674の少なくとも一部分又は全部を識別し、かつ受信したデバイストランザクションデータ678の妥当性検査データが商業エンティティサブシステム400に現在記憶されていることを確認する、又は、より具体的には、一部の実施形態では、受信したデバイストランザクションデータ678の妥当性検査データが、（例えば、プロセス500のステップ516と同様に）ステップ630で（例えば、表430内の）受信したデバイストランザクションデータ678の妥当性検査セッション識別子に対して、及び／又は受信したデバイストランザクションデータ678の販売事業者識別子（例えば、FQDN）に対して商業エンティティサブシステム400に現在記憶されていることを確認するように機能することができる。妥当性検査データと妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクを、リンクが自動的に削除される前の限られた時間量の間だけしか維持できないので、電子デバイス100は、妥当性検査された販売事業者オンラインリソースとの特定のセキュアなデータトランザクションを実行するため、そのデバイストランザクションデータ678のセキュアデバイスデータ677を商業エンティティサブシステム400によりセキュアとできるようにするために、ステップ624で妥当性検査レスポンスデータ674を受信し、そして、ステップ628でデバイストランザクションデータ678を、商業エンティティサブシステム400に送信しなければならない特定

10

20

30

40

50

の持続時間を限定することがある（例えば、商業エンティティサブシステム400は、特定時間後に商業エンティティサブシステム400におけるチャレンジデータと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、リンクが作成された後10分以内に表430からのリンクを除去する）ように機能することができ、それにより、トランザクションのセキュリティを向上させることができる）。追加的に、又は代替的に、妥当性検査データと、妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間の記憶されたリンクも、ステップ622で、ステップ614で販売事業者サブシステム200又はPSPサブシステム310により商業エンティティサブシステム400にとって利用できるようにした、デバイス100と販売事業者サブシステム200又はPSPサブシステム310との間で共有される特定のタイプのセキュアなデータ（例えば、財務トランザクション用の通貨及び金額ならびに決済タイプ）の識別などの、好適な特定の潜在的トランザクション識別情報と（例えば、チャレンジ要求データ664の一部として）関連付けることができ、また、同様の特定の潜在的トランザクション識別情報も、ステップ628のデバイストランザクションデータ678の一部として電子デバイス100により商業エンティティサブシステム400にとって利用できるようにすることができるので、ステップ630はまた、商業エンティティサブシステム400が（例えば、ステップ616で表430に記憶されているように）ステップ614で受信した妥当性検査データに対して現在記憶されている特定の潜在的トランザクション識別情報がステップ628で受信された特定の潜在的トランザクション識別情報少なくとも同様であることを確認することも含むことができる。

【0092】

次に、ステップ631では、プロセス600は、商業エンティティサブシステム400が販売事業者サブシステム200又はPSPサブシステム310（例えば、妥当性検査セッションのオンラインリソースのステップ606で鍵用の第1のCSRを生成し得たサブシステム）に関連付けられた販売事業者鍵（例えば、販売事業者鍵157）を識別することを含むことができる。すなわち、ステップ629で好適なアクセス情報を用いてデバイストランザクションデータ678の少なくとも一部分を解読した後（例えば、セキュアデバイスデータ677を解読し、デバイス決済クレデンシャルデータ676及びセキュアデバイスデータ677内に暗号化され得た任意の他の情報を達成した後）、商業エンティティサブシステム400は、そして、ステップ631で、デバイストランザクションデータ678の少なくとも一部分（例えば、デバイス決済クレデンシャルデータ676のトークンデータ及び／又は暗号データ）を、（例えば、第1の販売事業者構成のための）販売事業者サブシステム200の好適な販売事業者鍵157で、又は（例えば、第2及び第3の販売事業者構成のための）PSPサブシステム310の好適な販売事業者鍵157で、暗号化された販売事業者クレデンシャルデータ681として再暗号化することができ、この好適な販売事業者鍵157は、データ678内に含まれ得る妥当性検査データの任意の好適な識別子データを用いて、かつ（例えば、ステップ606の間に規定され得るように、テーブル430内の）その識別子データに関連付けられた事前に記憶された関連付けを用いて、商業エンティティサブシステム400により識別され得る。例えば、暗号化された販売事業者クレデンシャルデータ681は、デバイストランザクションデータ678からの少なくとも暗号化されたデバイス決済クレデンシャルデータ676、ならびに、デバイストランザクションデータ678及び／又は潜在的トランザクションデータ660からの、又はそれに基づいた購入額データ又は他の好適なトランザクションデータなどの好適なトランザクションデータを含むことができる。暗号化された販売事業者クレデンシャルデータ681は、販売事業者サブシステム200又はPSPサブシステム310により受信されると、そのサブシステムがこのような暗号化された販売事業者クレデンシャルデータ681の作成者として商業エンティティサブシステム400を確立できるように、及び／又はそのサブシステムがこのような暗号化された販売事業者クレデンシャルデータ681が署名された後修正されていないことを確実にすることを可能とすることができるように商業エンティティサブシステム400により署名され得る。このような暗号化された販売

事業者クレデンシャルデータ681は、ステップ631で生成され、そして、ステップ632で、セキュアなトランザクションデータ682として他の好適なデータとともにデバイス100に（例えば、図1Aの経路65を介して商業エンティティサブシステム400のサーバ410からデバイス100の通信構成要素106に）送信されてもよい。

【0093】

ステップ631及びステップ632は、図1Aのセキュアなトランザクションデータ682の一部として商業エンティティサブシステム400から送信されたクレデンシャルデータ（例えば、暗号化された販売事業者クレデンシャルデータ681のトークンデータ及び／又は暗号データ）が、セキュアエレメント145以外のデバイス100の一部により解読できないように暗号化されてもよいことを確実にするように機能することができる。すなわち、セキュアなトランザクションデータ682のクレデンシャルデータ（例えば、暗号化された販売事業者クレデンシャルデータ681のトークンデータ及び／又は暗号データ）を、いくつかの実施形態では、セキュアエレメント145を含む、デバイス100のいかなる部分にも露出されていない、又は他の方法により、それによりアクセスできない販売事業者鍵（例えば、販売事業者鍵157）で暗号化することができる。また、セキュアなトランザクションデータ682のクレデンシャルデータ（例えば、暗号化された販売事業者クレデンシャルデータ681のトークンデータ及び／又は暗号データ）を、セキュアエレメント145の外部のデバイス100のいかなる部分にも露出していない、又はアクセスできないクレデンシャル鍵155a'で暗号化することができる。

【0094】

第1及び第2の販売事業者構成では、セキュアなトランザクションデータ682は、ステップ634で、セキュアなトランザクションデータ684として、デバイス100によって販売事業者サブシステム200に（例えば、通信経路15を介して、又は非接触近接型通信5として）転送されてもよいし、代替的に、販売事業者クレデンシャルデータ681は、デバイス100を介して通信されずに商業エンティティサブシステム400から販売事業者サブシステム200に通信されてもよい（図示せず）。潜在的トランザクションデータ660の1つ、一部又は全部を、デバイス100及び／又は商業エンティティサブシステム400を通して、セキュアなトランザクションデータ682及び／又はセキュアなトランザクションデータ684に搬送することができるので、潜在的トランザクションの特定の識別子は、プロセス600中にエンティティのそれぞれによって識別され得る。

【0095】

決済クレデンシャルデータ675／676を含む販売事業者クレデンシャルデータ681が販売事業者サブシステム200によって（例えば、ステップ634でセキュアなトランザクションデータ684として）受信されると、プロセス600はまた、販売事業者サブシステム200が決済データ686を生成し送信するように構成され得るステップ636も含むことができる。第1の販売事業者構成では、例えば、ステップ636では、販売事業者サブシステム200は、その既知の販売事業者鍵157を活用して、セキュアなトランザクションデータ684の販売事業者クレデンシャルデータ681を少なくとも部分的に解読することができるので、決済データ686は、金融機関サブシステム350にとって利用可能ではない鍵ではなく、そのクレデンシャル鍵155a'（例えば、データ676）で暗号化されたクレデンシャルSSD154aのセキュアな決済クレデンシャルデータを含むことができ、そして、そのようなデータ686を、販売事業者サブシステム200によって任意の好適なサブシステム（例えば、取得銀行サブシステム300及び／又はPSPサブシステム310）に通信することができる。代替的に、第2の販売事業者構成では、例えば、ステップ636で、販売事業者サブシステム200は、決済データ686として、セキュアなトランザクションデータ684の再暗号化された販売事業者クレデンシャルデータ681をPSPサブシステム310に転送することができ、そして、PSPサブシステム310は、その既知の販売事業者鍵157を活用して、少なくとも部分的に、決済データ686のその再暗号化された販売事業者クレデンシャルデータ681を解読することができる。代替的に、第3の販売事業者構成では、セキュアなトランザクショ

ンデータ682はデバイス100によってPSPサブシステム310に（例えば、デバイス100によって現在アクセスされ得るPSPオンラインリソースを使用して）転送されてもよく、そして、PSPサブシステム310はその既知の販売事業者鍵157を活用して、少なくとも部分的に、その転送されたセキュアなトランザクションデータの再暗号化された販売事業者クレデンシャルデータ681を解読することができる。プロセス600の残りの部分は、販売事業者サブシステム200及びPSPサブシステム310のうち適切なサブシステム（単数又は複数）が適切な販売事業者構成に従ってデータをデバイス100と通信しながら、ステップ638～ステップ644に関して上記したように進行することができる。

