



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2024년12월31일

(11) 등록번호 10-2747890

(24) 등록일자 2024년12월24일

(51) 국제특허분류(Int. Cl.)
 G06Q 20/38 (2012.01) G06Q 20/22 (2012.01)
 G06Q 20/32 (2012.01) G06Q 20/40 (2012.01)
 H04L 9/32 (2006.01)

(52) CPC특허분류
 G06Q 20/3821 (2013.01)
 G06Q 20/2295 (2020.05)

(21) 출원번호 10-2024-7021968(분할)

(22) 출원일자(국제) 2017년01월25일

심사청구일자 2024년07월01일

(85) 번역문제출일자 2024년07월01일

(65) 공개번호 10-2024-0110090

(43) 공개일자 2024년07월12일

(62) 원출원 특허 10-2021-7021813

원출원일자(국제) 2017년01월25일

심사청구일자 2022년01월25일

(86) 국제출원번호 PCT/US2017/014965

(87) 국제공개번호 WO 2017/132273

국제공개일자 2017년08월03일

(30) 우선권주장

62/286,938 2016년01월25일 미국(US)

(뒷면에 계속)

(56) 선행기술조사문헌

JP3459376 B2*

(뒷면에 계속)

전체 청구항 수 : 총 9 항

심사관 : 이원재

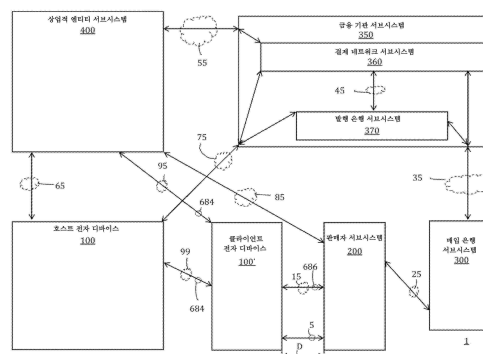
(54) 발명의 명칭 비-네이티브 크리덴셜들과 함께 전자 디바이스들을 사용하는 거래들의 수행

(57) 요약

비-네이티브 크리덴셜을 갖는 전자 디바이스를 사용하여 거래를 수행하기 위한 시스템, 방법 및 컴퓨터-관독가능 매체가 제공된다. 일 실시예에서, 크리덴셜 서브시스템, 프로세싱 서브시스템 및 호스트 전자 디바이스를 포함하는 시스템 내의 클라이언트 전자 디바이스는 온라인 통신 컴포넌트 및 프로세서를 포함할 수 있으며, 프로세서

(뒷면에 계속)

대 표 도 - 도1a



는 거래를 나타내는 잠재 거래 데이터를 프로세싱 서브시스템으로부터 액세스하고, 온라인 통신 컴포넌트를 사용하여 호스트 전자 디바이스에 잠재 거래 데이터에 기초한 크리덴셜 요청 데이터를 통신하고, 온라인 통신 컴포넌트를 사용하여 크리덴셜 요청 데이터에 기초하여 호스트 전자 디바이스로부터 호스트 크리덴셜 데이터를 수신하고, 프로세싱 서브시스템에 호스트 크리덴 데이터를 통신하고, 호스트 크리덴셜 데이터는 거래의 적어도 일부분을 지불하기 위해 크리덴셜 서브시스템으로부터 지불금 또는 다른 적합한 인에이블 요소들에 액세스하도록 동작한다. 추가적인 실시예들이 또한 제공된다.

(52) CPC특허분류

G06Q 20/3224 (2013.01)
G06Q 20/4015 (2023.05)
H04L 9/3263 (2013.01)
G06Q 2220/00 (2024.08)
H04L 2209/56 (2013.01)

(56) 선행기술조사문헌

KR100806993 B1*
 KR100949652 B1*
 KR101075891 B1*
 KR1020100075497 A*
 US20150058191 A1*
 US20150095219 A1
 US20150095238 A1*
 US20150348009 A1*
 US20150161587 A1*
 JP2015055952 A
 KR1020130021745 A
 KR1020130048647 A*
 KR1020150144363 A
 US20110289004 A1*

*는 심사관에 의하여 인용된 문헌

(30) 우선권주장

62/384,059 2016년09월06일 미국(US)
 62/348,958 2016년06월12일 미국(US)

명세서

청구범위

청구항 1

방법으로서,

클라이언트 전자 디바이스 및 호스트 전자 디바이스로부터 별개인 상업적 엔티티 서브시스템(commercial entity subsystem)에서:

상기 클라이언트 전자 디바이스로부터, 상기 클라이언트 전자 디바이스와 판매자 서브시스템(merchant subsystem) 간의 금융 거래(financial transaction)를 지불하기 위해 상기 판매자 서브시스템에 의해 수령가능한 적어도 하나의 결제 유형을 식별하는 호스트 이용가능성 요청(host availability request)을 수신하는 단계;

상기 호스트 전자 디바이스가 상기 클라이언트 전자 디바이스와 연관된다고 결정하는 단계;

상기 호스트 전자 디바이스가 상기 클라이언트 전자 디바이스와 연관된다는 상기 결정에 기초하여, 상기 호스트 전자 디바이스의 보안 요소(secure element) 상에 프로비저닝된(provisioned) 호스트 크리덴셜 애플리케이션(host credential application)이 상기 수신된 호스트 이용가능성 요청의 상기 식별된 적어도 하나의 결제 유형을 만족시킨다고 결정하는 단계;

상기 호스트 크리덴셜 애플리케이션이 상기 식별된 적어도 하나의 결제 유형을 만족시킨다는 상기 결정에 기초하여, 상기 호스트 전자 디바이스 상의 상기 호스트 크리덴셜 애플리케이션을 식별하는 호스트 이용가능성 응답(host availability response)을 상기 클라이언트 전자 디바이스에 송신하는 단계;

상기 호스트 이용가능성 응답에 응답하여 상기 클라이언트 전자 디바이스로부터, 상기 금융 거래에 대응하는 결제 요청 데이터를 수신하고 - 상기 결제 요청 데이터는 상기 호스트 크리덴셜 애플리케이션을 식별함 -, 상기 호스트 전자 디바이스에 상기 결제 요청 데이터를 송신하는 단계; 및

상기 판매자 서브시스템과의 상기 금융 거래를 수행하기 위해, 상기 결제 요청 데이터에 응답하여 상기 호스트 전자 디바이스로부터, 상기 송신된 결제 요청 데이터에 기초하여 상기 호스트 전자 디바이스에 의해 생성된 호스트 결제 크리덴셜 데이터를 포함하는 호스트 거래 데이터를 수신하고, 상기 클라이언트 전자 디바이스에 상기 호스트 거래 데이터를 송신하는 단계를 포함하는, 방법.

청구항 2

제1항에 있어서, 상기 호스트 이용가능성 응답은 상기 호스트 전자 디바이스의 상기 보안 요소 상에 프로비저닝된 상기 호스트 크리덴셜 애플리케이션을 식별하는 호스트 크리덴셜 애플리케이션 식별자 정보를 포함하는, 방법.

청구항 3

제1항에 있어서, 상기 호스트 이용가능성 응답은 상기 호스트 전자 디바이스의 현재 상태를 식별하는, 방법.

청구항 4

제1항에 있어서, 상기 호스트 이용가능성 응답은 상기 호스트 전자 디바이스의 현재 위치를 식별하는, 방법.

청구항 5

제1항에 있어서, 상기 호스트 이용가능성 응답은 상기 호스트 전자 디바이스의 현재 위치와 상기 클라이언트 전자 디바이스의 현재 위치 사이의 거리를 식별하는, 방법.

청구항 6

제1항에 있어서, 상기 호스트 전자 디바이스가 상기 클라이언트 전자 디바이스와 연관된다고 결정하는 단계는 상기 호스트 전자 디바이스 및 상기 클라이언트 전자 디바이스 둘 모두가 상기 상업적 엔티티 서브시스템의 특

정 사용자 계정과 연관된다고 결정하는 단계를 포함하는, 방법.

청구항 7

제1항에 있어서, 상기 호스트 전자 디바이스가 상기 클라이언트 전자 디바이스와 연관된다고 결정하는 단계는, 상기 호스트 전자 디바이스의 식별이 상기 클라이언트 전자 디바이스와 공유되는 것을 상기 호스트 전자 디바이스의 설정이 가능하게 한다고 결정하는 단계를 포함하는, 방법.

청구항 8

디바이스로서,

메모리; 및

제1항 내지 제7항 중 어느 한 항의 방법을 수행하도록 구성된 적어도 하나의 프로세서를 포함하는, 디바이스.

청구항 9

프로그램이 기록된 비일시적 컴퓨터 판독가능 기록매체로서,

상기 프로그램은, 하나 이상의 프로세서에 의해 실행될 때, 제1항 내지 제7항 중 어느 한 항의 방법을 포함하는 동작들을 수행하게 하는 명령어들을 포함하는, 비일시적 컴퓨터 판독가능 기록매체.

발명의 설명

기술 분야

[0001] 관련 출원에 대한 상호 참조

[0002] 본 출원은 각각이 전체적으로 본 명세서에 참고로 포함되는, 2016년 1월 25일자로 출원된 미국 가특허 출원 제 62/286,938호, 2016년 6월 12일자로 출원된 미국 가특허 출원 제 62/348,958호 및 2016년 9월 6일자로 출원된 미국 가특허 출원 제 62/384,059호의 우선권의 이익을 주장한다.

[0003] 기술분야

[0004] 본 발명은 비-네이티브 크리덴셜(non-native credential)과 함께 전자 디바이스를 사용하여 거래를 수행하는 것에 관한 것으로, 보다 상세하게는, 호스트 전자 디바이스로부터의 크리덴셜과 함께 클라이언트 전자 디바이스를 사용하여 거래를 수행하는 것에 관한 것이다.

배경 기술

[0005] 휴대용 전자 디바이스들(예컨대, 셀룰러 전화기들)에는, 다른 엔티티(예컨대, 판매자)와의 비접촉식 근접-기반 통신을 인에이블하기 위한 근거리 통신(near field communication, "NFC") 컴포넌트들이 제공될 수 있다. 종종, 이들 통신은 비접촉식 근접-기반 통신에서 전자 디바이스로 하여금 다른 엔티티와 신용 카드 크리덴셜과 같은 네이티브 결제 크리덴셜을 생성, 액세스 및/또는 공유하도록 요구하는 금융 거래들 또는 기타 보안 데이터 거래들과 연관된다. 그러나, 전자 디바이스에 의한 그러한 네이티브 결제 크리덴셜의 효율적인 사용은 다른 유형의 통신(예컨대, 온라인 금융 거래)에서는 종종 비효율적이었다.

발명의 내용

[0006] 본 문서는 비-네이티브 크리덴셜과 함께 전자 디바이스를 사용하여 거래를 수행하기 위한 시스템들, 방법들 및 컴퓨터-판독가능 매체들을 설명한다.

[0007] 예를 들어, 상업적 엔티티 서브시스템(subsystem), 클라이언트 전자 디바이스, 및 호스트 전자 디바이스 - 호스트 전자 디바이스는 보안 요소 및 보안 요소 상에 프로비저닝된(provisioned) 호스트 크리덴셜 애플리케이션을 포함함 - 를 사용하여 판매자 서브시스템과의 금융 거래를 수행하기 위한 방법은, 호스트 전자 디바이스에서, 클라이언트 전자 디바이스로부터 결제 요청 데이터를 수신하는 단계 - 결제 요청 데이터는 판매자 서브시스템을 식별하는 판매자 서브시스템 식별자 정보, 및 호스트 크리덴셜 애플리케이션을 식별하는 호스트 크리덴셜 애플리케이션 식별자 정보를 포함함 -, 보안 요소 상에, 수신된 결제 요청 데이터에 의해 식별된 호스트 크리덴셜 애플리케이션을 사용하여 호스트 결제 크리덴셜 데이터를 포함하는 제1 데이터를 생성하는 단계, 보안 요소 상

에, 제1 데이터 및 수신된 결제 요청 데이터의 판매자 서브시스템 식별자 정보를 제1 키를 이용하여 암호화함으로써 제2 데이터를 생성하는 단계, 상업적 엔티티 서브시스템에 제2 데이터를 송신하는 단계, 판매자 서브시스템 식별자 정보와 연관된 제2 키를 이용하여 암호화된 제1 데이터를 포함하는 제3 데이터를 수신하는 단계, 및 금융 거래의 적어도 일부분을 지불(fund)하기 위해, 수신된 제3 데이터를 송신하는 단계를 포함할 수 있다.

[0008] 다른 예로서, 클라이언트 전자 디바이스 및 호스트 전자 디바이스를 사용하여 판매자 서브시스템과의 금융 거래를 수행하기 위한 방법은, 클라이언트 전자 디바이스에서, 판매자 서브시스템으로부터 금융 거래를 나타내는 잠재 거래 데이터를 수신하는 단계; 수신된 잠재 거래 데이터에 기초하여 결제 요청 데이터를 호스트 전자 디바이스에 송신하는 단계; 송신된 결제 요청 데이터에 기초하여 호스트 전자 디바이스에 의해 생성된 호스트 결제 크리덴셜 데이터를 포함하는 호스트 거래 데이터를 수신하는 단계; 및 금융 거래의 적어도 일부분을 지불하기 위해, 수신된 호스트 거래 데이터의 호스트 결제 크리덴셜 데이터를 판매자 서브시스템에 송신하는 단계를 포함할 수 있다.