【0096】

図7の説明

図7は、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介した処理サブシステムに通信可能に結合された電子デバイスとの間のセキュアなトランザクションを行うために、管理エンティティサブシステムを使用するための例示的なプロセス700のフローチャートである。プロセス700のステップ702では、管理エンティティサブシステムは、オンラインリソースに対する妥当性検査要求を受信することができ、妥当性検査要求は、妥当性検査要求データを含むことができる（例えば、商業エンティティサブシステム400は、ステップ614でチャレンジ要求データ664を、及び／又はプロセス600のステップ620でチャレンジレスポンスデータ670を受信することができる）。プロセス700のステップ704では、管理エンティティサブシステムは、妥当性検査要求データ及び登録データを用いてオンラインリソースを妥当性検査することができ、登録データは、妥当性検査要求を受信する前に管理エンティティサブシステムにとって最初に利用できるようにすることができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ616で、チャレンジ要求データ664及びステップ606からの登録データを用いて、ならびに／又はプロセス600のステップ622で、チャレンジレスポンスデータ670及びステップ606からの登録データを用いて、オンラインリソース113を妥当性検査することができる）。プロセス700のステップ706では、管理エンティティサブシステムは、妥当性検査レスポンスデータを、妥当性検査要求データの少なくとも一部分と関連付けることができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ616及び／又はステップ622で識別子データに対して、妥当性検査データを関連付けることができる）。プロセス700のステップ708では、管理エンティティサブシステムは、妥当性検査レスポンスデータを電子デバイスに通信することができる（例えば、商業エンティティサブシステム400はプロセス600のステップ624で妥当性検査レスポンスデータ674の一部分としての妥当性検査データを電子デバイス100に通信することができる）。プロセス700のステップ710では、管理エンティティサブシステムは、電子デバイスからデバイストランザクションデータを受信することができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ628で電子デバイス100からデバイストランザクションデータ678を受信することができる）。プロセス700のステップ712では、管理エンティティサブシステムは、妥当性検査レスポンスデータを用いてデバイストランザクションデータを妥当性検査することができる（例えば、商業エンティティサブシステム400は、妥当性検査レスポンスデータ674を用いて、プロセス600のステップ630でデバイストランザクションデータ678の妥当性検査データを妥当性検査することができる）。プロセス700のステップ714では、デバイストランザクションデータが妥当性検査された後、管理エンティティサブシステムは、処理サブシステムに使用されるためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ631でデバイストランザクションデータ678に基づいて販売事業者クレデンシャルデータ681を生成することができる）。

【0097】

10

20

30

40

50

図7のプロセス700で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。

【0098】

図8の説明

図8は、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介して処理サブシステムに通信可能に結合された電子デバイスとの間で、セキュアなトランザクションを可能とするために、管理エンティティサブシステムを使用するための例示的なプロセス800のフローチャートである。プロセス800のステップ802では、管理エンティティサブシステムは、管理エンティティサブシステムと処理サブシステムとの間で処理する共有秘密を確立することによってオンラインリソースを登録することができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ606で販売事業者サブシステム200と共有秘密を確立することによってオンラインリソース113を登録することができる）。プロセス800のステップ804では、管理エンティティサブシステムはオンラインリソースに対する妥当性検査要求を受信することができ、妥当性検査要求はオンラインリソースを示す処理識別子を含むことができ、妥当性検査要求は、オンラインリソースを介した電子デバイスと処理サブシステムとの間の潜在的トランザクションに一意である妥当性検査セッション識別子を更に含むことができる（例えば、商業エンティティサブシステム400は、ステップ614で、販売事業者識別子及びセッション識別子を有するチャレンジ要求データ664を、ならびに／又はプロセス600のステップ620で、販売事業者識別子及びセッション識別子を有するチャレンジレスポンスデータ670を受信することができる）。プロセス800のステップ806では、管理エンティティサブシステムは、妥当性検査セッション識別子及び処理共有秘密を用いて、処理識別子が示すオンラインリソースを妥当性検査することができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ616でチャレンジ要求データ664及びステップ606からの登録データを用いて、及び／又は、プロセス600のステップ622で、チャレンジレスポンスデータ670及びステップ606から登録データを用いて、オンラインリソース113を妥当性検査することができる）。

【0099】

図8のプロセス800で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。

【0100】

図9の説明

図9は、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介した処理サブシステムに通信可能に結合された電子デバイスとの間のセキュアなトランザクションを行うために、管理エンティティサブシステムを使用するための例示的なプロセス900のフローチャートである。プロセス900のステップ902では、管理エンティティサブシステムはオンラインリソースに対する妥当性検査要求を受信することができ、妥当性検査要求は妥当性検査要求データを含むことができ、妥当性検査要求データは、オンラインリソースを介した電子装置と処理サブシステムとの間の潜在的トランザクションを示す潜在的トランザクション識別情報を含むことができる（例えば、商業エンティティサブシステム400は、ステップ614で、チャレンジ要求データ664を、及び／又はプロセス600のステップ620で、チャレンジレスポンスデータ670を受信することができる）。プロセス900のステップ904では、管理エンティティサブシステムは、妥当性検査要求データの少なくとも一部分を用いて、オンラインリソースを妥当性検査することができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ616でチャレンジ要求データ664を用いて、及び／又は、プロセス600のステップ622で、チャレンジレスポンスデータ670を用いて、オンラインリソース113を妥当性検査することができる）。プロセス900のステップ906では、管理エンテ

ィティサブシステムは、妥当性検査レスポンスデータを、少なくとも潜在的トランザクション識別情報と関連付けることができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ616及び／又はステップ622で潜在的トランザクション識別情報に対して、妥当性検査データを関連付けることができる）。プロセス900のステップ908では、管理エンティティサブシステムは、妥当性検査レスポンスデータを電子デバイスに通信することができる（例えば、商業エンティティサブシステム400はプロセス600のステップ624で妥当性検査レスポンスデータ674の一部としての妥当性検査データを電子デバイス100に通信することができる）。プロセス900のステップ910では、管理エンティティサブシステムは、電子デバイスからデバイストランザクションデータを受信することができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ628で電子デバイス100からデバイストランザクションデータ678を受信することができる）。プロセス900のステップ912では、管理エンティティサブシステムは、妥当性検査レスポンスデータ及び潜在的トランザクション識別情報を用いてデバイストランザクションデータを妥当性検査することができる（例えば、商業エンティティサブシステム400は、妥当性検査レスポンスデータ674及び潜在的トランザクション識別情報を用いて、プロセス600のステップ630でデバイストランザクションデータ678の妥当性検査データを妥当性検査することができる）。プロセス900のステップ914では、デバイストランザクションデータが妥当性検査された後、管理エンティティサブシステムは、処理サブシステムに使用されるためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することができる（例えば、商業エンティティサブシステム400は、プロセス600のステップ631でデバイストランザクションデータ678に基づいて販売事業者クレデンシャルデータ681を生成することができる）。

【0101】

図9のプロセス900で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。

【0102】

実施形態の更なる説明

デバイス100のセキュアエレメントのクレデンシャルが、トランザクションデータの決済クレデンシャルデータとして（例えば、非接触近接型通信として、販売事業者端末220に、及び／又はオンライン型の通信として、販売事業者サーバ210に）提供されるよう、適切にイネーブルされる（例えば、クレデンシャルSSD154aの可能にされたアプレット153aと関連付けられた商業クレデンシャルデータ）と、取得銀行サブシステム300は、金融機関サブシステム350との財務トランザクションを完了するために、このような決済クレデンシャルデータを利用することができる。例えば、デバイス100のユーザが購入する製品を選択し、決済に使用するデバイス100の特定のクレデンシャルを適切にイネーブルした後、販売事業者サブシステム200は、特定のクレデンシャルの決済クレデンシャルデータを示す決済クレデンシャルデータを受信することができる。販売事業者サーバ210及び／又は販売事業者端末220は、デバイス100が決済クレデンシャルデータを提供することに応じて、製品又はサービスをエンドユーザ用の電子デバイスのユーザに提供し得る好適な販売事業者又は販売事業者サブシステム200の販売事業者エージェントにより提供され得る。このような受信された決済クレデンシャルデータ（例えば、データ684として）に基づいて、販売事業者サブシステム200は、データ686を生成し、（例えば、販売事業者サブシステム200と取得銀行サブシステム300との間の通信経路25を介して）取得銀行サブシステム300に送信するように構成され得、データ686は、決済クレデンシャルデータと、デバイス決済クレデンシャル及び製品又はサービスの販売事業者の購入価格を示し得る許可要求を含むことができる。決済プロセッサ又は取得者としても知られる、取得銀行サブシステム300は、販売事業者サブシステム200に関連付けられた販売事業者の銀行パートナーであることができ、取

得銀行サブシステム300は金融機関サブシステム350と協働して、デバイス100が資金供給を試みたクレデンシャルトランザクションを、決済クレデンシャルデータによって承認及び決済するように構成され得る。そして、取得銀行サブシステム300は、（例えば、取得銀行サブシステム300と金融機関サブシステム350との間の通信経路35を介して）許可要求データ688として決済データ686からの許可要求を金融機関サブシステム350に転送することができる。

【0103】

決済ネットワークサブシステム360及び発行銀行サブシステム370は、単一のエンティティであってもよいし、又は別個のエンティティであってもよい。例えば、American Expressは、決済ネットワークサブシステム360と発行銀行サブシステム370の両方であってもよい。対照的に、Visa及びMasterCardは、決済ネットワーク360であってもよく、Chase、Wells Fargo、Bank of Americaなどの発行銀行370と連携して機能してもよい。金融機関サブシステム350はまた、取得銀行サブシステム300などの1つ以上の取得銀行も含むことができる。例えば、取得銀行サブシステム300は、発行銀行サブシステム370と同一のエンティティであってもよい。取得銀行サブシステム300の1つ、一部、又は全部の構成要素を、デバイス100のプロセッサ構成要素102と同一又は類似であり得る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と同一又は類似であり得る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と同一又は類似であり得る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。決済ネットワークサブシステム360の1つ、一部、又は全部の構成要素を、デバイス100のプロセッサ構成要素102と同一又は類似であり得る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と同一又は類似であり得る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と同一又は類似であり得る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。発行銀行サブシステム370の1つ、一部、又は全部の構成要素を、デバイス100のプロセッサ構成要素102と同一又は類似であり得る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と同一又は類似であり得る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と同一又は類似であり得る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。決済ネットワークサブシステム360と発行銀行サブシステム370が別々のエンティティである場合、決済ネットワークサブシステム360は、取得銀行サブシステム300からデータ690を受信することができ、そして、（例えば、決済ネットワークサブシステム360と発行銀行サブシステム370との間の通信経路45を介して）データ405として要求を発行銀行サブシステム370に転送することができる。決済ネットワークサブシステム360と発行銀行サブシステム370が同一のエンティティである場合、取得銀行サブシステム300は、データ690を直接発行銀行サブシステム370に提出することができる。更に、決済ネットワークサブシステム360は、（例えば、決済ネットワークサブシステム360と発行銀行サブシステム370との間に合意された条件に応じて）発行銀行サブシステム370の代わりに、取得銀行サブシステム300に応答することができる。取得銀行サブシステム300と発行銀行サブシステム370との間をインタフェースすることにより、決済ネットワークサブシステム360は、各取得銀行サブシステム300と各発行銀行サブシステム370と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。すなわち、金融機関サブシステム350の直接統合点を最小化するために、決済ネットワークサブシステム360は、種々の発行銀行370及び／又は種々の取得銀行300のためのアグリゲータの役割を果たすことができる。金融機関サブシステム350はまた、取得銀行サブシステム300などの1つ以上の取得銀行も含むことができる。例えば、取得銀行サブシステム300は、発行銀行サブシステム370と同一のエンティティであってもよい。

【0104】

発行銀行サブシステム370が（例えば、データ688として直接取得銀行サブシステ

10

20

30

40

50

ム300から、又はデータ405として間接的に決済ネットワークサブシステム360を介して)許可要求を受信すると、許可要求に含まれる決済情報(例えば、デバイス100の商業クレデンシャル情報)及び購入額は、商業クレデンシャルに関連付けられたアカウントが購入額をカバーするのに十分なクレジットを有するかを判定するように分析され得る。十分な資金が存在しない場合、発行銀行サブシステム370は、取得銀行サブシステム300に否定的許可レスポンスを送信することにより、要求されたトランザクションを断ることができる。しかし、十分な資金が存在する場合、発行銀行サブシステム370は、取得銀行サブシステム300に肯定的許可レスポンスを送信することにより、要求されたトランザクションを承認することができ、財務トランザクションを完了することができる。いずれかのタイプの許可レスポンスを、許可レスポンスデータ又はトランザクション状況データ690としてユーザ金融サブシステム350により取得銀行サブシステム300に提供することができる(例えば、通信経路45を介して発行銀行サブシステム370から決済ネットワークサブシステム360に提供され得る許可レスポンスデータ又はトランザクション状況データ415に基づいて、トランザクション状況データ690を、通信経路35を介して発行銀行サブシステム370から取得銀行サブシステム300に提供することができ、又はトランザクション状況データ690を決済ネットワークサブシステム360から取得銀行サブシステム300に提供することができる)。

10

【0105】

上述のように、図2に示すように、電子デバイス100には、非限定的に、音楽プレイヤー(例えば、カリフォルニア州クパチーノのアップル インコーポレイテッドにより供給可能なiPod(登録商標))、ビデオプレイヤー、静止画プレイヤー、ゲームプレイヤー、他のメディアプレイヤー、音楽レコーダ、ムービー若しくはビデオカメラ又はレコーダ、静止画カメラ、他のメディアレコーダ、ラジオ、医療用機器、家庭用若しくは商業用機器、輸送車両用計器、楽器、計算機、セルラ電話(例えば、アップル インコーポレイテッドにより供給可能な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、アップル インコーポレイテッドにより供給可能な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。いくつかの実施形態では、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、セキュアなデータトランザクションを行うために専小型電子デバイス用のデバイス)、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、セキュアなデータトランザクションを行い、音楽を再生し、電話呼出しを受信し、送信する)。電子デバイス100は、ユーザがどこを移動していても、財務トランザクションを行うように構成され得る、任意のポータブル、モバイル、ハンドヘルド、又は小型電子デバイスとすることができる。いくつかの小型電子デバイスは、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。例示する小型電子デバイスを、非限定的に、腕時計(例えば、アップル インコーポレイテッドによるApple Watch(登録商標))、リング、ネックレス、ベルト、ベルト用アクセサリ、ヘッドセット、靴用アクセサリ、仮想現実デバイス、眼鏡、他のウェアラブル電子機器、スポーツ用品用アクセサリ、フィットネス機器用アクセサリ、キーホルダ、又はそれらの任意の組合せを含みうる、種々の対象物に組み込むことができる。代替的に、電子デバイス100は、全く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。

20

30

40

【0106】

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、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はまた、デバイス100の他の種々の構成要素に、それらから、又はそれらの間に、データ及び/又は電力を転送するための1つ以上の有線若しくは無線通信リンク又

50

は経路を提供し得るバス118を含むことができる。いくつかの実施形態では、電子デバイス100の1つ以上の構成要素を組合せてもよいし、又は省略してもよい。また、電子デバイス100は、図2に組み合わされていない、又は含まれ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、図2に示す構成要素の任意の他の好適な構成要素又はいくつかのインスタンスを含むことができる。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。

【0107】

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得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内に固定して埋め込まれてもよいし、又は、電子デバイス100の中に反復的に挿入し、そこから取り出し得る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리카ード）に組み込まれてもよい。メモリ104には、メディアデータ（例えば、音楽及び画像ファイル）、（例えば、デバイス100上で機能を実施するための）ソフトウェア、ファームウェア、基本設定情報（例えば、メディア再生基本設定）、ライフスタイル情報（例えば、食の好み）、運動情報（例えば、運動監視機器により取得された情報）、トランザクション情報（例えば、クレジットカード情報などの情報）、無線接続情報（例えば、デバイス100が無線接続を確立するのを可能にし得る情報）、定期購読情報（例えば、ユーザが定期購読を受けているポットキャスト又はテレビ番組又は他のメディアを追跡記録する情報）、連絡先情報（例えば、電話番号及び電子メールアドレス）、カレンダー情報、任意の他の好適なデータ、又はそれらの組合せが含まれることができる。

【0108】

デバイス100が、任意の好適な通信プロトコルを用いて、1つ以上の他の電子デバイス又はサーバ又はサブシステム（例えば、1つ以上のサブシステム又はシステム1の他の構成要素）と通信できるように通信構成要素106を設けることができる。例えば、通信構成要素106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）、Ethernet、Bluetooth（登録商標）、BLE（Bluetooth（登録商標）Low Energy）、高周波数システム（例えば、900 MHz、2.4 GHz、及び5.6 GHz 通信システム）、赤外線、伝送制御プロトコル/インターネットプロトコル（「TCP/IP」）（例えば、TCP/IP層のそれぞれで使用されるプロトコルのいずれか）、ストリーム制御伝送プロトコル（「SCTP」）、動的ホスト構成プロトコル（「DHCP」）、ハイパーテキスト転送プロトコル（「HTTP」）、BitTorrent（登録商標）、ファイル転送プロトコル（「FTP」）、リアルタイム転送プロトコル（「RTP」）、リアルタイムストリーミングプロトコル（「RTSP」）、リアルタイム制御プロトコル（「RTCP」）、リモートオーディオ出力プロトコル（「RAOP」）、リアルデータ転送プロトコル（登録商標）（「RDTP」）、ユーザデータグラムプロトコル（「UDP」）、セキュアシェルプロトコル（「SSH」）、ワイヤレスディストリビューションシステム（「WDS」）ブリッジング、無線及び携帯電話ならびに個人用電子メールデバイス（例えば、移動通信用のグローバルシステム（「GSM（登録商標）」）、GSM（登録商標）プラスGSM（登録商標）進化型高速データレート（「EDGE」）、符号分割多元接続（「CDMA」）、直交周波数分割多元接続（「OFDMA」）、高速パケットアクセス（「HSPA」）、マルチバンドなど）が使用し得る任意の通信プロトコル、低電力無線パーソナルエリアネットワーク（「6LoWPAN」）モジュールが使用し得る任意の通信プロトコル、任意の他の通信プロトコル、又はそれらの組合せをサポートすることができる。通信構成要素106は、デバイス100が別のデ

10

20

30

40

50

バイス（例えば、ホストコンピュータ又はアクセサリデバイス）に通信可能に結合され、他のデバイスと無線又は有線接続（例えば、コネクタポートを用いて）通信するのを可能とする任意の好適な送受信機回路（例えば、送受信機回路又はバス118を介してアンテナ116）を含んでもよいし、又はそれに電氣的に結合されてもよい。通信構成要素106は、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、好適なインターネット接続）に好適なデータを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。通信構成要素106は、電子デバイス100の地理的位置を決定するように構成されてもよい。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又はWi-Fi技術を使用し得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。

10

【0109】

電源108は、電力を受信及び／又は生成し、電子デバイス100の1つ以上の他の構成要素にそのような電力を供給するために適切な回路を含むことができる。例えば、電源108を、（例えば、デバイス100がポータブルデバイスの役割を果たしていない場合、又はデバイスのバッテリーが電力プラントが発電した電力で電気コンセントに充電されているとき）電力グリッドに結合することができる。別の例として、電源108は、自然源（例えば、太陽電池を用いた太陽光）から電力を生成するように構成することができる。別の例として、電源108は、（例えば、デバイス100がポータブルデバイスの役割を果たすとき）電力を供給するための1つ以上のバッテリーを含むことができる。例えば、電源108は、バッテリー（例えば、ゲル、ニッケル金属水素化物、ニッケルカドミウム、ニッケル水素、鉛酸、又はリチウムイオンバッテリー）、無停電又は連続電源（「UPS」又は「CPS」）、及び発電源から受電した電力（例えば、電力プラントによって発電され、電気ソケット等を介してユーザに配電される電力）を処理する回路のうち1つ以上を含むことができる。電力は、電源108によって、交流又は直流として供給することができる。電力を変換し、又は受信した電力を特定の特性に制限するように処理することができる。例えば、電力を直流に、又は直流から変換することができ、平均電力、有効電力、ピーク電力、パルス当たりのエネルギー、電圧、（例えば、アンペアで測定された）電流、又は受信電力の他の特性の1つ以上の値に制約することができる。電源108は、（例えば、バッテリーが既に充電されているときよりもバッテリー充電中により多くの電力を要求するため）例えば、電子デバイス100又は電子デバイス100に結合され得る周辺デバイス周辺デバイスのニーズ又は要件に基づいて、異なる時間に特定の量の電力を要求又は提供するように機能することができる。