[0009] 다른 예로서, 상업적 엔티티 서브시스템, 클라이언트 전자 디바이스, 및 호스트 전자 디바이스 - 호스트 전자 디바이스는 보안 요소 및 보안 요소 상에 프로비저닝된 호스트 크리덴셜 애플리케이션을 포함함 - 를 사용하여 판매자 서브시스템과의 금융 거래를 수행하기 위한 방법은, 상업적 엔티티 서브시스템에서, 클라이언트 전자 디바이스로부터, 금융 거래를 지불하기 위해 판매자 서브시스템에 수령가능한(acceptable) 적어도 하나의 결제 유형을 식별하는 호스트 이용가능성(availability) 요청을 수신하는 단계; 호스트 전자 디바이스가 클라이언트 전자 디바이스와 연관된다는 결정에 기초하여, 호스트 전자 디바이스가 클라이언트 전자 디바이스와 연관된다고 결정하는 단계; 호스트 전자 디바이스의 보안 요소 상에 프로비저닝된 호스트 크리덴셜 애플리케이션이, 수신된 호스트 이용가능성 요청의 식별된 적어도 하나의 결제 유형을 만족시킨다고 결정하는 단계; 및 호스트 크리덴셜 애플리케이션이 식별된 적어도 하나의 결제 유형을 만족시킨다는 결정에 기초하여, 호스트 전자 디바이스를 식별하는 호스트 이용가능성 응답을 클라이언트 전자 디바이스에 송신하는 단계를 포함할 수 있다.

[0010] 또 다른 예로서, 금융 기관 서브시스템, 판매자 서브시스템 및 호스트 전자 디바이스를 포함하는 시스템 내의 클라이언트 전자 디바이스는 온라인 통신 컴포넌트 및 프로세서를 포함할 수 있으며, 프로세서는 온라인 통신 컴포넌트를 사용하여 판매자 서브시스템으로부터 금융 거래를 나타내는 잠재 거래 데이터에 액세스하고, 온라인 통신 컴포넌트를 사용하여, 잠재 거래 데이터에 기초하여 결제 요청 데이터를 호스트 전자 디바이스에 통신하고, 온라인 통신 컴포넌트를 사용하여 호스트 전자 디바이스로부터 결제 요청 데이터에 기초한 호스트 결제 크리덴셜 데이터를 수신하고, 온라인 통신 컴포넌트를 사용하여 판매자 서브시스템에 호스트 결제 크리덴셜 데이터를 통신하며, 호스트 결제 크리덴셜 데이터는 금융 거래의 적어도 일부분을 지불하기 위해 금융 기관 서브시스템으로부터의 지불금에 액세스하도록 동작한다.

[0011] 또 다른 예로서, 적어도 하나의 프로그램을 저장하는 비일시적 컴퓨터 판독가능 저장 매체가 제공될 수 있으며, 적어도 하나의 프로그램은, 사용자 인터페이스 출력 컴포넌트를 포함하는 전자 디바이스에 의해 실행될 때, 전자 디바이스로 하여금 잠재 거래를 지불하기 위해 판매자 서브시스템에 수령가능한 적어도 하나의 결제 유형을 식별하고, 식별된 적어도 하나의 결제 유형을 나타내는 호스트 이용가능성 요청 데이터를 송신하고, 호스트 이용가능성 요청 데이터에 기초하여 다른 전자 디바이스로부터의 호스트 이용가능성 응답 데이터를 프로세싱하고, 프로세싱에 응답하여, 사용자 인터페이스 출력 컴포넌트를 사용하여, 다른 전자 디바이스로의 결제 요청 데이터의 송신을 개시하도록 동작하는 사용자-선택가능한 옵션을 제시하게 하는 명령어를 포함한다.

[0012] 또 다른 예로서, 클라이언트 전자 디바이스 및 호스트 전자 디바이스를 사용하여 서비스 제공자 서브시스템과 거래를 수행하는 방법이 제공될 수 있다. 방법은, 클라이언트 전자 디바이스에서, 서비스 제공자 서브시스템의 제품에 대한 액세스를 구매하기 위해 거래의 적어도 일부분을 정의하기 위해 서비스 제공자 서브시스템과 통신하는 단계, 및 거래를 지불하기 위한 거래 크리덴셜을 생성하기 위해 호스트 전자 디바이스를 관여하게 하는 단계를 포함할 수 있다.

[0013] 본 발명의 내용은 단지 본 문서에 기술된 주제의 일부 양태들에 대한 기본적인 이해를 제공하도록 일부 예시적인 실시예들을 요약하기 위해서 제공될 뿐이다. 따라서, 본 발명의 내용에서 기술된 특징들은 단지 예시일 뿐이고 본 명세서에 설명된 주제의 범주 또는 기술적 사상을 어떤 방식으로든 한정하도록 해석되어서는 안된다는 것이 이해될 것이다. 달리 언급되지 않는 한, 일례의 문맥에서 설명된 특징은 하나 이상의 다른 예와 관련하여 기술된 특징과 결합되거나 사용될 수 있다. 본 명세서에 기술되는 주제의 다른 특징들, 양태들 및 이점들은 다음의 상세한 설명, 도면 및 청구범위로부터 명백해질 것이다.

도면의 간단한 설명

- [0014] 이하의 논의는 하기 도면들을 참조하며, 도면들에서 유사한 참조 부호들은 전체에 걸쳐 유사한 부분들을 지칭한다.
- 도 1은 거래를 수행하기 위한 예시적인 시스템의 개략도이다.
- 도 1a는 도 1의 시스템의 보다 상세한 개략도이다.
- 도 1b는 도 1 및 도 1a의 시스템의 다른 보다 상세한 개략도이다.
- 도 2는 도 1 내지 도 1b의 시스템의 전자 디바이스의 보다 상세한 개략도이다.
- 도 2a는 도 1 내지 도 2의 전자 디바이스의 다른 보다 상세한 개략도이다.
- 도 3은 도 1 내지 도 2a의 전자 디바이스의 정면도이다.
- 도 3a 내지 도 3h는 거래를 수행하기 위한 프로세스들을 예시하는 도 1 내지 도 3 중 하나 이상의 전자 디바이스의 그래픽 사용자 인터페이스의 스크린의 정면도이다.
- 도 4는 도 1 내지 도 1b의 시스템의 상업적 엔티티 서브시스템의 보다 상세한 개략도이다.
- 도 5 내지 도 10은 거래를 수행하기 위한 예시적인 프로세스들의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 크리덴셜-인에이블된(또는 결제-인에이블된) 호스트 전자 디바이스의 보안 요소 상에 프로비저닝된 크리덴셜(예컨대, 결제 크리덴셜 또는 임의의 다른 적합한 거래 크리덴셜)은 판매자 서브시스템과 인터페이싱하고 있을 수 있는 클라이언트 전자 디바이스를 통해 판매자(또는 서비스 제공자 또는 프로세서) 서브시스템과의 거래(예컨대, 금융 거래 또는 임의의 다른 적합한 크리덴셜 거래)를 안전하게 지불하거나 그렇지 않으면 수행하는 데 사용될 수 있다. 판매자 제품에 액세스(예컨대, 구매)하기 위하여 판매자 서브시스템과 인터페이싱하는 동안(예컨대, 온라인 리소스(예컨대, 온라인 애플리케이션 또는 웹 브라우저)를 통하거나 비접촉식 근접-기반 통신 매체를 포함), 클라이언트 디바이스는 호스트 디바이스를, 판매자 제품에 액세스하기 위한 거래를 지불하거나 그렇지 않으면 더 진행하는 데 사용될 크리덴셜의 요구되는 소스로 식별할 수 있다. 이어서, 클라이언트 디바이스는 지불될 거래를 나타낼 수 있는 크리덴셜(또는 결제) 요청(예컨대, 판매자, 구매될 제품(들), 거래의 비용, 거래의 화폐(currency), 거래의 배송 주소 등을 나타내는 데이터)을 식별된 호스트 디바이스에 전송할 수 있다. 호스트 디바이스가 결제 요청을 수신하는 것에 응답하여, 그리고 호스트 디바이스의 사용자가 요청을 승인한 후에, 호스트 디바이스 상에 프로비저닝된 크리덴셜(예컨대, 결제 크리덴셜)에 대한 특정 크리덴셜 데이터(예컨대, 토큰 데이터 및 연관된 암호화 데이터(crypto data))가 호스트 디바이스의 보안 요소에 의해 제공될 수 있고, 거래를 지불하기 위해, 호스트 디바이스로부터 클라이언트 디바이스로, 또는 판매자 서브시스템으로, 또는 금융 기관(또는 발행 또는 크리덴셜) 서브시스템으로 임의의 다른 적합한 거래 정보(예컨대, 판매자, 구매될 제품(들), 거래의 비용, 거래의 화폐, 거래의 배송 주소 등을 나타내는 데이터)와 함께 안전하게 통신될 수 있다. 그러한 크리덴셜 데이터는 호스트 전자 디바이스와 판매자 서브시스템 간에 직접 공유되지 않을 수 있다. 대신에, 클라이언트 디바이스는 호스트 디바이스로부터 크리덴셜 데이터를 수신할 수 있고 이어서, 클라이언트 디바이스는 크리덴셜 데이터를 판매자 서브시스템과 공유할 수 있다. 클라이언트 디바이스는, 클라이언트 디바이스와 연관되거나 연관되지 않을 수 있는 다양한 호스트 디바이스의 다양한 크리덴셜의 상태를 모니터링하도록 동작할 수 있는 상업적(또는 행정적 또는 신뢰) 엔티티 서브시스템의 아이덴티티 관리 서비스를 레버리지(leverage)하는 것을 포함하는 임의의 적합한 기술들을 사용하여 호스트 디바이스를 식별하고 그와 통신할 수 있다.
- [0016] 도 1에 도시된 시스템(1)에서, 호스트 전자 디바이스(100) 상에 프로비저닝된 크리덴셜은, 아마도 행정적(또는 상업적 또는 신뢰) 엔티티 서브시스템(400)과 공조하여 클라이언트 전자 디바이스(100')를 통해 또는 클라이언트 전자 디바이스(100')의 요청 시, 서비스 제공자(또는 판매자 또는 프로세서) 서브시스템(200)과의 거래를 수행하기 위해 호스트 전자 디바이스(100)에 의해 사용될 수 있다. 도 1a 및 도 1b에 더 상세하게 도시된 시스템(1)에서, 하나 이상의 크리덴셜은 상업적(또는 행정적 또는 신뢰) 엔티티 서브시스템(400)과 공조하여 금융 기관(또는 발행 또는 크리덴셜) 서브시스템(350)으로부터 호스트 전자 디바이스(100) 상에 프로비저닝될 수 있고, 그러한 크리덴셜들은 클라이언트 전자 디바이스(100')를 통해 또는 클라이언트 전자 디바이스(100')의 요청 시,

판매자(또는 서비스 제공자 또는 프로세서) 서브시스템(200) 및 연관된 매입(acquiring) 서브시스템(300)(예컨대, 매입 은행 서브시스템)과의 거래를 수행하기 위해 호스트 전자 디바이스(100)에 의해 사용될 수 있고, 도 2 내지 도 3은 시스템(1)의 하나 이상의 전자 디바이스의 특정 실시예들에 관한 추가의 상세사항을 도시하며, 도 3a 내지 도 3h는 그러한 거래 동안 시스템(1)의 하나 이상의 전자 디바이스의 그래픽 사용자 인터페이스들의 대표적인 수 있는 예시적인 스크린들(190a 내지 190h)을 도시하고, 도 4는 시스템(1)의 상업적 엔티티 서브시스템(400)의 특정 실시예들에 관한 추가의 상세사항을 도시하며, 도 5 내지 도 10은 그러한 거래를 수행하기 위한 예시적인 프로세스들의 흐름도들이다.

[0017] 도 1의 설명

[0018] 도 1은 클라이언트 전자 디바이스를 통해 또는 클라이언트 전자 디바이스의 요청 시 서비스 제공자(또는 판매자 또는 프로세서)와의 거래(예컨대, 온라인 결제 또는 비접촉식 근접-기반 결제)에서 호스트 전자 디바이스 상의 크리덴셜의 보안 사용을 허용할 수 있는 예시적인 시스템(1)의 개략도이다. 예를 들어, 도 1에 도시된 바와 같이, 시스템(1)은 최종 사용자(end-user) 호스트 전자 디바이스(100) 상에(예컨대, 호스트 전자 디바이스(100)의 보안 요소 상에) 프로비저닝된 적어도 하나의 크리덴셜을 구비한 최종 사용자 호스트 전자 디바이스(100), 최종 사용자 클라이언트 전자 디바이스(100') 상에 프로비저닝된 적어도 하나의 크리덴셜을 갖거나 갖지 않을 수 있는 최종 사용자 클라이언트 전자 디바이스(100'), 행정적(또는 상업적 또는 신뢰) 엔티티 서브시스템(400) 및 서비스 제공자(또는 판매자 또는 프로세서) 서브시스템(200)을 포함할 수 있다. 호스트 전자 디바이스(100), 클라이언트 전자 디바이스(100'), 서비스 제공자 서브시스템(200) 및 행정적 엔티티 서브시스템(400) 중 임의의 2개 사이의 임의의 적합한 데이터의 통신이 임의의 적합한 통신 설정(set-up)(9)을 통해 인에이블될 수 있으며, 이는 임의의 적합한 통신 프로토콜(들) 및/또는 임의의 적합한 네트워크 및/또는 클라우드 아키텍처(들)를 사용하여 임의의 적합한 유선 통신 경로, 무선 통신 경로, 또는 둘 이상의 유선 및/또는 무선 통신 경로의 조합을 포함할 수 있다.

[0019] 크리덴셜(예컨대, 결제 크리덴셜 또는 임의의 다른 적합한 거래 크리덴셜)은 임의의 적합한 크리덴셜 발행 서브시스템(예컨대, 금융 기관 서브시스템)으로부터 호스트 전자 디바이스(100) 상에(예컨대, 호스트 전자 디바이스(100)의 보안 요소 또는 다른 저장 컴포넌트 상에) 프로비저닝될 수 있으며, 크리덴셜 발행 서브시스템으로부터 직접, 또는 크리덴셜 데이터를 호스트 디바이스(100)에 안전하게 통신하고 그러한 크리덴셜 데이터를 관리하도록 동작할 수 있는 행정적 엔티티 서브시스템(400)을 통해 프로비저닝될 수 있다. 거래 크리덴셜은 호스트 디바이스(100) 상에 프로비저닝되면, 이어서, 서비스 제공자 서브시스템(200)(예컨대, 거래의 일부로서 임의의 적합한 상품 또는 서비스에 대한 액세스를 제공하도록 동작할 수 있는 임의의 적합한 서브시스템)과의 거래(예컨대, 금융 거래 또는 임의의 다른 적합한 크리덴셜 거래)를 안전하게 지불하거나 그렇지 않으면 수행하기 위해 호스트 디바이스(100)에 의해 사용될 수 있으며, 서비스 제공자 서브시스템(200)과 인터페이싱 중일 수 있는 클라이언트 디바이스(100')를 통해, 또는 서비스 제공자 서브시스템(200)과 거래를 개시했을 수 있는 클라이언트 디바이스(100')를 대신하여 사용될 수 있다.