20

30

【0110】

1つ以上の入力構成要素110を、ユーザにデバイス100と相互作用させる又はインタフェースさせるために設けることができる。例えば、入力構成要素110は、限定されることなく、タッチパッド、ダイヤル、クリックホイール、スクロールホイール、タッチスクリーン、1つ以上のボタン（例えば、キーボード）、マウス、ジョイスティック、トラックボール、マイクロフォン、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(登録商標)などのコードから製品識別情報を取得し得る任意の他の好適なスキャナ）、接近センサ、光検出器、動きセンサ、バイオメトリックセンサ（例えば、ユーザを認証するために電子デバイス100にとってアクセス可能であり得る特徴処理アプリケーションとともに動作し得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。各入力構成要素110を、操作デバイス100に関連付けられた選択を行う、又はコマンドを発行するための1つ以上の専用制御機能を提供するように構成することができる。

40

【0111】

電子デバイス100はまた、デバイス100のユーザに情報（例えば、グラフィカル、聴覚、及び／又は触覚情報）を提示し得る1つ以上の出力構成要素112も含むことができる。例えば、電子デバイス100の出力構成要素112は、限定されることなく、オーディオスピーカ、ヘッドホン、オーディオラインアウト、視覚ディスプレイ、アンテナ、

50

赤外線ポート、触覚出力構成要素（例えば、ランブラー、バイブレータなど）、又はそれらの組合せを含む様々な形態をとることができる。

【0112】

具体例として、電子デバイス100は、出力構成要素112として表示出力構成要素を含むことができる。このような表示出力構成要素は、ユーザに視覚データを提示するための好適なタイプのディスプレイ又はインタフェースを含むことができる。表示出力構成要素は、デバイス100に埋め込まれるか、又はデバイス100（例えば、リムーバブルディスプレイ）に結合されたディスプレイを含むことができる。表示出力構成要素は、例えば、液晶ディスプレイ（「LCD」）、発光ダイオード（「LED」）ディスプレイ、有機発光ダイオード（「OLED」）ディスプレイ、表面伝導型電子放出素子ディスプレイ（「SED」）、カーボンナノチューブディスプレイ、ナノクリスタルディスプレイ、任意の他の適切なタイプのディスプレイ、又はそれらの組合せを含むことができる。代替的に、表示出力構成要素は、例えば、ビデオプロジェクタ、ヘッドアップディスプレイ、又は三次元（例えば、ホログラフィック）ディスプレイのような、電子デバイス100から離れた表面にコンテンツの表示を提供するための可動ディスプレイ又は投影システムを含むことができる。別の例として、表示出力構成要素は、コンパクトデジタルカメラ、レフカメラ、又は他の好適な静止又はビデオカメラで求められるタイプのビューファインダのようなデジタル又は機械式ビューファインダを含むことができる。表示出力構成要素は、ディスプレイドライバ回路、ディスプレイドライバを駆動する回路、又は両者を含むことができ、また、このような表示出力構成要素は、プロセッサ102の指示の下であり得るコンテンツ（例えば、メディア再生情報、電子デバイス100に実装されたアプリケーションのアプリケーション画面、通信中の動作に関する情報、入ってくる通信要求に関する情報、デバイス操作画面等）を表示するように機能することができる。

【0113】

ここで、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、入出力（「I/O」）構成要素又はI/Oインタフェースと総称する（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インタフェース114と総称する）場合があることを留意されたい。例えば、入力構成要素110及び出力構成要素112は、表示画面へのユーザのタッチにより入力情報を受信でき、また同一の表示画面を介してユーザに視覚情報を提供し得るタッチスクリーンのような単一のI/O構成要素114である場合がある。

【0114】

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性能を制御するように機能し得る任意の処理回路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、かつ／又は出力構成要素112を介し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のような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は、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低電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、又は他の好適なアプリケーションを含むことができるが、これらに限定されない。例えば、プロセッサ102は、ユーザインタフェースプログラムとしてアプリケーション103／113／143をロードし、情報が記憶され、及び／又は出力構成要素112を介してユーザに提供され得る方法を、入力構成要素110又はデバイス100の他の構成要素を介して受信された命令又はデータがどのように、操作し得るかを決定することができる。アプリケーション103／113／143は、プロセッサ102によって、メモリ104（例えば、バス118を介して）から、又は（例えば、通信構成要素106を介して）別のデバイス又はサーバからなどの、任意の適切なソースからアクセスされ得る。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、汎用及び特定目的用マイクロプロセッサ、命令セットプロセッサ、グラフィックスプロセッサ、ビデオプロセッサ、及び／又は関連チップセットの組合せ、及び／又は特定目的マイクロプロセッサを含むことができる。プロセッサ102はまた、キャッシュ目的のオンボードメモリを含むことができる。

【0115】

電子デバイス100はまた、近距離無線通信（「NFC」）構成要素120も含むことができる。NFC構成要素120は、電子デバイス100と販売事業者サブシステム200（例えば、販売事業者決済端末220）との間の非接触近接型トランザクション又は通信を可能とする任意の好適な近接型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、424kbp/s）での近接範囲通信を可能とすることができ、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。追加的に、又は代替的に、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販売事業者サブシステム200の間の通信は、おおよそ2～4センチメートルの範囲など、NFC構成要素と販売事業者サブシステム200の間における好適な任意の近接範囲距離（例えば、図1及び図1AにおけるNFC構成要素120と販売事業者決済端末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デバイスと通信し得ること及び／又は無線周波数識別（「RFID」）回路を有するタグから情報を取り出すことを可能にし得る、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、又は他の方法により外部デバイスと通信する（例えば、NFC構成要素120と販売事業者端末220の間で通信する）方法を提供することができる。

【0116】

NFC構成要素120は、電子デバイス100と販売事業者サブシステム200との間の非接触近接型通信を可能とする好適な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NFCメモリモジュール150を含むことができる。

【0117】

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データモジュール132は、非接触近接型又はNFC通信5の一部としてNFC構成要素120によって販売事業者サブシステム200に送信され得る好適なデータを収容し、経路設定し、又は他の方法により提供するように構成されてもよい。追加的に、又は代替的に、NFCデータモジュール132は、非接触近接型通信（例えば、NFC構成要素120と販売事業者端末220との間の通信5）の一部として販売事業者サブシステム200からNFC構成要素120によって受信され得る好適なデータを収容し、経路設定し、又は他の方法により受信するように構成されてもよい。

【0118】

NFC送受信機又はNFCアンテナ134は、NFCデータモジュール132から販売事業者サブシステム200への通信及び／又はサブシステム200からNFCデータモジュール132への通信の通信を一般的に可能にし得る任意の好適なアンテナ又は他の好適な送受信機回路とすることができる。したがって、特にNFC構成要素120の非接触近接型通信能力を可能とするために、NFCアンテナ134（例えば、ループアンテナ）を設けることができる。

【0119】

追加的に、又は代替的に、NFC構成要素120は、電子デバイス100の別の通信構成要素（例えば、通信構成要素106）が利用し得る、同一の送受信機回路又はアンテナ（例えば、アンテナ116）を利用することができる。例えば、通信構成要素106は、アンテナ116を活用して、電子デバイス100と他のリモートエンティティとの間のWi-Fi、Bluetooth（登録商標）、セルラ、又はGPS通信を可能とすることができ、NFC構成要素120は、アンテナ116を活用してNFCデバイスモジュール130のNFCデータモジュール132と別のエンティティ（例えば、販売事業者サブシステム200）との間の非接触近接型又はNFC通信を可能とすることができる。このような実施形態では、NFCデバイスモジュール130はNFCブースタ136を含むことができ、それは、NFC構成要素120のデータ（例えば、NFCデータモジュール132内のデータ）に対して適切な信号増幅を行うことで、そのようなデータが共有アンテナ116によってサブシステム200に通信として適切に送信され得るように構成され得る。例えば、電子デバイス100と販売事業者サブシステム200との間で非接触近接型又はNFC通信を通信するために、アンテナ116（例えば、非ループアンテナ）が正しくイネーブルされ得る前に、共有アンテナ116はブースタ136からの増幅を必要とする場合がある（例えば、アンテナ116を用いて他のタイプのデータを送信するのに必要とされるよりも、アンテナ116を用いてNFCデータを送信するのにより多くの電力が必要となる場合がある）。

10

【0120】

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、NFCデバイスモジュール130とともに動作し、電子デバイス100と販売事業者サブシステム200との間でNFC通信を通信するためのNFC構成要素120を可能とする、アクティブにする、許可する、及び／又は、他の方法により制御することができる。NFCプロセッサモジュール142は別個の構成要素として存在してもよいし、別のチップセットに統合されてもよいし、あるいは、例えば、システムオンチップ（「SOC」）の一部としてプロセッサ102と統合されてもよい。図2に示すように、NFCコントローラモジュール140のNFCプロセッサモジュール142は、NFC構成要素120の機能を命令するのに役立ちうるNFC低電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のに使用され得る。アプリケーション143は、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、NFC低電力アプリケーション、又はNFC構成要素120（例えばアプリケーション103／113）にとってアクセス可能となり得る任意の他の好適なアプリケーションを含むことができるが、これらに限定されない。NFCコントローラモジュール140は、別のNFCデバイス（例えば、販売事業者サブシステム200）と通信するための、近接場通信インタフェース及びプロトコル（「NFCIP-1」）などの1つ以上のプロトコルを含むことができる。プロトコルは、通信速度を適応させるとともに、接続されたデバイスのうち1つを近距離無線通信を制御するイニシエータデバイスに指定するのに使用され得る。