[0020] 예를 들어, 서비스 제공자 제품에 액세스(예컨대, 구매)하기 위하여 서비스 제공자 서브시스템(200)과 인터페이싱하는 동안(예컨대, 온라인 리소스(예컨대, 온라인 애플리케이션 또는 웹 브라우저)를 통하거나 비접촉식 근접-기반 통신 매체를 통한), 클라이언트 디바이스(100')는 호스트 디바이스(100)를, 서비스 제공자 제품에 액세스하기 위한 거래를 지불하거나 그렇지 않으면 더 진행하는 데 사용될 거래 크리덴셜의 요구되는 소스로 식별할 수 있다. 클라이언트 디바이스(100')는 거래를 지불하는데 사용하기 위한 거래 크리덴셜을 저장하거나 그렇지 않으면 프로비저닝하도록 구성될 수 없는 유형의 디바이스(예컨대, 클라이언트 디바이스(100')는 결제 크리덴셜을 안전하게 활용하도록 동작하는 보안 요소를 포함하지 않을 수 있음), 또는 거래 크리덴셜을 저장하도록 구성되지만, 클라이언트 디바이스(100')에 의해 개시된 특정 거래에서 사용되도록 요구되는 특정 크리덴셜을 현재 저장하지 않은 유형의 디바이스일 수 있다. 예를 들어, 서비스 제공자 서브시스템(200)의 제품에 액세스하기 위해 거래를 정의하기 위한 클라이언트 디바이스(100')와 서비스 제공자 서브시스템(200) 사이의 임의의 적합한 통신 동안의 임의의 적합한 시점에서, 클라이언트 디바이스(100')는 거래를 지불하기 위한 용도로 이용가능할 수 있는, 호스트 디바이스(100) 상에 저장된 적어도 하나의 거래 크리덴셜의 이용가능성을 식별하거나 자신을 대신하여(예컨대, 행정적 엔티티 서브시스템(400)에 의해) 식별하게 할 수 있다. 이어서, 클라이언트 디바이스(100')는 클라이언트 디바이스(100')를 대신하여 거래를 지불하기 위해, 호스트 디바이스(100) 상의 그러한 거래 크리덴셜이 서비스 제공자 서브시스템(200)과 공유되도록 요청하기 위해 호스트 디바이스(100)와 임의의 적합한 데이터를 공유할 수 있다. 그러한 요청에 응답하여, 호스트 디바이스(100)는 거래를 지불하도록 동작할 수 있는 임의의 적합한 거래 크리덴셜 데이터를 생성할 수 있다. 이어서, 일부 실시예들에서, 호스트 디바이스

(100)는 클라이언트 디바이스(100')가 거래 크리덴셜 데이터를 핸들링하지 않고 거래의 지불을 완료하기 위해 서비스 제공자 서브시스템(200)에게 임의의 다른 적합한 거래 데이터(예컨대, 클라이언트 디바이스(100')로부터의 요청에 포함된 거래 데이터)와 함께 그러한 거래 크리덴셜 데이터를 통신할 수 있다(예컨대, 클라이언트 디바이스(100')는 (예컨대, 거래 크리덴셜에 대한 요청과 함께 통신에서) 호스트 디바이스(100)에게 거래의 제어를 핸드오프할 수 있음). 대안적으로, 다른 실시예들에서, 호스트 디바이스(100)는 그러한 거래 크리덴셜 데이터를 클라이언트 디바이스(100')에 다시 통신할 수 있고, 이어서, 클라이언트 디바이스(100')는 거래의 지불을 완료하기 위해 거래 크리덴셜 데이터를 서비스 제공자 서브시스템(200)에 통신할 수 있다(예컨대, (예컨대, 마치 거래 크리덴셜 데이터가 클라이언트 디바이스(100') 상에서 국부적으로 생성된 것과 같이) 서비스 제공자 서브시스템(200)이 호스트 디바이스(100)와 통신하거나 호스트 디바이스(100)를 인식할 필요가 없음). 어떤 시나리오에서든, 행정적 엔티티 서브시스템(200)은 거래 크리덴셜 데이터를 통신할 수 있는 서비스 제공자 서브시스템(200)과 어느 하나의 디바이스 사이에서, (예컨대, 임의의 적합한 공유 비밀(들) 또는 행정적 제공자 서브시스템(200)의 다른 보안 특징들을 사용하여 보안 통신 경로를 인에이블하기 위해) 도관으로서 활용될 수 있다. 또한, 클라이언트 디바이스(100')는 피어-투-피어 또는 다른 직접 링크를 통하여 직접적으로, 또는 클라이언트 디바이스(100')와 연관되거나 연관되지 않을 수 있는 다양한 호스트 디바이스의 다양한 크리덴셜의 상태를 모니터링하도록 동작할 수 있는 행정적 엔티티 서브시스템(200)의 아이덴티티 관리 서비스 또는 임의의 다른 적합한 서비스를 사용하는 것을 포함하는 임의의 적합한 기술을 사용하여 호스트 디바이스(100)를 식별하고/하거나 그렇지 않으면 그와 통신할 수 있다(예컨대, 호스트 디바이스(100)와 클라이언트 디바이스(100')는 행정적 엔티티 서브시스템(200)에 의해 관리되는 공통 사용자 계정에 기초하여 서로 페어링되거나 그렇지 않으면 서로 연관될 수 있으며, 이는 거래 프로세스의 임의의 적합한 부분들을 용이하게 할 수 있음).

[0021] 도 1a의 설명

[0022] 이제 도 1a를 참조하면, 도 1a는 도 1과 관련하여 전술한 시스템(1)의 확대도를 도시한 것으로서, 시스템(1)은 클라이언트 전자 디바이스를 통한 판매자와의 거래(예컨대, 온라인 결제 또는 비접촉식 근접-기반 결제)에서 호스트 전자 디바이스 상의 크리덴셜의 보안 사용을 허용할 수 있다. 예를 들어, 도 1a에 도시된 바와 같이, 시스템(1)은 최종 사용자 호스트 전자 디바이스(100) 뿐만 아니라 및 호스트 전자 디바이스(100) 상에 하나 이상의 크리덴셜을 안전하게 프로비저닝하기 위한 상업적 엔티티 서브시스템(400) 금융 기관(또는 크리덴셜 또는 발행) 서브시스템(350)을 포함할 수 있다. 또한, 도 1a에 도시된 바와 같이, 시스템(1)은 또한 최종 사용자 클라이언트 전자 디바이스(100') 및 판매자(또는 서비스 제공자 또는 프로세서) 서브시스템(200)을 포함할 수 있으며, 그러한 프로비저닝된 크리덴셜은 클라이언트 디바이스(100')를 통해 판매자 서브시스템(200)과의 금융 거래를 수행하기 위해 호스트 디바이스(100)에 의해 사용될 수 있다. 예를 들어, 판매자 서브시스템(200)과의 특정 금융 거래에 대해 클라이언트 디바이스(100')로부터의 클라이언트 결제 요청을 수신하는 것에 응답하여, 호스트 디바이스(100)는 클라이언트 디바이스(100')와 호스트 거래 데이터 또는 프로비저닝된 크리덴셜의 호스트 결제 크리덴셜 데이터를 (예컨대, 보안 호스트 거래 데이터(684)로서) 공유할 수 있고, 이어서, 클라이언트 디바이스(100')는 판매자 서브시스템(200)과의 특정 금융 거래를 지불하기 위해 비접촉식 근접-기반 통신(5)(예컨대, 근거리 통신 또는 블루투스(Bluetooth™) 통신) 및/또는 온라인 기반 통신(686)(예컨대, 네트워크 원격통신 또는 그 외의 방식)으로서 상기 호스트 결제 크리덴셜 데이터를 판매자 서브시스템(200)과 공유할 수 있다. 시스템(1)은 또한 금융 기관 서브시스템(350)과의 금융 거래를 완료하기 위해 그러한 비접촉식 근접-기반 통신(5) 및/또는 그러한 온라인 기반 통신(686)을 활용할 수 있는 매입 은행 서브시스템(300)을 포함할 수 있다.

[0023] 시스템(1)은 클라이언트 디바이스(100')와 판매자 서브시스템(200) 사이의 통신을 인에이블하기 위한 통신 경로(15), 판매자 서브시스템(200)과 매입 은행 서브시스템(300) 사이의 통신을 인에이블하기 위한 통신 경로(25), 매입 은행 서브시스템(300)과 금융 기관 서브시스템(350) 사이의 통신을 인에이블하기 위한 통신 경로(35), 금융 기관 서브시스템(350)의 결제 네트워크 서브시스템(360)과 금융 기관 서브시스템(350)의 발행 은행 서브시스템(370) 사이의 통신을 인에이블하기 위한 통신 경로(45), 금융 기관 서브시스템(350)과 상업적 엔티티 서브시스템(400) 사이의 통신을 인에이블하기 위한 통신 경로(55), 상업적 엔티티 서브시스템(400)과 호스트 전자 디바이스(100) 사이의 통신을 인에이블하기 위한 통신 경로(65), 금융 기관 서브시스템(350)과 호스트 전자 디바이스(100) 사이의 통신을 인에이블하기 위한 통신 경로(75), 상업적 엔티티 서브시스템(400)과 판매자 서브시스템(200) 사이의 통신을 인에이블하기 위한 통신 경로(85), 상업적 엔티티 서브시스템(400)과 클라이언트 디바이스(100') 사이의 통신을 인에이블하기 위한 통신 경로(95), 및 호스트 디바이스(100)와 클라이언트 디바이스(100') 사이의 통신을 인에이블하기 위한 통신 경로(99)를 포함할 수 있다. 경로들(15, 25, 35, 45, 55, 65, 75, 85, 95 및 99) 중 하나 이상의 경로는 하나 이상의 신뢰 서비스 관리자(trusted service manager, "TSM")에 의해 적어도 부분적으로 관리될 수 있다. 통신 네트워크를 생성하도록 동작할 수 있는 임의의 적합한 회로

부, 디바이스, 시스템 또는 이들의 조합(예컨대, 하나 이상의 통신 타워, 원격통신 서버 등을 포함할 수 있는 무선 통신 인프라구조)이 경로들(15, 25, 35, 45, 55, 65, 75, 85, 95 및 99) 중 하나 이상의 경로를 제공하는 데 사용될 수 있으며, 이는 임의의 적합한 유선 또는 무선 통신 프로토콜을 사용하여 통신을 제공할 수 있다. 예를 들어, 경로들(15, 25, 35, 45, 55, 65, 75, 85, 95 및 99) 중 하나 이상의 경로는 Wi-Fi(예컨대, 802.11 프로토콜), ZigBee(예컨대, 802.15.4 프로토콜), WiDi™, 이더넷, Bluetooth™, BLE, 고주파수 시스템(예컨대, 900 MHz, 2.4 GHz 및 5.6 GHz 통신 시스템), 적외선, TCP/IP, SCTP, DHCP, HTTP, BitTorrent™, FTP, RTP, RTSP, RTCP, RAOP, RDTP, UDP, SSH, WDS-브리징, 무선 및 셀룰러 전화 및 개인 전자 메일 디바이스에 의해 사용될 수 있는 임의의 통신 프로토콜(예컨대, GSM, GSM + EDGE, CDMA, OFDMA, HSPA, 다중 대역 등), 저전력 무선 개인 영역 네트워크("6LoWPAN") 모듈, 임의의 다른 통신 프로토콜 또는 이들의 임의의 조합을 지원할 수 있다. 경로들(15, 25, 35, 45, 55, 65, 75, 85, 95 및 99)들 중 하나 이상의 경로는 임의의 적합한 통신 설정(set-up)(예컨대, 도 1의 통신 설정(9))에 의해 인에이블될 수 있다.