20

30

【0121】

NFCコントローラモジュール140はNFC構成要素120の近距離無線通信モードを制御することができる。例えば、NFCプロセッサモジュール142は、NFCタグから（例えば、販売事業者サブシステム200から）NFCデータモジュール132に情報（例えば、通信5）を読み出すためのリーダ／ライタモード、データ（例えば、通信5）を別のNFC可能化デバイス（例えば、販売事業者サブシステム200）と交換するためのピアツーピアモード、及び、別のNFC可能化デバイス（例えば、販売事業者サブシステム200）がNFCデータモジュール132から情報（例えば、通信5）を読み出すのを可能とするためのカードエミュレーションモード間でNFCデバイスモジュール130を切り替えるように構成されてもよい。NFCコントローラモジュール140は、NFC構成要素120をアクティブモードと受動モードとの間で切り替えるように構成されてもよい。例えば、NFCプロセッサモジュール142は、RFフィールドを生成する別のデ

40

50

バイス（例えば、販売事業者サブシステム200）にデータを転送するために、NFCデバイスモジュール130が自身のRFフィールドを生成することができるアクティブモードと、NFCデバイスモジュール130が負荷変調を用いることができる受動モードとの間で（例えば、NFCアンテナ134又は共有アンテナ116とともに）NFCデバイスモジュール130を切り替えるように構成され得る。このような受動モードでの動作は、このようなアクティブモードでの動作に比べて、電子デバイス100のバッテリー寿命を延ばすことができる。NFCデバイスモジュール130のモードは、デバイス100（例えば、アプリケーション103及び／又はアプリケーション143）上で実行されるアプリケーションによって定義され得るか、又は他の方法により命令され得る、ユーザの好みに基づいて、及び／又はデバイス100の製造業者の好みに基づいて、制御されてもよい。

10

【0122】

NFCメモリモジュール150は、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とともに動作し、電子デバイス100と販売事業者サブシステム200との間のNFC通信を可能とすることができる。NFCメモリモジュール150は、NFCデバイスハードウェア内又はNFC集積回路（「IC」）内に埋め込まれてもよい。NFCメモリモジュール150は、耐タンパ性であってもよく、セキュアエレメントの少なくとも一部分を提供してもよい。例えば、NFCメモリモジュール150は、NFCコントローラモジュール140によってアクセスされ得るNFC通信に関連付けられた1つ以上のアプリケーション（例えば、アプリケーション143）を記憶してもよい。例えば、このようなアプリケーションは、金融決済アプリケーション、セキュアアクセスシステムアプリケーション、ロイヤリティカードアプリケーション、及び他のアプリケーションを含むことができ、それは暗号化されてもよい。いくつかの実施形態では、NFCコントローラモジュール140及びNFCメモリモジュール150は、電子デバイス100上で感応アプリケーションを記憶及び実行するために使用されることを目的とするオペレーティングシステム、メモリ、アプリケーション環境、及びセキュリティプロトコルを含み得る専用マイクロプロセッサシステムを独立して、又は組合せて、提供することができる。NFCコントローラモジュール140及びNFCメモリモジュール150は、独立に又は組合せて、耐タンパ性であり得る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145は、識別され信頼された権限者の集合（例えば、金融機関サブシステム、及び／又は、Global Platformのような業界標準の権限者）によって定められ得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の機密及び暗号データ（例えば、アプレット153及び鍵155）をセキュアにホスティングすることが可能である耐タンパ性プラットフォームを（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）提供するように構成され得る。NFCメモリモジュール150は、メモリ104の一部分であってもよいし、又はNFC構成要素120に特有の少なくとも1つの専用チップであってもよい。NFCメモリモジュール150は、SIM上に、電子デバイス100のマザーボード上の専用チップ上に、又はメモリカード内の外部プラグとして常駐してもよい。NFCメモリモジュール150は、NFCコントローラモジュール140から完全に独立していてもよく、デバイス100の種々の構成要素によって提供されてもよく、及び／又は様々なリムーバブルサブシステムによって電子デバイス100に提供されてもよい。セキュアエレメント145は、機密データ又は電子デバイス100上のアプリケーションを記憶するために使用され得る、チップ内の高度にセキュアな、耐タンパ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(登録商標)」）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に使用され得る、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。追加的に、又は代替的に、デバイス100の製造中に電子デバイス100に埋め込まれ得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

20

30

40

50

けてもよい。追加的に、又は代替的に、電子デバイス100にプラグイン、挿入、又は他の方法により結合され得る、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。

【0123】

図2に示すように、NFCメモリモジュール150は、NFC仕様標準（例えば、GlobalPlatform）によって定義及び管理され得る、発行者セキュリティドメイン（「ISD」）152及び補足的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（「TSM」）等）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の一部とすることができ、その部分には、信頼されたサービスマネージャ（「TSM」）又は発行金融機関（例えば、商業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）が、クレデンシャル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つ以上のクレデンシャル（例えば、各種クレジットカード、銀行カード、ギフトカード、アクセスカード、交通パス、デジタル通貨（例えば、ビットコイン及び関連決済ネットワーク）などに関連付けられた商業クレデンシャル）を形成し、又は他の方法により、供給するための鍵及び／又は他の好適な情報を記憶することができる。特定の補足的セキュリティドメイン（「SSD」）154（例えば、SSD154a）を、特定のTSM及び、電子デバイス100に特定の特典又は決済権を提供し得る少なくとも1つの特定の商業クレデンシャル（例えば、特定のクレジットカードクレデンシャル又は特定の公衆交通カードクレデンシャル）と関連付けることができる。例えば、第1の決済ネットワークサブシステム360（例えば、Visa）は、第1のSSD154a用のTSMとすることができ、第1のSSD154aのアプレット153aは、その第1の決済ネットワークサブシステム360によって管理された商業クレデンシャルと関連付けられてもよく、第2の決済ネットワークサブシステム360（例えば、MasterCard）は、別のSSD154用のTSMとすることができる。

【0124】

NFC構成要素120の使用を可能とするため（例えば、デバイス100上に供給された商業クレデンシャルのアクティブ化を可能とするため）、クレデンシャルのクレジットカード情報又は銀行アカウント情報などの機密決済情報を電子デバイス100から販売事業者サブシステム200に送信する際に特に有用であり得るセキュリティ特徴を設けることができる。このようなセキュリティ特徴はまた、アクセスが制限され得るセキュアな記憶領域を含むことができる。（例えば、ユーザがセキュアエレメントのセキュリティドメインエレメントのライフサイクル状態を変更するため）セキュアな記憶領域にアクセスするために、例えば、個人識別番号（「PIN」）の入力を介した、又はバイオメトリックセンサとのユーザ相互作用を介したユーザ認証を設けることが必要とされ得る。特定の実施形態では、セキュリティ特徴の一部又は全部がNFCメモリモジュール150内に記憶されてもよい。更に、サブシステム200と通信するための認証鍵のようなセキュリティ情報を、NFCメモリモジュール150内に記憶してもよい。特定の実施形態では、NFCメモリモジュール150は、電子デバイス100内に埋め込まれたマイクロコントローラを含むことができる。

【0125】

図1Aの販売事業者サブシステム200の販売事業者端末220は、電子デバイス100からNFC通信（例えば、デバイス100が販売事業者端末220の特定の距離内に、又はその近傍に来たときの通信5）を検出し、読み取り、又は他の方法により受信するリーダを含むことができる。したがって、このような販売事業者端末と電子デバイス100との間のNFC通信が無線で生じ得ること、よって、各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。上述のように、NFCデバイスモジュール130は受動的であってもよいし、又はアクティブであってもよい。受動的であるとき、NFC

デバイスモジュール130は、このような販売事業者端末の好適なリーダの応答範囲内にある場合にのみアクティブ化することができる。例えば、このような販売事業者端末のリーダは、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特有のアンテナ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（例えば、クレジットカードクレデンシャル情報）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販売事業者端末にNFC通信として送信することを可能と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、又は他の方法により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特有のアンテナ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（例えば、クレジットカードクレデンシャル情報）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を介して販売事業者端末220にNFC通信としてアクティブに送信することを可能とすることができる。販売事業者端末220は、販売事業者サブシステム200の販売事業者により（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販売事業者のストアにて）提供され得る。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、好適な非接触近接型の任意のモバイル決済又は電子デバイス100とこのような販売事業者端末の間の他の好適な任意のタイプの非接触近接型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無線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。

【0126】

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、好適な非接触近接型の任意のモバイル決済又は電子デバイス100と販売事業者サブシステム200の間の他の好適な任意のタイプの非接触近接型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無線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。代替的に、いくつかの実施形態では、プロセッサ102又はデバイス100の任意の他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、販売事業者サブシステム200の販売事業者端末220との間の任意の好適な非接触近接型通信として通信することを可能とする任意の好適な構成要素を含むようにデバイス100のNFC構成要素120を構成することができるが、NFC構成要素120は、プロセス600のクレデンシャルデータのような、財務トランザクションにセキュアに資金供給するためにデバイス100上にセキュアなクレデンシャルデータを生成するクレデンシャルアプレットをセキュア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いし、含まなくてもよい。

【0127】

電子デバイス100は、デバイス100の外部のゴミ又は他の劣化力から保護するためデバイス100の構成要素のうち1つ以上を少なくとも部分的に囲み得る筐体101を備えることもできる。いくつかの実施形態では、構成要素の1つ以上を、自身の筐体内に設けることができる（例えば、入力構成要素110は、自身の筐体内に設けられ得るプロセッサ102と無線で、又は有線を通じて通信し得る、自身の筐体内の独立したキーボード又はマウスとすることができる）。互いに関連して動作する2つ以上のデバイス（例えば、好適な近接通信プロトコル（例えば、Bluetooth（登録商標））を介して通信可能に結合された携帯電話及びスマートウォッチ）の組合せとしていずれかのデバイス100を設けてもよいことを理解されたい。

【0128】

上述のように、かつ図3に示すように、電子デバイス100の特定の一例はiPhone（登録商標）のようなハンドヘルド型電子デバイスとすることができ、筐体101は、

デバイス100とユーザならびに／又は周辺環境とが互いにインタフェースし得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とすることができる。入力構成要素110aは、押下されると、デバイス100によって現在実行中のアプリケーションの「ホーム」画面又はメニューを表示させることができるボタンを含むことができる。入力構成要素110bは、スリープモードとウェークモードとの間で、又は他の好適なモード間で電子デバイス100をトグルするためのボタンとすることができる。入力構成要素110cは、電子デバイス100の特定の態様で1つ以上の出力構成要素112を不能にし得る2つの位置のスライダを含むことができる。入力構成要素110d、110eは、電子デバイス100の出力構成要素112のボリューム出力又は他の特性出力を増減させるためのボタンを含むことができる。入力構成要素110a～110eのそれぞれは、ドームスイッチ、スライドスイッチ、制御パッド、キー、ノブ、スクロールホイール、又は任意の好適な形態でサポートされたボタンなどの機械式入力構成要素とすることができる。

【0129】

出力構成要素112aは、ユーザが電子デバイス100と相互作用することを可能にし得る視覚的又はグラフィックユーザインタフェース（「GUI」）180を表示するために使用され得るディスプレイとすることができる。GUI180は、表示出力構成要素112aの領域の全部又は一部に表示され得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）の種々の層、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は、第1の画面190を表示するように構成されていてもよい。ユーザ入力構成要素110a～110iのうち1つ以上は、GUI180を介してナビゲートするのに使用され得る。例えば、1つのユーザ入力構成要素110は、ユーザがGUI180の1つ以上のグラフィック要素又はアイコン182を選択するのを可能とするスクロールホイールを含むことができる。アイコン182は、表示出力構成要素112a及び関連付けられたタッチ入力構成要素110fを含み得るタッチスクリーンI/O構成要素114aを介して選択されてもよい。このようなタッチスクリーンI/O構成要素114aは、限定されることなく、抵抗性、容量性、赤外線、弾性表面波、電磁、又は近接場撮像などの、任意の好適なタイプのタッチスクリーン入力技術を採用することができる。更に、タッチスクリーンI/O構成要素114aは、単一ポイント又はマルチポイント（例えば、マルチタッチ）入力感知を採用することができる。

【0130】

アイコン182は、種々の層、ウィンドウ、スクリーン、テンプレート、要素、及び／又はユーザによる選択の際に、表示構成要素112aの一部又は全部に表示され得る他の構成要素を表すことができる。更に、特定のアイコン182の選択は、階層ナビゲーションプロセスに導くことができる。例えば、特定のアイコン182の選択は、同じアプリケーションの、又はそのアイコン182と関連付けられた新しいアプリケーションの、1つ以上の追加アイコン又は他のGUI要素を含み得るGUI180の新しい画面に導くことができる。各グラフィカル要素アイコン181のユーザ解釈を容易にするために、各アイコン182上又はその近くにテキストインジケータ182を表示してもよい。GUI180は階層構造及び／又は非階層構造に配置された種々の構成要素を含んでもよいことを理解されたい。特定のアイコン182が選択されると、デバイス100は、そのアイコン182に関連付けられた新たなアプリケーションを開き、そのアプリケーションに関連付けられたGUI180の対応する画面を表示するように構成することができる。例えば、「Merchant 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）が選択されると、デバイス100は、特定の販売事業者アプリケーションを起動し、又は他の方法によりそのアプリケーションにアクセスしてもよく、特定の方法でデバイス100と相互作用する1つ以上のツール又は特徴を含み得る特定のユーザインタフェースの画面を表示することができる。各アプリケ

10

20

30

40

50

ーションのために、画面は表示出力構成要素 112 a 上に表示されてもよく、種々のユーザインタフェース要素（例えば、図 3 A～図 3 D の画面 190 a～190 d）を含むことができる。追加的に、又は代替的に、各アプリケーションに対して、他の種々のタイプの非視覚情報を、デバイス 100 の種々の他の出力構成要素 112 を介してユーザに提供してもよい。種々の GUI 180 に関して説明する動作は、幅広い種類のグラフィカル要素及び視覚的方式により実現されてもよい。したがって、説明する実施形態は、本明細書で採用するユーザインタ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、幅広い種類のユーザインタフェーススタイルを含んでもよい。

【0131】

電子デバイス 100 はまた、デバイス 100 と他のデバイスとの間の通信を可能にし得る種々の他の I/O 構成要素 114 も含むことができる。I/O 構成要素 114 b は、リモートデータソースからメディアファイル又は顧客注文ファイルなどのデータファイルを、及び／又は外部電源から電力を送受信するように構成され得る接続ポートとすることができる。例えば、I/O 構成要素 114 b は、カリフォルニア州クパチーノのアップルインコーポレイテッドからのライトニング（登録商標）コネクタ又は 30 ピンドックコネクタなど、専用のポートとすることができる。I/O 構成要素 114 c は、SIM カード又は任意の他のタイプのリムーバブル構成要素を受け入れるための接続スロットとすることができる。I/O 構成要素 114 d は、マイクロフォン構成要素を含んでもよいし、あるいは含まなくてもよいオーディオヘッドホンを接続するためのヘッドホンジャックとすることができる。電子デバイス 100 はまた、マイクロフォンなどの少なくとも 1 つのオーディオ入力構成要素 110 g と、オーディオスピーカなどの少なくとも 1 つのオーディオ出力構成要素 112 b とを含むことができる。

【0132】

電子デバイス 100 はまた、少なくとも 1 つの触知又は触覚出力構成要素 112 c（例えば、回転機）と、カメラ及び／又はスキャナ入力構成要素 110 h（例えば、ビデオ又はスチルカメラ、及び／又はバーコードスキャナ、又はバーコード、QR コード（登録商標）又は同様のものなどのコードから製品識別情報を取得し得る任意の好適なスキャナ）と、バイOMETリック入力構成要素 110 i（例えば、ユーザを認証するための電子デバイス 100 にとってアクセス可能となり得る特徴処理アプリケーションとともに動作し得る指紋リーダ又は他の特徴認識センサ）と、を含むこともできる。図 3 に示すように、バイOMETリック入力構成要素 110 i の少なくとも一部分を、入力構成要素 110 a 又はデバイス 100 の任意の他の好適な入力構成要素 110 に組み込んでもよいし、又は他の方法により、それと組合せてもよい。例えば、バイOMETリック入力構成要素 110 i は、ユーザが、入力構成要素 110 a をユーザの指で押すことによって機械式入力構成要素 110 a と相互作用する際にユーザの指の指紋をスキャンするように構成され得る指紋リーダとすることができる。別の例として、バイOMETリック入力構成要素 110 i は、タッチスクリーン I/O 構成要素 114 a のタッチ入力構成要素 110 f と組み合わせられ得る指紋リーダとすることができるので、バイOMETリック入力構成要素 110 i は、ユーザがユーザの指でタッチスクリーン入力構成要素 110 f を押圧するか、又は、それに沿ってスライドすることによってタッチスクリーン入力構成要素 110 f と相互作用する際、ユーザの指の指紋をスキャンするように構成することができる。また、上述のように、電子デバイス 100 は、アンテナ 116 及び／又はアンテナ 134（図 3 には示されない）を介してサブシステム 200 にとって通信可能にアクセス可能であり得る NFC 構成要素 120 を更に含むことができる。NFC 構成要素 120 を、少なくとも部分的に筐体 101 内に配置してもよく、また、NFC 構成要素 120 と関連付けられたアンテナの 1 つ以上の一般的な位置（例えば、アンテナ 116 及び／又はアンテナ 134 の一般的位置）を識別し得るマーク又はシンボル 121 を、筐体 101 の外面に設けることができる。

【0133】

図 1～図 9 に関して記載のプロセスの 1 つ、いくつか、又はすべてはそれぞれ、ソフトウェアによって実施され得るが、ハードウェア、ファームウェア、又はソフトウェア、ハ

10

20

30

40

50

ードウェア及びファームウェアのいずれかの組合せで実施されてもよい。これらのプロセスを実行する命令は、機械又はコンピュータ可読媒体上に記録された機械又はコンピュータ可読コードとして具現化されてもよい。いくつかの実施形態では、コンピュータ可読媒体は非一時的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コンピュータ可読媒体の例としては、読み出し専用メモリ、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、及びデータ記憶装置（例えば、図2のメモリ104及び／又はメモリモジュール150）が挙げられるが、これらに限定されない。他の実施形態では、コンピュータ可読媒体は非一時的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、一時的コンピュータ可読媒体は、コンピュータ可読コードが分散形式で記憶及び実行されるように、ネットワークに結合されたコンピュータシステムにわたって分散させることができる。例えば、一時的コンピュータ可読媒体を、任意の好適な通信プロトコルを用いて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、コンピュータ可読媒体を、（例えば、アプリケーション103の少なくとも一部分として、及び／又は、アプリケーション113の少なくとも一部分として、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）通信構成要素106を介して電子デバイス100に通信することができる）。このような一時的コンピュータ可読媒体は、搬送波又は他のトランスポート機構などの、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、又は変調されたデータ信号の他のデータを具現化することができ、任意の情報配信メディアを含むことができる。変調されたデータ信号は、信号内の情報を符号化するように設定又は変更された1つ以上の特性を有する信号とすることができる。

【0134】

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つ以上の特定のタスクを実行し得るか若しくは1つ以上の具体的な概要データタイプを実装し得る、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。

【0135】

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、又は他の方法によりシステム1のエンティティにとっ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いし、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

【0136】

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、モジュールのすべてを相互接続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。

10

【０１３７】

20

本開示は、この技術のそのような個人情報データを使用してユーザを利することができることを理解する。例えば、個人情報データは、ユーザがより興味があるものを絞ったコンテンツを配信するために使用することができる。したがって、そのような個人情報データの使用は、配信されるコンテンツの計算された制御を可能とする。更に、ユーザを利する個人情報データに関するその他の使用もまた、本開示により意図されている。