[0024] 도 1b의 설명

[0025] 이제 도 1b를 참조하면, 도 1b는 도 1a와 관련하여 전술한 시스템(1)의 보다 상세한 도면을 도시한다. 도 1b에 도시된 바와 같이, 예를 들어, 호스트 전자 디바이스(100)는 프로세서(102), 통신 컴포넌트(106) 및/또는 근거리 통신("NFC") 컴포넌트(120)를 포함할 수 있다. NFC 컴포넌트(120)는 잘 식별된 신뢰 기관들의 세트에 의해 제시될 수 있는 규칙 및 보안 요건들(예컨대, 금융 기관 서브시스템의 권한 및/또는 글로벌플랫폼(GlobalPlatform)과 같은 산업 표준)에 따라 애플리케이션들 및 그 기밀의 암호화 데이터(예컨대, 도 1b에 도시된 바와 같이, 크리덴셜 키(155a') 및 액세스 키(155a) 및/또는 발행자 보안 도메인("ISD") 키(156k)와 같은 크리덴셜 애플릿들 및 연관된 크리덴셜 키들)를 안전하게 호스팅할 수 있을 수 있는 변조 방지 플랫폼을 (예컨대, 단일 칩 또는 다중 칩 보안 마이크로 컨트롤러로서) 제공하도록 구성될 수 있는 보안 요소(145)를 포함하거나 그렇지 않으면 제공할 수 있다. 보다 상세히 후술하는 바와 같이, 호스트 디바이스(100)의(예컨대, NFC 컴포넌트(120)의) 보안 요소(145) 상의 크리덴셜 애플릿 또는 결제 애플리케이션은 호스트 결제 크리덴셜 데이터를 호스트 거래 데이터로서 (예컨대, 금융 기관 서브시스템(350)에서) 지불 계좌 또는 다른 금융 상품 또는 신용 소스를 식별하기 위한 충분한 세부사항과 함께 제공하도록 구성될 수 있으며, 그러한 호스트 결제 크리덴셜 데이터는 금융 거래를 용이하게 하기 위해 클라이언트 디바이스(100') 및/또는 판매자 서브시스템(200) 및/또는 상업적 엔티티 서브시스템(400)과의 하나 이상의 통신에서 호스트 디바이스(100)에 의해 사용될 수 있다. NFC 컴포넌트(120)는 그러한 호스트 결제 크리덴셜 데이터를 비접촉식 근접-기반 통신(예컨대, 근거리 통신)으로서 판매자 서브시스템(200)과 함께(예컨대, 통신 경로(도시되지 않음) - 통신 경로는 호스트 디바이스(100)의 사용자가 호스트 디바이스(100)에 저장된 크리덴셜을 사용하여 비접촉식 근접-기반 통신을 통해 근거리에 위치한 판매자 단말기(220)와 금융 거래를 수행할 수 있는 브릭(brick) 및 모르타르(mortar) 저장소 또는 임의의 물리적 위치에 위치할 수 있음 -를 통해 판매자 서브시스템(200)의 판매자 단말기(220))와 함께) 통신하고/하거나 클라이언트 디바이스(100')의 NFC 컴포넌트(120')와 함께 통신하도록 구성될 수 있다. 대안적으로 또는 부가적으로, 호스트 디바이스(100)가 (예컨대, 통신 경로들(65, 75, 및/또는 99) 중 하나 이상의 통신 경로를 통해) 임의의 적합한 유선 또는 무선 프로토콜을 사용하여 하나 이상의 다른 전자 디바이스 또는 서버 또는 서브시스템(예컨대, 시스템(1)의 하나 이상의 서브시스템 또는 다른 컴포넌트)과 임의의 적합한 호스트 결제 크리덴셜 데이터를 통신하게 허용하도록 통신 컴포넌트(106)가 제공될 수 있다. 호스트 디바이스(100)의 프로세서(102)는 호스트 디바이스(100)의 하나 이상의 컴포넌트의 동작 및 성능을 제어하도록 동작할 수 있는 임의의 프로세싱 회로부를 포함할 수 있다. 예를 들어, 프로세서(102)는 예를 들어, 클라이언트 디바이스를 통해, 판매자 서브시스템(200)과의 금융 거래를 지불하기 위해 데이터(예컨대, 호스트 거래 데이터의 호스트 결제 크리덴셜 데이터)가 호스트 디바이스(100)에 의해 통신될 수 있는 방식(예컨대, 데이터가 호스트 디바이스(100)와 클라이언트 디바이스(100') 사이에서 (예컨대, 통신 경로(99)를 통해) 통신될 수 있는 방식 및/또는 데이터가 호스트 디바이스(100)와 상업적 엔티티 서브시스템(400) 사이에서 (예컨대, 통신 경로(65)를 통해) 통신될 수 있는 방식 - 데이터는 궁극적으로 상업적 엔티티 서브시스템(400)으로부터 통신 경로(95)를 통해 클라이언트 디바이스(100')에 통신될 수 있음 -)을 적어도 부분적으로 지시할 수 있는 디바이스(100) 상의 하나 이상의 애플리케이션(예컨대, 애플리케이션(103) 및/또는 온라인 리소스 또는 판매자 애플리케이션(113))을 실행하도록 구성될 수 있다. 또한, 도 1b에 도시된 바와 같이, 호스트 디바이스(100)는 프로세서(102) 또는 디바이스(100)의 임의의 다른 적합한 부분에 액세스가능할 수 있는 임의의 적합한 호스트 디바이스 식별 정보(119)를 포함할 수 있다. 호스트 디바이스 식별 정보(119)는 판매자 서브시스템(200)과의 금융 거래를 용이하게 하고/하거나 호스트 디바이스(100)와의 임의의 적합한 보안 통신을 인에이블하기 위해 호스트 디바이스(100)를 고유하게 식별하기 위해, 클라이언트 디바이스(100')의 사용자 및/또는 상업적 엔티티 서브시스템(400) 및/또는 판매자 서브시스템(200) 및/또

는 금융 기관 서브시스템(350)에 의해 활용될 수 있다. 단지 하나의 예로서, 호스트 디바이스 식별 정보(119)는 전화 번호 또는 이메일 주소 또는 디바이스(100)와 연관될 수 있는 임의의 고유 식별자일 수 있다.

[0026]

클라이언트 디바이스(100')는 호스트 디바이스(100)와 동일한 컴포넌트들 또는 호스트 디바이스(100)에 의해 제공되지 않는 임의의 컴포넌트들 중 하나, 일부 또는 전부를 포함할 수 있다. 예를 들어, 도 1b에 도시된 바와 같이, 클라이언트 디바이스(100')는 (예컨대, 통신 경로(99)를 통해) 호스트 디바이스(100) 및/또는 (예컨대, 통신 경로(95)를 통해) 상업적 엔티티 서브시스템(400) 및/또는 (예컨대, 통신 경로(15)를 통해) 판매자 서브시스템(200)과의 임의의 적합한 통신을 통신할 수 있는 임의의 적합한 통신 컴포넌트(106')를 포함할 수 있다. 부가적으로 또는 대안적으로, 도 1b에 도시된 바와 같이, 클라이언트 디바이스(100')는 비접촉식 근접-기반 통신(5)을 판매자 서브시스템(200)의 단말기(220)와 통신하도록 동작할 수 있는 임의의 적합한 비접촉식 근접-기반 또는 NFC 컴포넌트(120')를 포함할 수 있다. 부가적으로 또는 대안적으로, 도 1b에 도시된 바와 같이, 클라이언트 디바이스(100')는, 판매자 서브시스템(200)과의 금융 거래를 지불하기 위해 클라이언트 디바이스(100')에 의해 호스트 디바이스(100)로부터의 호스트 결제 크리덴셜 데이터가 통신될 수 있는 방식을 적어도 부분적으로 지시할 수 있는 디바이스(100') 상의 하나 이상의 적합한 애플리케이션(예컨대, 온라인 리소스 또는 판매자 애플리케이션(113'))을 실행하도록 동작할 수 있는 임의의 적합한 프로세서(102')를 포함할 수 있다. 또한, 도 1b에 도시된 바와 같이, 클라이언트 디바이스(100')는 프로세서(102') 또는 디바이스(100')의 임의의 다른 적합한 부분에 액세스가능할 수 있는 임의의 적합한 클라이언트 디바이스 식별 정보(119')를 포함할 수 있다. 클라이언트 디바이스 식별 정보(119')는 판매자 서브시스템(200)과의 금융 거래를 용이하게 하도록 그리고/또는 클라이언트 디바이스(100')와의 임의의 적합한 보안 통신을 인에이블하게 하도록 클라이언트 디바이스(100')를 고유하게 식별하기 위해 호스트 디바이스(100) 및/또는 상업적 엔티티 서브시스템(400) 및/또는 판매자 서브시스템(200) 및/또는 금융 기관 서브시스템(350)의 사용자에게 의해 활용될 수 있다. 단지 하나의 예로서, 클라이언트 디바이스 식별 정보(119')는 전화 번호 또는 이메일 주소 또는 디바이스(100')와 연관될 수 있는 임의의 고유 식별자일 수 있다. 도시되지는 않았지만, 클라이언트 전자 디바이스(100')는 또한, 도 2의 전자 디바이스(100)의 I/O 인터페이스(114)와 동일하거나 유사할 수 있는 I/O 인터페이스, 도 2의 전자 디바이스(100)의 버스(118)와 동일하거나 유사할 수 있는 버스, 도 2의 전자 디바이스(100)의 메모리 컴포넌트(104)와 동일하거나 유사할 수 있는 메모리 컴포넌트, 및/또는 도 2의 전자 디바이스(100)의 전원 공급 장치 컴포넌트(108)와 동일하거나 유사할 수 있는 전원 공급 장치 컴포넌트를 포함할 수 있다.

[0027]

판매자 서브시스템(200)은 도 1b에 도시된 바와 같이, 임의의 적합한 판매자 서버(210)를 포함할 수 있으며, 이는 (예컨대, 통신 경로(85)를 통해) 상업적 엔티티 서브시스템(400)의 통신 컴포넌트 및/또는 (예컨대, 통신 경로(25)를 통해) 매입 은행(300)의 통신 컴포넌트 및/또는 (예컨대, 통신 경로(15)를 통해) 클라이언트 디바이스(100')의 통신 컴포넌트와의 임의의 적합한 통신 프로토콜(예컨대, Wi-Fi, 블루투스™, 셀룰러, 유선 네트워크 프로토콜 등)을 통해 임의의 적합한 데이터를 통신하도록 구성된 임의의 적합한 컴포넌트 또는 서브시스템을 포함할 수 있다. 예를 들어, 판매자 서버(210)는 잠재 거래 데이터(660) 및/또는 업데이트된 잠재 거래 데이터(672)를 임의의 적합한 온라인 콘텍스트 내에서 클라이언트 디바이스(100')의 통신 컴포넌트(106')와 통신하도록 동작할 수 있으며, 온라인 콘텍스트는 클라이언트 디바이스(100')의 사용자가 클라이언트 디바이스(100') 상에 실행될 수 있는 임의의 적합한 판매자 온라인 리소스(113')를 통해 금융 거래를 수행하기 위해 판매자 서버(210)와 통신할 때와 같거나, 판매자 서버(210)에 의해 관리될 수 있는 클라이언트 디바이스(100') 상에 실행되는 제3자 판매자 애플리케이션(113') 또는 목표 리소스 또는 웹 리소스가 판매자 서버(210)에 의해 관리될 수 있는 URL(Uniform Resource Locator)을 가리킬 수 있는 클라이언트 디바이스(100') 상에 실행되는 인터넷 애플리케이션(113')(예컨대, 애플 인크.의 Safari™)과 같을 수 있다. 따라서, 판매자 서버(210)와 클라이언트 디바이스(100') 사이의 통신은 무선 및/또는 유선 경로들을 통해(예컨대, 인터넷을 통해) 발생할 수 있음을 유의한다. 판매자 서버(210)는 판매자 서브시스템(200)의 판매자에 의해 (예컨대, 웹사이트 데이터를 호스팅하고/하거나 제3자 애플리케이션 데이터를 관리하기 위한 웹서버로서) 제공될 수 있다. 부가적으로 또는 대안적으로, 도 1b에 도시된 바와 같이, 판매자 서브시스템(200)은 임의의 적합한 데이터를 호스트 디바이스(100)의 및/또는 클라이언트 디바이스(100')의 비접촉식 근접-기반 통신(예컨대, 클라이언트 디바이스(100')의 NFC 컴포넌트(120')와의 비접촉식 근접-기반 통신(5)) 컴포넌트와 통신하도록 구성된 임의의 적합한 컴포넌트 또는 서브시스템을 포함할 수 있는 임의의 적합한 판매자 단말기(220)(예컨대, 판매자 결제 단말기)를 포함할 수 있다. 또한, 도 1b에 도시된 바와 같이, 판매자 서브시스템(200)은 판매자 키(157)를 포함할 수 있다. 도시되지는 않았지만, 판매자 서브시스템(200)은 또한 도 1b 및 도 2의 전자 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 판매자 프로세서 컴포넌트, (예컨대, 서버(210)의 일부로서) 도 1b 및 도 2의 전자 디바이스(100)의 통신 컴포넌트(106)와 동일하거나 유사할 수 있는 판매자 통신 컴포넌트, 도 2의 전자

디바이스(100)의 I/O 인터페이스(114)와 동일하거나 유사할 수 있는 판매자 I/O 인터페이스, 도 2의 전자 디바이스(100)의 버스(118)와 동일하거나 유사할 수 있는 판매자 버스, 도 2의 전자 디바이스(100)의 메모리 컴포넌트(104)와 동일하거나 유사할 수 있는 판매자 메모리 컴포넌트, 및/또는 도 2의 전자 디바이스(100)의 전원 공급 장치 컴포넌트(108)와 동일하거나 유사할 수 있는 판매자 전원 공급 장치 컴포넌트를 포함할 수 있다.

[0028] 금융 기관 서브시스템(350)은 결제 네트워크 서브시스템(360)(예컨대, 결제 카드 협회 또는 신용 카드 협회) 및/또는 발행 은행 서브시스템(370)을 포함할 수 있다. 예를 들어, 발행 은행 서브시스템(370)은 특정 크리덴셜을 이용하여 소비자가 발생시킬 수 있는 부채를 상환할 수 있는 소비자의 능력에 대한 1차 책임(primary liability)을 질 수 있는 금융 기관일 수 있다. 호스트 디바이스(100)의 NFC 컴포넌트(120)의 각각의 특정 크리덴셜 애플릿은 특정 사용자의 계정 또는 계정들에 전자적으로 링크될 수 있는 특정 결제 카드와 연관될 수 있다. 신용 카드, 직불 카드, 충전 카드, 선불 카드, 플릿(fleet) 카드, 선물 카드 등을 포함하여 다양한 유형의 결제 카드가 적합할 수 있다. 특정 결제 카드의 상거래 크리덴셜은 (예컨대, 직접적으로 또는 상업적 엔티티 서브시스템(400)을 통해 및/또는 클라이언트 디바이스(100')를 통해) 판매자 서브시스템(200)과의 상거래 크리덴셜 데이터 통신(예컨대, 비접촉식 근접-기반 통신 및/또는 온라인 기반 통신)에 사용하기 위해 은행 서브시스템(370)을 발행함으로써 호스트 디바이스(100) 상에 (예컨대, 후술되는 바와 같이, NFC 컴포넌트(120)의 크리덴셜 보충적 보안 도메인의 크리덴셜을 이용하여) 프로비저닝될 수 있다. 각각의 크리덴셜은 결제 네트워크 서브시스템(360)에 의해 브랜드화될 수 있는 결제 카드의 특정 브랜드일 수 있다. 결제 네트워크 서브시스템(360)은 특정 브랜드의 결제 카드들(예컨대, 상거래 크리덴셜들)의 사용을 프로세싱할 수 있는 다양한 발행 은행(370) 및/또는 다양한 매입 은행(300)의 네트워크일 수 있다.

[0029] 금융 거래가 시스템(1) 내에 발생하기 위해서는, 적어도 하나의 상거래 크리덴셜이 호스트 전자 디바이스(100)의 NFC 컴포넌트(120)의 보안 요소 상에 안전하게 프로비저닝되어야 한다. 예를 들어, 그러한 상거래 크리덴셜은 금융 기관 서브시스템(350)으로부터 직접 호스트 디바이스(100)의 NFC 컴포넌트(120)의 보안 요소 상에 적어도 부분적으로 프로비저닝될 수 있다(예컨대, 금융 기관 서브시스템(350)과 디바이스(100) 사이의 통신 경로(75)를 통해 크리덴셜 데이터(654)로서 프로비저닝될 수 있으며, 이는 통신 컴포넌트(106)를 통해 NFC 컴포넌트(120)로 전달될 수 있음). 부가적으로 또는 대안적으로, 그러한 상거래 크리덴셜은 상업적 엔티티 서브시스템(400)을 통해 금융 기관 서브시스템(350)으로부터 호스트 디바이스(100)의 NFC 컴포넌트(120)의 보안 요소 상에 적어도 부분적으로 프로비저닝될 수 있다(예컨대, 금융 기관 서브시스템(350)과 상업적 엔티티 서브시스템(400) 사이의 통신 경로(55)를 통해 크리덴셜 데이터(654)로서 프로비저닝될 수 있으며, 이는 상업적 엔티티 서브시스템(400)의 서버(410)와 디바이스(100)의 통신 컴포넌트(106) 사이의 통신 경로(65)를 통해 크리덴셜 데이터(654)로서 디바이스(100)에 전달될 수 있고, 이어서, 통신 컴포넌트(106)로부터 NFC 컴포넌트(120)로 전달될 수 있음). 경로(75) 및/또는 경로들(55/65)을 통한 크리덴셜 데이터(654)는 NFC 컴포넌트(120)의 크리덴셜 보충적 보안 도메인의 적어도 일부 또는 전부로서 디바이스(100)의 보안 요소 상에 프로비저닝될 수 있고, 크리덴셜 정보를 갖는 크리덴셜 애플릿 및/또는 크리덴셜 정보(161a) 및 크리덴셜 키(155a')를 갖는 결제 애플리케이션 또는 크리덴셜 애플릿(153a)과 같은 크리덴셜 키를 포함할 수 있다. 도 1b에 도시된 바와 같이, 예를 들어, 금융 기관 서브시스템(350)은 또한 (예컨대, 크리덴셜 키(155a'))를 사용하여 디바이스(100)에 의해 암호화된 데이터를 복호화하기 위해) 크리덴셜 키(155a')에 대한 액세스를 가질 수 있다. 금융 기관 서브시스템(350)은 그러한 키의 생성, 교환, 저장, 사용 및 대체를 포함할 수 있는 크리덴셜 키(155a')의 관리를 담당할 수 있다. 금융 기관 서브시스템(350)은 그의 크리덴셜 키(155a')의 버전을 금융 기관 서브시스템(350)의 보안 요소에 저장할 수 있다. NFC 컴포넌트(120) 및 금융 기관 서브시스템(350)의 크리덴셜 키(155a')는 전자 디바이스(100)의 보안 요소 및 금융 기관 서브시스템(350) 모두에 이용가능한 임의의 적합한 공유 비밀(예컨대, 패스워드, 패스프레이즈(passphrase), 무작위로 선택된 바이트들의 배열, 하나 이상의 대칭 키들, 공개-개인 키들(예컨대, 비대칭 키들) 등)로서, 임의의 다른 적합한 암호화 데이터(예컨대, 암호문) 또는 임의의 다른 적합한 데이터가 (예컨대, 금융 거래를 위한 결제 데이터를 검증하기 위한) 전자 디바이스(100) 및 금융 기관 서브시스템(350)에 의해, 예를 들어, 공유 비밀(shared secret) - 공유 비밀은 금융 기관 서브시스템(350)에 의해 디바이스(100) 상에 프로비저닝될 수 있음 - 에 의해 적어도 부분적으로 기능 출력이 결정될 수 있는 임의의 적합한 암호화 알고리즘 또는 암호(cipher)를 사용함으로써 독립적으로 생성되는 것을 가능하게 하도록 동작할 수 있음이 이해되어야 한다. 공유 비밀은 (예컨대, 금융 기관 서브시스템(350)에 의한 디바이스(100) 상의 크리덴셜의 프로비저닝 동안) 금융 기관 서브시스템(350)과 호스트 디바이스(100) 간에 미리 공유될 수 있으며, 이 경우에 그러한 공유 비밀은 사전 공유 키(pre-shared key)로 지칭될 수 있거나 키-약정 프로토콜을 사용하여 특정 금융 거래에 사용하기 전에 (예컨대, Diffie-Hellman과 같은 공개 키 암호화를 사용하거나 Kerberos와 같은 대칭 키 암호화를 사용하여) 공유 비밀을 생성할 수 있다. 공유 비밀 및 그것의 기능 출력이 공유 비밀에 의해 적어도 부분적으로

결정될 수 있는 임의의 적합한 암호화 알고리즘 또는 암호는 디바이스(100)의 보안 요소에 액세스가능할 수 있다.

[0030]

상업적 엔티티 서브시스템(400)은 크리덴셜이 디바이스(100)의 보안 요소에 프로비저닝될 때 및/또는 그러한 프로비저닝된 크리덴셜이 디바이스(100)와 판매자 서브시스템(200) 사이의 상거래 크리덴셜 데이터 통신의 일부로서 사용될 때, 금융 기관 서브시스템(350)과 호스트 디바이스(100) 사이의 매개체로서 제공될 수 있으며, 상업적 엔티티 서브시스템(400)은 새로운 보안 층을 제공하고/하거나 더 끊임없는 사용자 경험을 제공하도록 구성될 수 있다. 상업적 엔티티 서브시스템(400)은 특정 상업적 엔티티에 의해 제공될 수 있는 것으로, 사용자-특정 로그인 정보를 통해(예컨대, 사용자-특정 식별 및 패스워드 조합을 통해) 디바이스(100)의 사용자 및/또는 디바이스(100')의 사용자에게 그 상업적 엔티티의 사용자-특정 계정에 다양한 서비스를 제공할 수 있다. 단지 하나의 예로서, 상업적 엔티티 서브시스템(400)은 캘리포니아 주 쿠파티노 소재의 애플 인크.(Apple Inc.)에 의해 제공될 수 있으며, 애플 인크.는 또한 디바이스(100) 및/또는 디바이스(100')의 사용자에게 대한 다양한 서비스의 제공자일 수 있고(예컨대, 디바이스(100)에 의해 재생되는 미디어를 판매/대여하기 위한 아이튠즈(iTunes)TM 스토어, 디바이스(100)에 사용할 애플리케이션을 판매/대여하기 위한 애플 앱 스토어(Apple App Store)TM, 디바이스(100)로부터 데이터를 저장하고/하거나 다수의 사용자 디바이스 및/또는 다수의 사용자 프로파일을 서로 연관시키는 애플 아이클라우드(Apple iCloud)TM 서비스, 다양한 애플 제품을 온라인에서 구입하기 위한 애플 온라인 스토어(Apple Online Store), 디바이스 간 미디어 메시지 통신을 위한 애플 아이메시지(Apple iMessage)TM 서비스, 등) 및 애플 인크.는 또한 디바이스(100) 자체 및/또는 디바이스(100') 자체 및/또는 디바이스(100) 및/또는 디바이스(100')의 운영 시스템(예컨대, 디바이스 애플리케이션(103))의 제공자, 제조자, 및/또는 개발자일 수 있다(예컨대, 디바이스(100)가 아이팟(iPod)TM, 아이패드(iPad)TM, 아이폰(iPhone)TM 등인 경우). 상업적 엔티티 서브시스템(400)을 제공할 수 있는 상업적 엔티티(예컨대, 애플 인크.)는 금융 기관 서브시스템(350)의 임의의 금융 엔티티와 별개이고 그에 독립적일 수 있다. 예를 들어, 상업적 엔티티 서브시스템(400)을 제공할 수 있는 상업적 엔티티는 임의의 신용 카드 또는 최종 사용자 호스트 디바이스(100) 상에 프로비저닝된 임의의 다른 상거래 크리덴셜을 제공 및/또는 관리할 수 있는 임의의 결제 네트워크 서브시스템(360) 또는 발행 은행 서브시스템(370)과 별개이고/이거나 그에 독립적일 수 있다. 부가적으로 또는 대안적으로, 상업적 엔티티 서브시스템(400)(예컨대, 애플 인크.)을 제공할 수 있는 상업적 엔티티는 판매자 서브시스템(200)의 임의의 판매자로부터 별개이고 그에 독립적일 수 있다. 예를 들어, 상업적 엔티티 서브시스템(400)을 제공할 수 있는 상업적 엔티티는 NFC 통신, 제3자 애플리케이션(113) 및/또는 임의의 다른 양태의 판매자 서브시스템(200)에 대한 판매자 단말기를 제공할 수 있는 판매자 서브시스템(200)의 임의의 판매자와 별개일 수 있고/있거나 그에 독립적일 수 있다. 그러한 상업적 엔티티는, 예를 들어, 디바이스(100)의 사용자가 금융 기관 서브시스템(350)에 의해 제공된 크리덴셜을 호스트 디바이스(100) 상에 프로비저닝하기를 원할 때 및/또는 금융 거래를 지불하기 위해 그러한 프로비저닝된 크리덴셜이 판매자 서브시스템(200)과의 상거래 크리덴셜 데이터 통신의 일부로서 사용 중일 때, 디바이스(100)의 사용자에게 더욱 끊임없는 사용자 경험을 제공하기 위하여, 디바이스(100)의 다양한 컴포넌트(예컨대, 그 상업적 엔티티가 디바이스(100)를 적어도 부분적으로 생성 또는 관리할 수 있을 때와 같은 때의 디바이스(100)의 소프트웨어 및/또는 하드웨어 컴포넌트들)를 구성 또는 제어하는 자신의 잠재 능력을 레버리지할 수 있다. 예를 들어, 일부 실시예들에서, 디바이스(100)는 (예컨대, 디바이스(100)와 판매자 서브시스템(200) 사이의 온라인 기반 상거래 크리덴셜 데이터 통신 동안) 보다 높은 수준의 보안을 가능하게 할 수 있는 특정 데이터를 공유 및/또는 수신하기 위해 디바이스(100)의 사용자에게 상업적 엔티티 서브시스템(400)과 (예컨대, 통신 경로(65)를 통해) 끊임없고 투명하게 통신하도록 구성될 수 있다. 도시되지는 않았지만, 상업적 엔티티 서브시스템(400)은 또한 도 1b 및 도 2의 전자 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 프로세서 컴포넌트, 도 1b 및 도 2의 전자 디바이스(100)의 통신 컴포넌트(106)와 동일하거나 유사할 수 있는 통신 컴포넌트, 도 2의 전자 디바이스(100)의 I/O 인터페이스(114)와 동일하거나 유사할 수 있는 I/O 인터페이스, 도 2의 전자 디바이스(100)의 버스(118)와 동일하거나 유사할 수 있는 버스, 도 2의 전자 디바이스(100)의 메모리 컴포넌트(104)와 동일하거나 유사할 수 있는 메모리 컴포넌트, 및/또는 도 2의 전자 디바이스(100)의 전원 공급 장치 컴포넌트(108)와 동일하거나 유사할 수 있는 전원 공급 장치 컴포넌트, 서버(410)에 의해 적어도 부분적으로 제공될 수 있는 하나, 일부 또는 전부를 포함할 수 있다.

[0031]

(예컨대, 크리덴셜 키(155a') 및 크리덴셜 정보(161a)를 갖는 크리덴셜 SSD의 일부로서) 호스트 디바이스(100)의 NFC 컴포넌트(120)의 보안 요소 상에 프로비저닝된 적어도 하나의 상거래 크리덴셜에 부가하여, 디바이스(100)가 판매자 서브시스템(200)과의 금융 거래를 보다 안전하게 수행할 수 있도록, 액세스 키(155b)를 갖는 적어도 하나의 액세스 SSD가 디바이스(100)의 NFC 컴포넌트(120)의 보안 요소 상에 또한 프로비저닝될 수 있다. 예를 들어, 액세스 SSD는 상업적 엔티티 서브시스템(400)으로부터 직접 호스트 디바이스(100)의 NFC 컴포넌트

(120)의 보안 요소 상에 적어도 부분적으로 프로비저닝될 수 있다(예컨대, 상업적 엔티티 서브시스템(400)의 서버(410)와 디바이스(100)의 통신 컴포넌트(106) 사이의 통신 경로(65)를 통해 액세스 데이터(652)로서 적어도 부분적으로 프로비저닝될 수 있으며, 액세스 데이터(652)는 이어서, 통신 컴포넌트(106)로부터 NFC 컴포넌트(120)로 전달될 수 있다). 경로(65)를 통한 액세스 데이터(652)는 액세스 SSD의 적어도 일부 또는 전부로서 디바이스(100)의 보안 요소 상에 프로비저닝될 수 있고, 액세스 키(155b)를 갖는 액세스 애플릿(153b)을 포함할 수 있다. 도 1b에 도시된 바와 같이, 상업적 엔티티 서브시스템(400)은 (예컨대, 액세스 키(155b)를 사용하여 디바이스(100)에 의해 암호화된 데이터를 복호화하기 위해) 액세스 키(155b)에 대한 액세스를 또한 가질 수 있다. 상업적 엔티티 서브시스템(400)은 그러한 키의 생성, 교환, 저장, 사용 및 대체를 포함할 수 있는 액세스 키(155b)의 관리를 담당할 수 있다. 상업적 엔티티 서브시스템(400)은 상업적 엔티티 서브시스템(400)의 보안 요소에 그의 액세스 키(155b)의 버전을 저장할 수 있다. 액세스 키(155b)를 갖는 NFC 컴포넌트(120)의 액세스 SSD는 (예컨대, 생체인식 입력 컴포넌트와 같은, 디바이스(100)의 하나 이상의 입력 컴포넌트(110)를 통해) 디바이스(100)의 사용자의 의도(intent) 및 로컬 인증을 결정하도록 구성될 수 있으며, 그러한 결정에 응답하여, (예컨대, NFC 컴포넌트(120)의 크리덴셜 SSD의 크리덴셜을 이용하여) 결제 거래를 수행하기 위해 또 다른 특정 SSD를 인에이블하도록 구성될 수 있다. 그러한 액세스 SSD를 디바이스(100)의 보안 요소 내에 저장함으로써, 금융 거래의 사용자 의도 및 인증을 신뢰성 있게 결정하는 그 능력이 증가될 수 있다. 또한, NFC 컴포넌트(120)의 액세스 SSD의 액세스 키(155b)는 디바이스(100)의 보안 요소 외부에서 통신될 수 있는 금융 거래 데이터에 증가된 암호화를 제공하기 위해 레버리지될 수 있다. 부가적으로 또는 대안적으로, 이하에서 설명되는 바와 같이, 액세스 데이터(652)는 전자 디바이스(100)의 보안 요소의 ISD에 대한 발행자 보안 도메인("ISD") 키(156k)를 포함할 수 있으며, 이는 또한 이하에서 설명되는 바와 같이, 상업적 엔티티 서브시스템(400)에 의해 유지될 수 있으며, 액세스 키(155b)에 부가로 또는 대안으로서 사용될 수 있다.