【０１３８】

本開示は、そのような個人情報データの収集、分析、開示、伝送、記憶、又はその他の使用に応答するエンティティは、確固たるプライバシーのポリシー及び／又はプライバシー慣行に従うであろうことを更に意図している。具体的には、そのようなエンティティは、個人情報データを秘密として厳重に保守するための業界又は政府の要件を満たすか又は上回るものとして一般に認識されている、プライバシーのポリシー及び慣行を実施し常に使用すべきである。例えば、ユーザからの個人情報は、そのエンティティの合法的かつ正当な使用のために収集されるべきであり、それらの合法的使用を除いて、共有又は販売されるべきではない。更には、そのような収集は、ユーザに告知して同意を得た後にのみ実施するべきである。更には、そのようなエンティティは、そのような個人情報データへのアクセスを保護して安全化し、その個人情報データへのアクセスを有する他者が、それらのプライバシーのポリシー及び手順を遵守することを確実にするための、あらゆる必要な措置を講じるであろう。更には、そのようなエンティティは、広く受け入れられているプライバシーのポリシー及び慣行に対する自身の遵守を証明するために、第三者による評価を自らが受けることができる。

30

40

【０１３９】

前述のことながらもかかわらず、本開示はまた、ユーザが、個人情報データの使用又は個人情報データへのアクセスを選択的に阻止する実施形態も企図している。すなわち、本開示は、そのような個人情報データへのアクセスを防止又は阻止するために、ハードウェア要素及び／又はソフトウェア要素を提供できると想到する。例えば、広告配信サービスの場合において、本技術は、ユーザが、サービスの登録の間、個人情報データの収集への参加の「オプトイン」又は「オプトアウト」を選択することを可能とするように構成することができる。別の実施例では、ユーザは、ターゲットコンテンツ配信サービスに位置情報を提供しないように選択することができる。更に別の例では、ユーザは正確な位置情報を提供しないが、位置領域情報の転送を許可することを選択することができる

50

【 0 1 4 0 】

説明するコンセプトの更なる用途

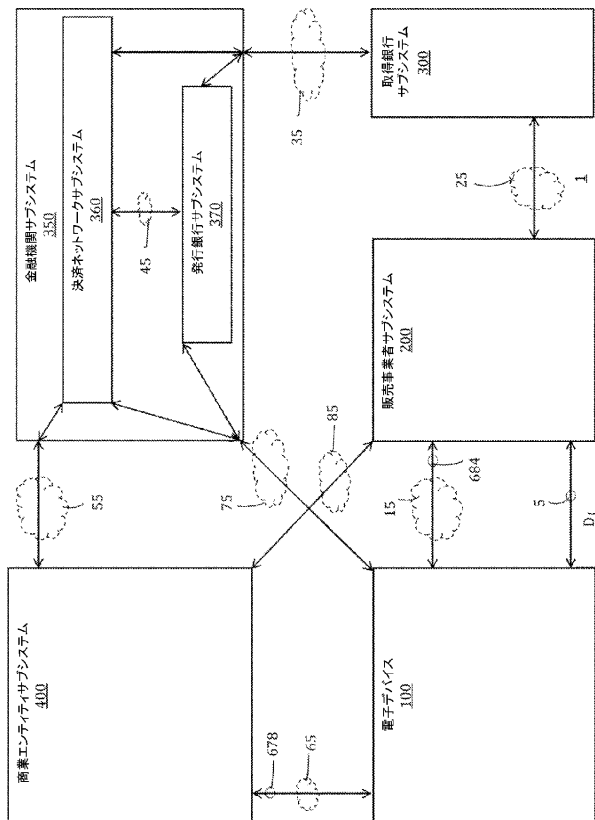
セキュアデバイス機能へのオンラインアクセスを妥当性検査するためのシステム、方法、及びコンピュータ可読媒体が記載されているが、本明細書に記載されている主題の趣旨及び範囲をいかなる方法でも逸脱せずに多くの変更を行うことができることを理解されたい。当業者から見て、特許請求された主題からの本質的でなく、現在既知であるか、又は今後で考案された変更は、特許請求の範囲内と均等であると明示的に考えられる。したがって、当業者に、現在既知であるか、又は今後既知となる明白な置換は、定義された要素の範囲内にあるものと定義される。

【 0 1 4 1 】

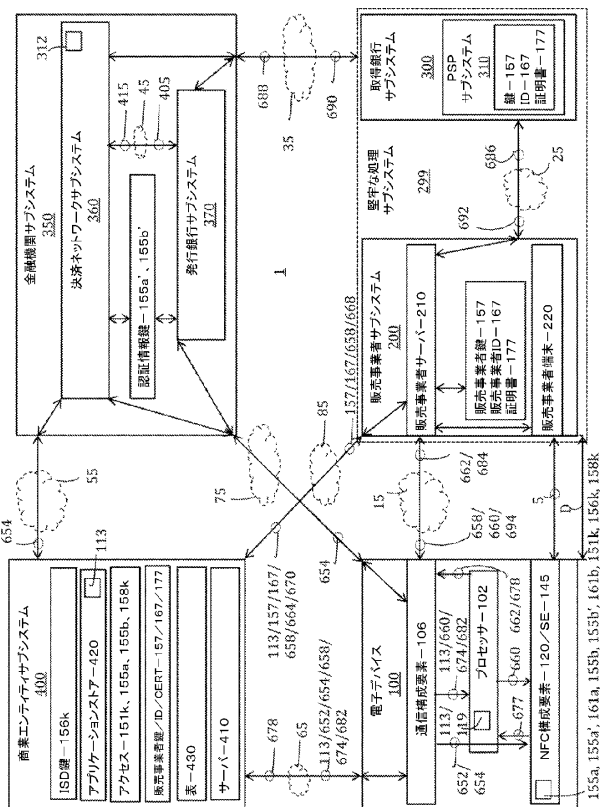
したがって、当業者は、限定ではなく例示を目的として提示される説明した実施形態とは異なる方法で本発明を実践できることを理解するであろう。