[0032] 명시적으로 도시되거나 설명되지는 않았지만, 상업적 엔티티 서브시스템(400)은, (예컨대, 클라이언트 디바이스(100'))가 호스트 디바이스로서 동작하도록 크리덴셜이 클라이언트 디바이스(100') 상에 프로비저닝될 수 있는 경우) 상업적 엔티티 서브시스템(400)이 호스트 디바이스(100)와 상호작용하거나 호스트 디바이스(100)와 연관되도록 동작할 수 있는 임의의 또는 모든 동일한 방식으로, 클라이언트 디바이스(100')와 상호작용하거나 클라이언트 디바이스(100')와 연관되도록 동작할 수 있다는 것이 이해되어야 한다.

[0033] 판매자 애플리케이션 또는 온라인 리소스(113')는 디바이스(100')와 판매자 서브시스템(200) 사이에서 온라인 금융 거래를 용이하게 하기 위해 클라이언트 디바이스(100')에 의해 액세스될 수 있다. 먼저, 그러한 애플리케이션(113')은 애플리케이션(113')이 클라이언트 디바이스(100')에 의해 액세스가능하기 전에 상업적 엔티티 서브시스템(400)에 의해 승인되거나 그렇지 않으면 인에이블될 수 있다. 예를 들어, 상업적 엔티티 서브시스템(400)의 애플리케이션 스토어(420)(예컨대, 애플 앱 스토어™)는 통신 경로(85)를 통해 판매자 서브시스템(200)으로부터 애플리케이션(113')을 표현하는 적어도 일부 데이터를 수신할 수 있다. 또한, 일부 실시예들에서, 상업적 엔티티 서브시스템(400)은 애플리케이션(113')에 대한 판매자 키(157')를 생성하거나 그렇지 않으면 할당할 수 있고, (예컨대, 경로(85)를 통해) 판매자 서브시스템(200)에게 그러한 판매자 키(157')를 제공할 수 있다. 대안적으로, 판매자 서브시스템(200)은 애플리케이션(113')에 대한 판매자 키(157')를 생성하거나 그렇지 않으면 할당할 수 있고, (예컨대, 경로(85)를 통해) 상업적 엔티티 서브시스템(400)에 그러한 판매자 키(157')를 제공할 수 있다. 판매자 서브시스템(200) 또는 상업적 엔티티 서브시스템(400) 중 어느 하나는 그러한 키의 생성, 교환, 저장, 사용 및 교체를 포함할 수 있는 판매자 키(157')의 관리를 담당할 수 있다. 그러한 판매자 키(157')가 생성되고/되거나 관리될 수 있는 방식 또는 위치에 관계없이, 판매자 서브시스템(200) 및 상업적 엔티티 서브시스템(400) 둘 모두는 판매자 키(157')의 버전을(예컨대, 판매자 서브시스템(200) 및 상업적 엔티티 서브시스템(400)의 각각의 보안 요소에) 저장할 수 있다. 일부 실시예들에서, 그러한 판매자 키(157')는 특히 판매자 애플리케이션(113')과 연관될 수 있는 한편, 다른 실시예들에서, 판매자 키(157')는 특히 판매자 서브시스템(200)의 판매자와 연관되어, 판매자 키(157')가 판매자 서브시스템(200)의 동일한 판매자에 의해 동작되는 다수의 제3자 애플리케이션과 연관될 수 있다. 특정 판매자 키(157')를 특정 판매자 애플리케이션(113') 또는 판매자 엔티티와 연관시키기 위해 상업적 엔티티 서브시스템(400)에 액세스가능할 수 있는 테이블 (430) 또는 임의의 다른 적합한 데이터 구조 또는 정보의 소스가 제공될 수 있다. 테이블(430)은 키(157')와 연관된 판매자 애플리케이션(113')을 통해 판매자 서브시스템(200)과 인터페이싱하는 클라이언트 디바이스(100')를 포함할 수 있는 상업적 엔티티 서브시스템(400)이 금융 거래를 위해 판매자 서브시스템(200)에게 통신되는 임의의 상거래 크리덴셜 데이터(예컨대, 호스트 디바이스(100)에 네이티브한 결제 크리덴셜 데이터를 포함할 수 있는 상거래 크리덴셜 데이터)에 보안 층을 제공하기 위해 적절한 판매자 키(157')를 결정하고 활용하게 할 수 있다. 디바이스(100')는 (예컨대, 통신 경로(95)를 통해 애플리케이션 스토어(420)로부터) 애플리케이션(113')에 액세스

하고 (예컨대, 프로세서(102'))를 이용하여) 애플리케이션(113')을 실행하도록 구성될 수 있다. 대안적으로 또는 부가적으로, 판매자 키(157')는 판매자의 제3자 애플리케이션(예컨대, 애플리케이션(113')) 보다는 오히려 또는 그에 부가하여 판매자의 웹사이트(예컨대, 하나 이상의 URL) 또는 판매자와 일반적으로 연관될 수 있다. 예를 들어, 판매자 서브시스템(200)의 판매자는 특정 판매자 웹사이트 또는 판매자를 일반적으로 테이블(430) 내의 특정 판매자 키(157')와 연관시키기 위해 상업적 엔티티 서브시스템(400)과 협력할 수 있으며, 이는 상업적 엔티티 서브시스템(400)이, 클라이언트 디바이스(100')의 판매자 서버(210)와의 인터페이싱을 수반할 수 있는 금융 거래를 위해 판매자 서브시스템(200)에 통신된 임의의 상거래 크리덴셜 데이터(예컨대, 호스트 디바이스(100)에 네이티브한 결제 크리덴셜 데이터를 포함할 수 있는 상거래 크리덴셜 데이터)에게 보안 층을 제공하기 위해 적절한 판매자 키(157')를 결정 및 활용하게 하여, 목표 리소스 또는 웹 리소스가 그 판매자 키(157')와 연관될 수 있는 URL을 가리킬 수 있는 디바이스(100') 상에 실행 중인 인터넷 애플리케이션 또는 웹 브라우저를 통해 금융 거래를 수행할 수 있다. 디바이스(100')는 예를 들어, 판매자 서버(210)로부터 통신 경로(15)를 통해 (예컨대, 디바이스(100') 상의 인터넷 애플리케이션(113'))을 사용하여 그러한 URL에 액세스하도록 구성될 수 있다. 다른 실시예들에서, 애플리케이션(113')은 특정 판매자, 판매자 서브시스템(200) 및/또는 판매자 키(157')와 연관되지 않고, 대신에 디바이스(100')가 이용할 수 있는 독립적인 애플리케이션일 수 있다. 일부 실시예들에서, 도시된 바와 같이, 판매자 키(157)를 갖는 유사한 애플리케이션(113)이 호스트 디바이스(100)에게 제공될 수 있으며, 여기서 애플리케이션(113)은 애플리케이션(113')과 동일하거나 상이할 수 있고/있거나, 키(157)는 키(157')와 동일하거나 상이할 수 있다.

[0034] 도 2의 설명

[0035] 이제 도 2를 참조하면, 도 2는 도 1 내지 도 1b와 관련하여 상술한 시스템(1)의 전자 디바이스(100)의 보다 상세한 도면을 도시한다. 도 2에 도시된 바와 같이, 예를 들어, 전자 디바이스(100)는 프로세서(102), 메모리(104), 통신 컴포넌트(106), 전원 공급장치(108), 입력 컴포넌트(110), 출력 컴포넌트(112), 안테나(116), 및 근거리 통신("NFC") 컴포넌트(120)를 포함할 수 있다. 전자 디바이스(100)는 또한, 디바이스(100)의 다양한 다른 컴포넌트들로, 그것들로부터, 또는 그것들 사이에서 데이터 및/또는 전력을 전송하기 위한 하나 이상의 유선 또는 무선 통신 링크 또는 경로를 제공할 수 있는 버스(118)를 포함할 수 있다. 전자 디바이스(100)에는 또한, 디바이스(100) 외부의 잔해물 및 다른 분해하는 힘(degrading force)들로부터의 보호를 위해 디바이스(100)의 컴포넌트들 중 하나 이상을 적어도 부분적으로 둘러쌀 수 있는 하우징(101)이 제공될 수 있다. 일부 실시예들에서, 전자 디바이스(100)의 하나 이상의 컴포넌트는 조합되거나 생략될 수 있다. 또한, 전자 디바이스(100)는 도 2에서 조합되거나 포함되지 않은 다른 컴포넌트들을 포함할 수 있다. 예를 들어, 전자 디바이스(100)는 임의의 다른 적합한 컴포넌트들 또는 도 2에 도시된 컴포넌트들의 여러 예들을 포함할 수 있다. 단순화하기 위하여, 컴포넌트들 각각 중 단지 하나만이 도 2에 도시된다. 하나 이상의 입력 컴포넌트(110)는, 사용자가 디바이스(100)와 상호작용하거나 그와 인터페이싱하는 것을 허용하기 위해 제공될 수 있고/있거나 하나 이상의 출력 컴포넌트(112)가 정보(예컨대, 그래픽, 청각적 및/또는 촉각적 정보)를 디바이스(100)의 사용자에게 제시하기 위해 제공될 수 있다. 하나 이상의 입력 컴포넌트 및 하나 이상의 출력 컴포넌트는 때때로 본 명세서에서 총칭하여 입력/출력("I/O") 컴포넌트 또는 I/O 인터페이스(114)로서 지칭될 수 있음을 유의해야 한다(예컨대, I/O 컴포넌트 또는 I/O 인터페이스(114)로서의 입력 컴포넌트(110) 및 출력 컴포넌트(112)). 예를 들어, 입력 컴포넌트(110) 및 출력 컴포넌트(112)는 때때로, 사용자의 디스플레이 스크린의 터치를 통해 입력 정보를 수신할 수 있고 또한 그 동일한 디스플레이 스크린을 통해 사용자에게 시각적 정보를 제공할 수 있는, 터치 스크린과 같은, 단일 I/O 컴포넌트(114)일 수 있다. 전자 디바이스(100)의 프로세서(102)는 전자 디바이스(100)의 하나 이상의 컴포넌트의 동작들 및 성능을 제어하도록 동작할 수 있는 임의의 프로세싱 회로를 포함할 수 있다. 예를 들어, 프로세서(102)는 입력 컴포넌트(110)로부터 입력 신호들을 수신하고/하거나 출력 컴포넌트(112)를 통해 출력 신호들을 구동할 수 있다. 도 2에 도시된 바와 같이, 프로세서(102)는 애플리케이션(103) 및/또는 애플리케이션(113)과 같은 하나 이상의 애플리케이션을 실행하는 데 사용될 수 있다. 하나의 예로서, 애플리케이션(103)은 운영 시스템 애플리케이션일 수 있는 한편, 애플리케이션(113)은 제3자 애플리케이션 또는 임의의 다른 적합한 온라인 리소스(예컨대, 판매자 서브시스템(200)의 판매자와 연관된 애플리케이션)일 수 있다. 또한, 도시된 바와 같이, 프로세서(102)는 호스트 디바이스 식별 정보(119)에 대한 액세스를 가질 수 있으며, 이는 디바이스(100)의 식별을 (예컨대, 금융 거래를 용이하게 하기 위해) 판매자 서브시스템(200)에 제공하고/하거나 (예컨대, 디바이스들(100 및 100')) 사이의 보안 통신을 용이하게 하기 위해) 클라이언트 디바이스(100')에 제공하기 위해, 디바이스(100)의 사용자 및/또는 상업적 엔티티 서브시스템(400)에 의해 활용될 수 있다.

[0036] NFC 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200)의 판매자 단말기(예컨대, 판매자 단말기의 판매자 결제 단말기(220)) 사이에서 비접촉식 근접-기반 거래들 또는 통신을 인에이블할 수 있는 임의의 적합한

근접-기반 통신 메커니즘일 수 있다. NFC 컴포넌트(120)는 전자 디바이스(100)와 그러한 판매자 단말기 사이에서 비접촉식 근접-기반 통신을 인에이블하기 위한 임의의 적합한 모듈들을 포함할 수 있다. 도 2에 도시된 바와 같이, 예를 들어, NFC 컴포넌트(120)는 NFC 디바이스 모듈(130), NFC 컨트롤러 모듈(140), 및/또는 NFC 메모리 모듈(150)을 포함할 수 있다. NFC 디바이스 모듈(130)은 NFC 데이터 모듈(132), NFC 안테나(134), 및 NFC 부스터(136)를 포함할 수 있다. NFC 데이터 모듈(132)은, NFC 컴포넌트(120)에 의해 판매자 단말기로 비접촉식 근접-기반 또는 NFC 통신의 일부로서 송신될 수 있는 임의의 적합한 데이터를 포함, 라우팅, 또는 그렇지 않으면 제공하도록 구성될 수 있다. 부가적으로 또는 대안적으로, NFC 데이터 모듈(132)은, 비접촉식 근접-기반 통신의 일부로서 판매자 단말기로부터 NFC 컴포넌트(120)에 의해 수신될 수 있는 임의의 적합한 데이터를 포함, 라우팅, 또는 그렇지 않으면 수신하도록 구성될 수 있다. NFC 컨트롤러 모듈(140)은 적어도 하나의 NFC 프로세서 모듈(142)을 포함할 수 있다. NFC 프로세서 모듈(142)은 NFC 디바이스 모듈(130)과 공조하여 동작하여, 전자 디바이스(100)와 판매자 단말기 사이의 NFC 통신을 통신하기 위해 NFC 컴포넌트(120)를 인에이블, 활성화, 허용, 및/또는 그렇지 않으면 제어할 수 있다. NFC 컨트롤러 모듈(140)은, NFC 컴포넌트(120)의 기능을 지시하도록 도움을 줄 수 있는 NFC 저전력 모드 또는 지갑 애플리케이션(143)과 같은, 하나 이상의 애플리케이션을 실행하는 데 사용될 수 있는 적어도 하나의 NFC 프로세서 모듈(142)을 포함할 수 있다. NFC 메모리 모듈(150)은 NFC 디바이스 모듈(130) 및/또는 NFC 컨트롤러 모듈(140)과 공조하여 동작하여, 전자 디바이스(100)와 판매자 서브시스템(200) 사이의 NFC 통신을 허용할 수 있다. NFC 메모리 모듈(150)은 변조 방지(tamper resistant)일 수 있고 보안 요소(145)의 적어도 일부분을 제공할 수 있다(예컨대, 도 2a 참조). 예를 들어, 그러한 보안 요소는, 잘-식별된 신뢰 기관들의 세트에 의해 제시될 수 있는 규칙들 및 보안 요건들(예컨대, 금융 기관 서브시스템의 권한 및/또는 글로벌플랫폼과 같은 산업 표준)에 따라 애플리케이션들 및 그것들의 기밀의 암호화 데이터(예컨대, 애플릿(153) 및 키(155))를 안전하게 호스팅할 수 있는 변조 방지 플랫폼을(예컨대, 단일 칩 또는 다중 칩 보안 마이크로컨트롤러로서) 제공하도록 구성될 수 있다.

[0037] 예를 들어, 도 2에 도시된 바와 같이, NFC 메모리 모듈(150)은 발행자 보안 도메인("ISD")(152) 및 보충적 보안 도메인("SSD")(154)(예컨대, 서비스 제공자 보안 도메인("SPSD"), 신뢰 서비스 관리자 보안 도메인("TSMSSD") 등) 중 하나 이상을 포함할 수 있으며, 이는 NFC 규격 표준(예컨대, 글로벌플랫폼)에 의해 정의 및 관리될 수 있다. 예를 들어, ISD(152)는, 신뢰 서비스 관리자("TSM") 또는 발행 금융 기관(예컨대, 금융 기관 서브시스템(350))이, 크리덴셜 콘텐츠 관리, 및/또는 보안 도메인 관리를 위해, (예컨대, 통신 컴포넌트(106)를 통해) 하나 이상의 크리덴셜(예컨대, 다양한 신용 카드, 은행 카드, 선물 카드, 액세스 카드, 교통 패스 등과 연관된 크리덴셜들)을 생성하거나 그렇지 않으면 전자 디바이스(100) 상에 프로비저닝하기 위한 키들 및/또는 다른 적합한 정보를 저장할 수 있는 NFC 메모리 모듈(150)의 일부분일 수 있다. 크리덴셜은 사용자/소비자에게 할당될 수 있고, 신용 카드 결제 번호(예컨대, 디바이스 기본 계정 번호("DPAN"), DPAN 만료 일자, CVV 등)와 같은, 전자 디바이스(100) 상에 안전하게 저장될 수 있는 크리덴셜 데이터(예컨대, 크리덴셜 정보(161a))를 포함할 수 있다(예컨대, 토큰 또는 그 외의 것). NFC 메모리 모듈(150)은 적어도 2개의 SSD(154)(예컨대, 적어도 제1 SSD(154a) 및 제2 SSD(154b))를 포함할 수 있다. 예를 들어, 제1 SSD(154a)(예컨대, 크리덴셜 SSD(154a))는 전자 디바이스(100)에 특정 특권 또는 결제 권한을 제공할 수 있는 특정 크리덴셜(예컨대, 금융 기관 서브시스템(350)에 의해 프로비저닝된 특정 신용 카드 크리덴셜 또는 특정 대중 교통 카드 크리덴셜)과 연관될 수 있는 한편, 제2 SSD(154b)(예컨대, 액세스 SSD(154b))는 예를 들어, 특정 특권 또는 결제 권한을 전자 디바이스(100)에 제공하기 위해 다른 SSD(예컨대, 제1 SSD(154a))의 특정 크리덴셜에 대한 디바이스(100)의 액세스를 제어할 수 있는 상업적 엔티티(예컨대, 디바이스(100)에 대한 제어 엔티티일 수 있는 상업적 엔티티 서브시스템(400)의 상업적 엔티티)와 연관될 수 있다. 대안적으로, 제1 SSD(154a) 및 제2 SSD(154b)의 각각은 특정 특권 또는 결제 권한을 전자 디바이스(100)에 제공할 수 있는 각각의 특정 크리덴셜(예컨대, 금융 기관 서브시스템(350)에 의해 프로비저닝된 특정 신용 카드 크리덴셜 또는 특정 대중 교통 카드 크리덴셜)과 연관될 수 있다. 각각의 SSD(154)는 적어도 하나의 애플릿(153)을 포함하고/하거나 그와 연관될 수 있다(예컨대, SSD(154a)와 애플릿(153a), 및 SSD(154b)와 애플릿(153b)). 예컨대, SSD(154)의 애플릿(153)은 (예컨대, 글로벌플랫폼 환경에서) NFC 컴포넌트(120)의 보안 요소 상에 실행될 수 있는 애플리케이션일 수 있다. 크리덴셜 애플릿(153)은 크리덴셜 정보(161)를 포함하거나 그와 연관될 수 있다(예컨대, 애플릿(153a)의 정보(161a) 및/또는 애플릿(153b)의 정보(161b)). 각각의 SSD(154) 및/또는 애플릿(153)은 또한 그 자신의 키들(155) 중 적어도 하나를 포함하고/하거나 그와 연관될 수 있다(예컨대, 애플릿(153a)과 적어도 하나의 키(155a) 및 애플릿(153b)과 적어도 하나의 키(155b)).

[0038] SSD(154)의 키(155)는 암호화 알고리즘 또는 암호의 기능 출력을 결정할 수 있는 하나의 정보일 수 있다. 예를 들어, 암호화에서, 키는 암호 평문에서 암호문으로의 특정 변환을 지정할 수 있거나, 복호화 중에는 그 반대로

지정할 수 있다. 키들은 디지털 서명 스킴 및 메시지 인증 코드들과 같은 다른 암호화 알고리즘들에서도 사용될 수 있다. SSD의 키는 다른 엔티티에게 임의의 적합한 공유 비밀을 제공할 수 있다. 각각의 키 및 애플릿은 TSM 또는 인가된 에이전트에 의해 디바이스(100)의 보안 요소 상에 로딩되거나 또는 디바이스(100) 상에 처음 제공될 때 보안 요소 상에 미리 로딩될 수 있다. 하나의 예로서, 크리덴셜 SSD(154a)는 특정 신용 카드 크리덴셜과 연관될 수 있는 한편, 그 특정 크리덴셜은 그 크리덴셜 SSD(154a)의 애플릿(153a)이 인에이블될 때, 또는 그렇지 않으면 그러한 용도를 위해 활성화 또는 잠금해제될 때, 금융 거래를 위해 디바이스(100)의 보안 요소로부터(예컨대, NFC 컴포넌트(120)로부터) 판매자 서브시스템(200)에 상거래 크리덴셜 데이터 통신으로서만 통신될 수 있다.

[0039] 보안 특징들은 NFC 컴포넌트(120)의 사용을 인에이블하기 위해 제공될 수 있으며, 이는 크리덴셜의 신용 카드 정보 또는 은행 계좌 정보와 같은 기밀 결제 정보를 전자 디바이스(100)로부터 판매자 서브시스템(200)으로 (예컨대, 상업적 엔티티 서브시스템(400)을 통해 및/또는 디바이스(100')를 통해) 송신할 때 특히 유용할 수 있다. 그러한 보안 특징들은 또한 제한된 액세스를 가질 수 있는 보안 저장 영역을 포함할 수 있다. 예를 들어, 보안 저장 영역에 액세스하기 위해 개인 식별 번호("PIN") 입력을 통한 사용자 인증, 또는 생체인식 센서와의 사용자 상호작용을 통한 사용자 인증이 제공될 필요가 있을 수 있다. 예를 들어, 액세스 SSD(154b)는 다른 SSD(154)들(예컨대, 크리덴셜 SSD(154a))이 그것의 크리덴셜 정보(161a)를 통신하는데 사용되도록 허용하기 전에 그러한 인증이 발생했는지 여부를 결정하기 위해 애플릿(153b)을 레버리지할 수 있다. 소정 실시예들에서, 보안 특징들의 일부 또는 모두가 NFC 메모리 모듈(150) 내에 저장될 수 있다. 또한, 판매자 서브시스템(200)과 상거래 크리덴셜 데이터를 통신하기 위한 보안 정보, 예컨대 인증 키가 NFC 메모리 모듈(150) 내에 저장될 수 있다. 소정 실시예들에서, NFC 메모리 모듈(150)은 전자 디바이스(100) 내에 임베드된 마이크로컨트롤러를 포함할 수 있다. 단지 하나의 예로서, 액세스 SSD(154b)의 애플릿(153b)은 (예컨대, 생체인식 입력 컴포넌트와 같은 하나 이상의 입력 컴포넌트(110)를 통해) 디바이스(100)의 사용자의 의도 및 로컬 인증을 결정하도록 구성될 수 있으며, 그러한 결정에 응답하여, 결제 거래를 수행하기 위해 (예컨대, 크리덴셜 SSD(154a)의 크리덴셜을 이용하여) 다른 특정 SSD를 인에이블하도록 구성될 수 있다.

[0040] 도 2a의 설명

[0041] 이제 도 2a를 참조하면, 도 2a는 도 1 내지 도 2와 관련하여 기술한 시스템(1)의 전자 디바이스(100)의 일부분의 다른 상세도를 도시한다. 도 2a에 도시된 바와 같이, 예를 들어, NFC 컴포넌트(120)의 보안 요소(145)는 애플릿(153a), 크리덴셜 정보(161a), 액세스 키(155a) 및/또는 크리덴셜 키(155a')를 포함하거나 또는 이와 연관될 수 있는 SSD(154a) 및 애플릿(153b), 크리덴셜 정보(161b), 액세스 키(155b) 및/또는 크리덴셜 키(155b')를 포함하거나 그와 연관될 수 있는 SSD(154b)를 포함할 수 있다. 일부 실시예들에서, 특정 보충적 보안 도메인("SSD")(154)(예컨대, SSD(154a, 154b) 중 하나)은 전자 디바이스(100)에 특정 특권 또는 결제 권한을 제공할 수 있는 특정 TSM 및 적어도 하나의 특정 상거래 크리덴셜(예컨대, 특정 신용 카드 크리덴셜 또는 특정 대중 교통 카드 크리덴셜)과 연관될 수 있다. 각각의 SSD(154)는 NFC 디바이스 모듈(130)에 의한 사용을 위해 그 SSD(154)의 기능을 인에이블하도록 활성화될 필요가 있을 수 있는 자체 관리자 키(155)(예컨대, 키(155ak 및 155bk)의 각각)를 가질 수 있다. 부가적으로 또는 대안적으로, 각각의 SSD(154)는 그 자신의 크리덴셜 애플리케이션들 또는 특정 상거래 크리덴셜과 연관된 크리덴셜 애플릿들(예컨대, 자바(Java) 카드 애플릿 인스턴스들) 중 적어도 하나를 포함하고/하거나 그와 연관될 수 있으며(예컨대, SSD(154a)의 크리덴셜 애플릿(153a)은 제1 상거래 크리덴셜과 연관될 수 있고/있거나, SSD(154b)의 크리덴셜 애플릿(153b)은 제2 상거래 크리덴셜과 연관될 수 있음), 크리덴셜 애플릿에는 그 자신의 액세스 키(예컨대, 크리덴셜 애플릿(153a)에 대한 액세스 키(155a) 및/또는 크리덴셜 애플릿(153b)에 대한 액세스 키(155b)) 및/또는 그 자신의 크리덴셜 키(예컨대, 크리덴셜 애플릿(153a)에 대한 크리덴셜 키(155a') 및/또는 크리덴셜 애플릿(153b)에 대한 크리덴셜 키(155b'))가 있을 수가 있으며, 크리덴셜 애플릿은 (예컨대, 판매자 단말기(220)를 이용한) NFC 통신으로서 및/또는 전자 디바이스(100)와 판매자 서브시스템(200) 사이의 (예컨대, 상업적 엔티티 서브시스템(400) 및/또는 클라이언트 디바이스(100'))를 통한) 온라인 기반 통신으로서의 NFC 디바이스 모듈(130)에 의한 그것의 관련된 상거래 크리덴셜의 사용을 인에이블하기 위해 활성화될 필요가 있을 수 있다. 일부 실시예들에서, 크리덴셜 애플릿의 크리덴셜 키(예컨대, 크리덴셜 애플릿(153a)에 대한 크리덴셜 키(155a') 및/또는 크리덴셜 애플릿(153b)에 대한 크리덴셜 키(155b'))는, 그러한 크리덴셜에 대한 책임이 있을 수 있는 금융 기관 서브시스템(350)에 의해 생성될 수 있고, 보안 요소(145)와 금융 기관 서브시스템(350) 사이의 (예컨대, 판매자 서브시스템(200)을 통한) 그 애플릿의 그 크리덴셜 정보의 보안 송신을 인에이블하기 위해 금융 기관 서브시스템(350)에 의해 액세스가능할 수 있다(예컨대, 도 1b에 도시된 바와 같음). 부가적으로 또는 대안적으로, 크리덴셜 애플릿의 액세스 키(예컨대, 크리덴셜 애플릿(153a)에 대한 액세스 키(155a) 및/또는 크리덴셜 애플릿(153b)에 대한 액세스 키(155b))는 상

업적 엔티티 서브시스템(400)에 의해 생성될 수 있고, 보안 요소(145)와 상업적 엔티티 서브시스템(400) 사이의 그 애플릿의 그 크리덴셜 정보의 보안 송신을 인에이블하기 위해 상업적 엔티티 서브시스템(400)에 의해 액세스 가능할 수 있다(예컨대, 도 1b에 도시된 바와 같음). 부가적으로 또는 대안적으로, 도시된 바와 같이, 각각의 애플릿은 애플릿(153a)의 AID(155aa) 및/또는 애플릿(153b)의 AID(155ba)와 같은 그 자신 고유의 애플리케이션 식별자("AID")를 포함할 수 있다. 예를 들어, AID는 특정 카드 스킵 및 제품, 프로그램 또는 네트워크(예컨대, 마스터카드 시러스, 비자 플러스, 인터랙(Interac) 등)을 식별할 수 있으며, AID는 AID와 연관된 크리덴셜의 시스템의 결제 시스템(예컨대, 카드 스킵) 또는 네트워크(예컨대, 마스터 카드, 비자, 인터랙, 등)를 식별하는 데 사용될 수 있는 등록된 애플리케이션 공급자 식별자(registered application provider identifier)("RID") 뿐만 아니라, AID와 연관된 크리덴셜의 제공자 또는 결제 시스템에 의해 제공되는 제품들, 프로그램들 또는 애플리케이션들의 차이를 구별하는 데 사용할 수 있는 전용 애플리케이션 식별자 확장(proprietary application identifier extension)("PIX")을 포함할 수 있다. 보안 요소(145)의 펌웨어를 관장하기 위해 동작할 수 있는 임의의 적합한 사양(예컨대, 자바 카드 사양)은 보안 요소(145) 상의 각각의 AID의 고유성을 보장하거나, 그렇지 않으면 강요하도록 동작할 수 있다(예컨대, 보안 요소(145) 상의 각각의 크리덴셜 인스턴스는 그 자신 고유 AID와 연관될 수 있음).