10

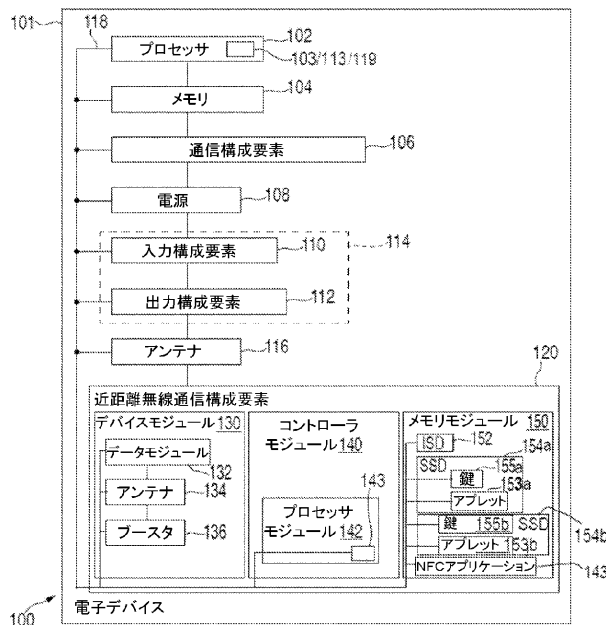
【図 1】



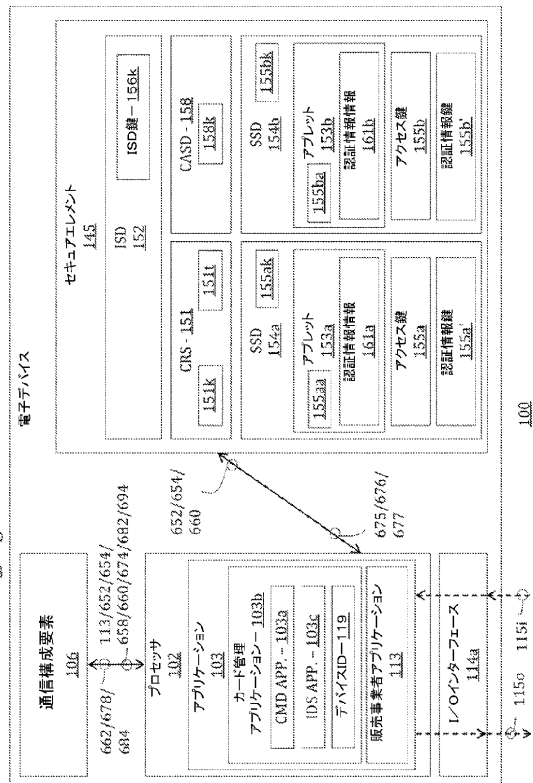
【図 1 A】



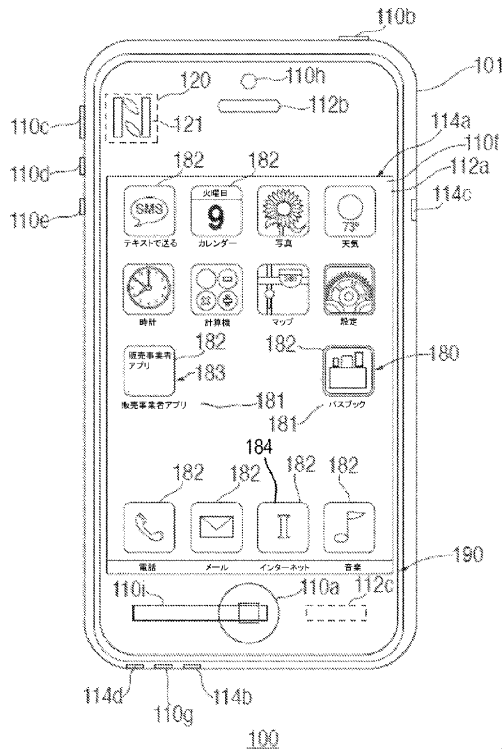
【図 2】



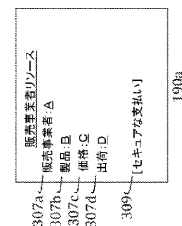
【図 2 A】



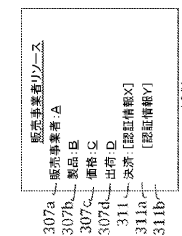
【図 3】



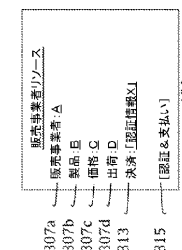
【図 3 A】



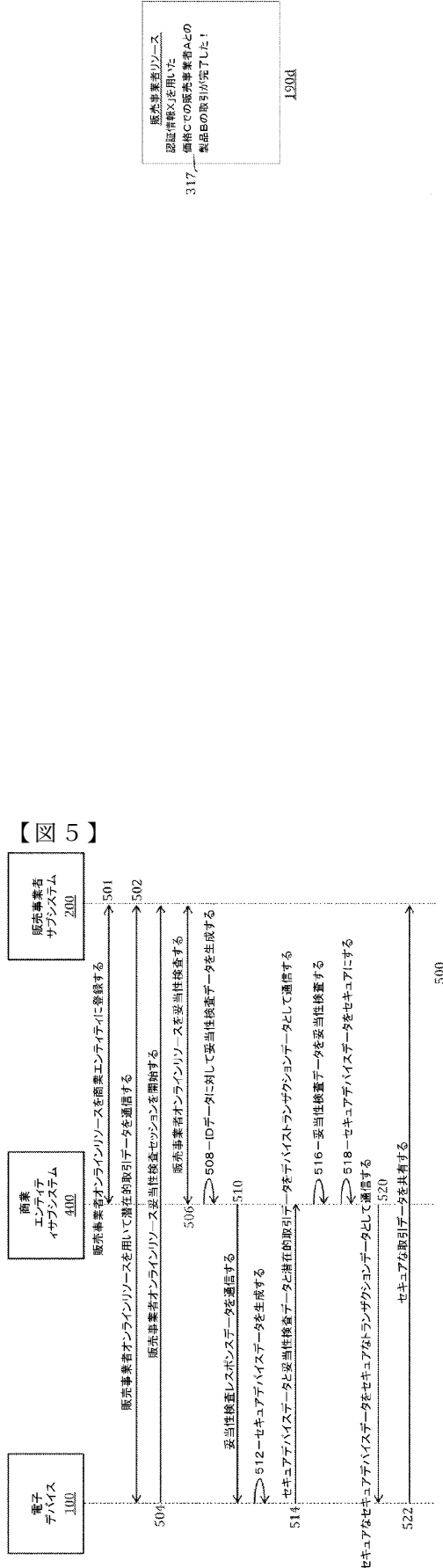
【図 3 B】



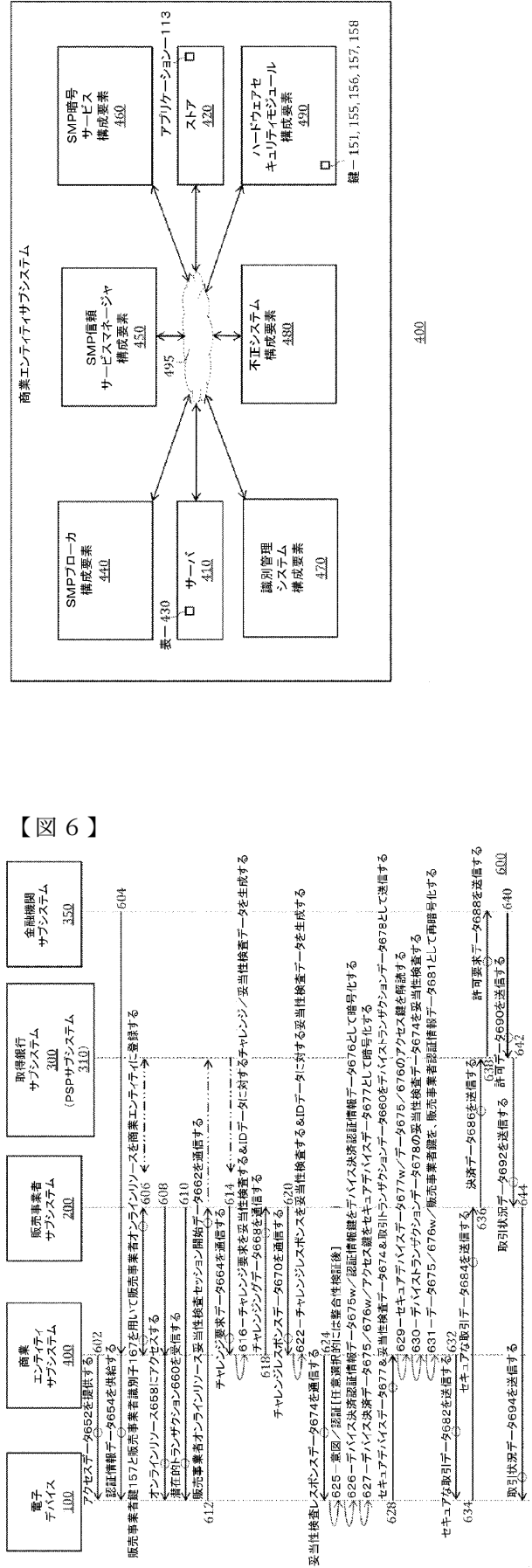
【図 3 C】



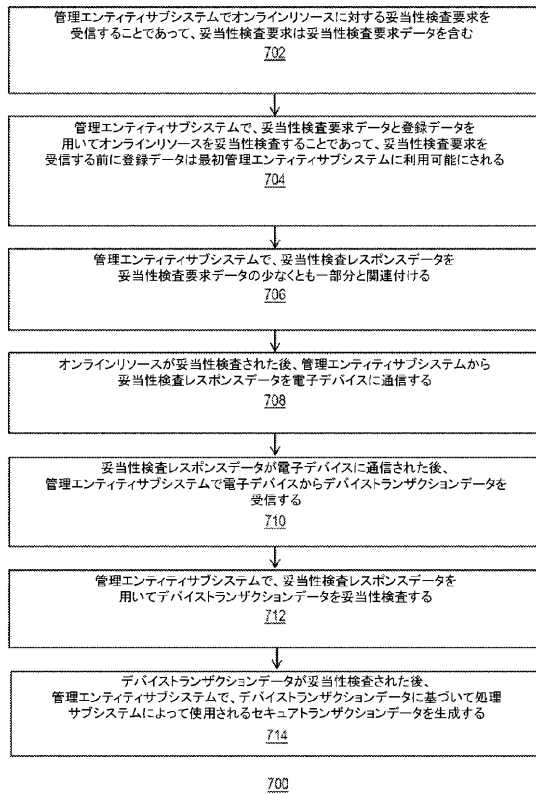
【図 3 D】



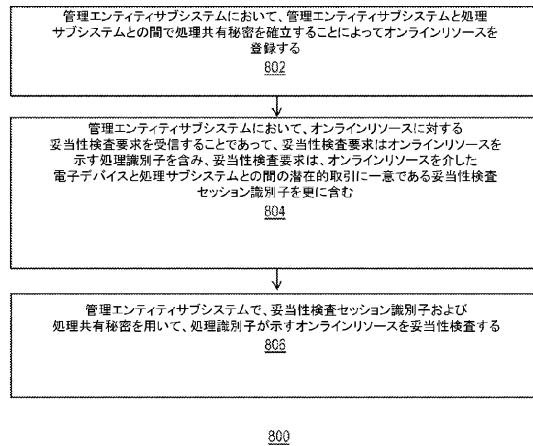
【図 4】



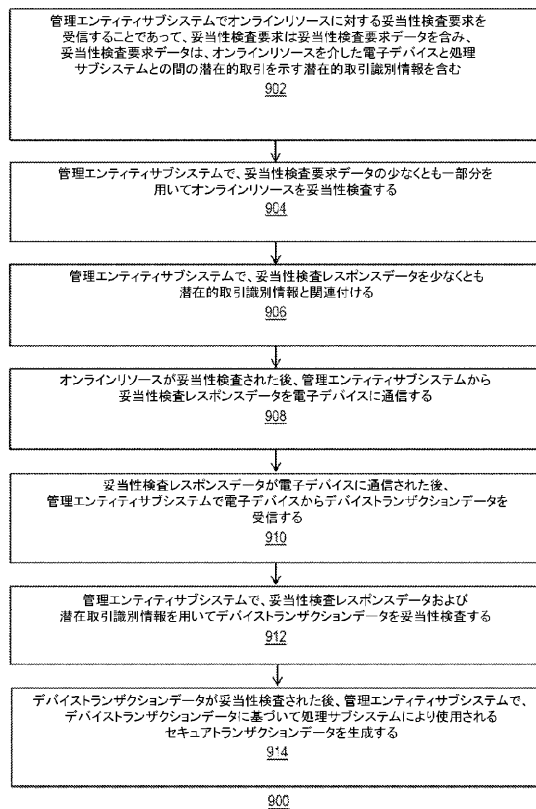
【図 7】



【図 8】



【図 9】



フロントページの続き

(31)優先権主張番号 62/348,960

(32)優先日 平成28年6月12日(2016.6.12)

(33)優先権主張国・地域又は機関
米国(US)

(31)優先権主張番号 15/275,122

(32)優先日 平成28年9月23日(2016.9.23)

(33)優先権主張国・地域又は機関
米国(US)

(31)優先権主張番号 62/348,979

(32)優先日 平成28年6月12日(2016.6.12)

(33)優先権主張国・地域又は機関
米国(US)

(74)代理人 100067013

弁理士 大塚 文昭

(74)代理人 100086771

弁理士 西島 孝喜

(74)代理人 100139712

弁理士 那須 威夫

(74)代理人 100122563

弁理士 越柴 絵里

(72)発明者 カールソン カール アンダース

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 ディードリッヒ アントン ケイ

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 シャープ クリストファー

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 ファソリ ジャンパオロ

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 スタチョウィアク マチエイ

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 バイイントン マシュー シー

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 シアラー ニコラス ジェイ

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 ウェイニグ サミュエル エム

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 金沢 史明

(56)参考文献 特表2013-539567(JP, A)

米国特許出願公開第2015/0019443(US, A1)

米国特許出願公開第2015/0095219(US, A1)

米国特許出願公開第2015/0088756(US, A1)

米国特許出願公開第2015/0371226(US, A1)

米国特許出願公開第2014/0289833(US, A1)

(58)調査した分野(Int.Cl., DB名)

H04L	9/32
G06F	21/44
G06F	21/60
G06Q	20/38