[0042] 부가적으로 또는 대안적으로, 도 2a에 도시된 바와 같이, 보안 요소(145)는 ISD 키(156k)를 포함할 수 있는 ISD(152)를 포함할 수 있으며, ISD 키(156k)는 그 보안 도메인과 연관된 신뢰 서비스 관리자(예컨대, 도 1b에 도시된 바와 같이, 상업적 엔티티 서브시스템(400))에게도 공지될 수 있다. ISD 키(156k)는 디바이스(100)의 상업적 엔티티 서브시스템(400)과 보안 요소(145) 사이의 보안 송신을 인에이블하기 위해 액세스 키(155a) 및/또는 액세스 키(155b)와 유사하게 그리고/또는 그를 대신하여 상업적 엔티티 서브시스템(400) 및 전자 디바이스(100)에 의해 레버리될 수 있다. 또한, 도 2a에 도시된 바와 같이, 다양한 데이터가 프로세서(102)와 보안 요소(145) 사이에서 통신될 수 있다. 예를 들어, 디바이스(100)의 프로세서(102)는 프로세서(102)의 판매자 애플리케이션(113) 뿐만 아니라 보안 요소(145), I/O 인터페이스 컴포넌트(114a)(예컨대, I/O 입력 데이터(115i)의 수신용 및/또는 I/O 출력 데이터(115o)의 송신용), 및/또는 통신 컴포넌트(106)와 정보를 통신할 수 있는 디바이스 애플리케이션(103)을 실행하도록 구성될 수 있다. 또한, 도시된 바와 같이, 프로세서(102)는 디바이스(100)와 원격 엔티티 사이의 보안 통신을 인에이블하기 위해 활용될 수 있는 디바이스 식별 정보(119)에 액세스를 가질 수 있다.

[0043] 부가적으로 또는 대안적으로, 도 2a에 도시된 바와 같이, 보안 요소(145)는 제3자 요소-상(on-element) 신뢰점(root of trust)으로서 기능하도록 구성될 수 있는 특수 목적 보안 도메인일 수 있는 제어 기관 보안 도메인(controlling authority security domain)("CASD")(158)을 포함할 수 있다. CASD(158)의 연관 애플리케이션은 다른 애플리케이션 및/또는 특정 관리 층(예컨대, 글로벌 플랫폼 관리 층)에 글로벌 서비스로서 요소-상 비밀 키 생성을 제공하도록 구성될 수 있다. CASD(158) 내에 사용될 수 있는 기밀 키 자료는 보안 요소(145)의 발급자를 포함한 임의의 엔티티가 검사 또는 수정할 수 없도록 구성될 수 있다. CASD(158)는 CASD 액세스 키(158k)(예컨대, CASD 개인 키("CASD-SK"), CASD 공개 키(CASD-PK)), CASD 인증서("CASD-Cert.") 및/또는 CASD 서명 모듈)를 포함하도록 구성될 수 있고/있거나, 이들을 생성하고/하거나 그렇지 않으면 포함하도록 구성될 수 있다. 예를 들어, CASD(158)는 (예컨대, CASD 액세스 키(158k)를 사용하여) 보안 요소(145) 상에 소정 데이터를 서명한 후 디바이스(100)의 다른 부분(예컨대, 시스템(1)의 다른 서브시스템들과 공유하기 위한 통신 컴포넌트(106))에 그러한 데이터를 제공하도록 구성될 수 있다. 예를 들어, CASD(158)는 보안 요소(145)에 의해 제공되는 임의의 데이터에 서명하도록 구성되어, 다른 서브시스템들(예컨대, 상업적 엔티티 서브시스템(400))이 (예컨대, 상업적 엔티티 서브시스템(400)에서 연관된 CASD 키(158k)를 사용하여) 그러한 서명된 데이터가 보안 요소(145)에 의해 서명된 것을 확인하는 것이 가능할 수 있다.

[0044] 부가적으로 또는 대안적으로, 도 2a에 도시된 바와 같이, 보안 요소(145)는 특정 보안 도메인 요소의 수명 주기 상태(예컨대, 활성화, 비활성화, 잠금 등)를 수정하고, 특정 수명 주기 상태에서의 특정 보안 도메인 요소에 관한 특정 출력 정보(115o)를 디바이스(100)의 사용자와 (예컨대, 사용자 I/O 인터페이스(114a)를 통해) 공유하기 위해 전자 디바이스(100)에 로컬 기능을 제공하도록 구성될 수 있는 비접촉식 레지스트리 서비스(contactless registry services)("CRS") 애플릿 또는 애플리케이션(151)을 포함할 수 있다. 예컨대, CRS 애플리케이션(151)은 보안 요소(145) 상의 각각의 보안 도메인 요소의 현재 수명 주기 상태의 리스트를 유지할 수 있는 CRS 리스트(151t)(예컨대, SSD(154a)의 크리덴셜 애플릿(153a) 및/또는 SSD(154b)의 크리덴셜 애플릿(153b) 중 하나, 일부 또는 전부의 수명 주기 상태를 포함할 수 있는 리스트)를 포함할 수 있고, CRS 애플리케이션(151)은 보안 요소(145)의 하나 이상의 보안 도메인 요소들의 수명 주기 상태를, 디바이스(100)의 애플리케이션과(예컨대, 운영 체제 애플리케이션(103) 및/또는 카드 관리 애플리케이션(113b)(예컨대, 애플 링크.의 패스북

(Passbook)TM 또는 월렛(Wallet)TM 애플리케이션) 및/또는 판매자 애플리케이션(113c)(예컨대, 판매자 키(157)와 연관될 수 있는 판매자 애플리케이션), 및/또는 아이덴티티 서비스("IDS") 애플리케이션(113d) 내의 백그라운드 프로세스로서 실행될 수 있으나 디바이스(100)의 상호작용 사용자의 제어 하에 있을 필요는 없는, 데몬과 같은 카드 관리 데몬("CMD") 애플리케이션(113a)과 같은 임의의 적합한 애플리케이션 유형과) 공유하도록 구성될 수 있고, 이는 이어서, I/O 인터페이스(114a) 및 사용자 인터페이스("UI") 애플리케이션(예컨대, 카드 관리 애플리케이션(113b)의 UI)을 통해, 출력 정보(115o)로서 디바이스(100)의 사용자에게 소정 수명 주기 상태 정보를 제공할 수 있으며, 이는 (예컨대, CRS 리스트(151t) 및 보안 도메인 요소의 수명 주기 상태를 업데이트하기 위해, 예를 들어, 금융 거래의 용도를 위한 특정 크리덴셜 애플릿의 상거래 크리덴셜을 인에이블하기 위해) 사용자가 보안 도메인 요소의 수명 주기 상태를 변경하는 것을 가능하게 할 수 있다. 부가적으로 또는 대안적으로, CRS(151)는 CRS(151)와 연관된 신뢰 서비스 관리자(예컨대, 도 1b에 도시된 바와 같은 상업적 엔티티 서브시스템(400))에게 또한 공지될 수 있는 CRS 액세스 키(151k)를 포함할 수 있다. CRS 액세스 키(151k)는 전자 디바이스(100)의 상업적 엔티티 서브시스템(400)과 보안 요소(145) 사이의 보안 송신을 인에이블하기 위해 액세스 키(155a) 및/또는 액세스 키(155b)와 유사하게 그리고/또는 그 대신에 상업적 엔티티 서브시스템(400) 및 전자 디바이스(100)에 의해 레버리질될 수 있다.

[0045] IDS 애플리케이션(113d)은 운영 체제 애플리케이션(103) 및/또는 카드 관리 애플리케이션(113b) 내에서 백그라운드 프로세스로서 실행될 수 있고/있거나, CMD 애플리케이션(113a)에 의해 제공될 수 있으며, 임의의 적합한 IDS 서비스를 통해 전송될 수 있는 IDS 메시지를 청취하고 그 IDS 메시지에 응답하기 위한 IDS 관리자로서 동작할 수 있는 데몬과 같은, 임의의 적합한 애플리케이션 유형일 수 있다. 이는 애플 인크.의 아이메시지TM 등(예컨대, 애플 인크.의 페이스타임(FaceTime)TM 또는 ContinuityTM)과 같은 임의의 적합한 메시징 서비스와 유사할 수 있으며, 이는 호스트 디바이스(100)의 IDS 애플리케이션(113d)과 다른 디바이스(예컨대, 클라이언트 디바이스(100'))의 IDS 애플리케이션)의 유사한 IDS 애플리케이션 사이의 메시지의 고유한 종단 간 암호화를 인에이블할 수 있다. 그러한 메시지들은 통신 디바이스들 중 하나 또는 둘 모두에 대한 고유 식별자들(예컨대, 호스트 디바이스 고유 식별자(119) 및/또는 클라이언트 디바이스 고유 식별자(119')) 및/또는 통신 디바이스들의 특정 사용자들 중 하나 또는 둘 모두에 대한 고유 식별자들을 사용하여 암호화될 수 있다. 그러한 메시지들은 로컬 링크로서 통신되거나 또는 실제로 디바이스들(예컨대, 피어 투 피어) 통신될 수 있고, 또는 (예컨대, 아이덴티티 관리 시스템 컴포넌트(470)를 통해) 상업적 엔티티 서브시스템(400)을 통해 통신될 수 있다. 그러한 메시지들은 구조화된 형식들(예컨대, 프로토콜 버퍼들) 및/또는 구조화되지 않은 형식들로 데이터가 교환되도록 허용할 수 있는 저 레이턴시 솔루션으로 인에이블될 수 있다. IDS 애플리케이션(113d)은 IDS 메시지가 수신될 때 실행되는 중이 아니었다면 자동으로 어웨이크(awake) 상태가 될 수 있다. IDS 애플리케이션(113d)은 적절한 사용자 인터페이스를 제시하고, 수신된 IDS 통신의 요청된 데이터를 다시 요청 디바이스로 인도(shepherd)하도록 동작할 수 있다. 호스트 디바이스의 IDS 애플리케이션(113d)은, 클라이언트 디바이스로부터 초기 요청이 검출될 수 있을 때 카드 관리 애플리케이션(113b)의 카드 관리 데몬 애플리케이션(113a)을 웨이크 업(wake up)하도록 동작할 수 있으며, 이는 호스트 디바이스가 저전력 '슬립(sleep)'모드로 동작할 수 있게 한다. 부가적으로 또는 대안적으로 IDS 애플리케이션(113d)은, 클라이언트 디바이스로부터의 결제 요청에 대해 소정 기간(예컨대, 그러한 요청에 응답하는 활성 호스트 디바이스 사용자 상호작용이 없는 것에 기인하여, 60초) 동안 호스트 디바이스 상에서 반응하지 않을 경우, 그러한 요청에 대한 '타임 아웃'을 관리하도록 동작할 수 있으며, 이어서, IDS 애플리케이션(113d)은 요청을 종료하기로 결정하도록 동작할 수 있으며, 그 결과, 호스트 디바이스가 '취소' 상태를 생성하여 클라이언트 디바이스로 다시 전달할 수 있고, 이는 적절한 메시지(예컨대, 클라이언트 디바이스의 사용자에게 '타임 아웃 에러')를 디스플레이할 수 있다.

[0046] 도 3 및 도 3a 내지 도 3h의 설명

[0047] 도 3에 도시된 바와 같이, 그리고 이하에서 더욱 상세히 기술되는 바와 같이, 전자 디바이스(100)의 특정 예는 아이폰(iPhone)TM과 같은 핸드헬드 전자 디바이스일 수 있으며, 여기서 하우징(101)은 다양한 입력 컴포넌트(110a 내지 110i), 다양한 출력 컴포넌트(112a 내지 112c), 및 디바이스(100)와 사용자 및/또는 주변 환경이 그것들을 통해 서로 인터페이스할 수 있는 다양한 I/O 컴포넌트(114a 내지 114d)에 대한 액세스를 허용할 수 있다. 예를 들어, 터치 스크린 I/O 컴포넌트(114a)는 디스플레이 출력 컴포넌트(112a) 및 연관된 터치 입력 컴포넌트(110f)를 포함할 수 있으며, 여기서 디스플레이 출력 컴포넌트(112a)는, 사용자가 전자 디바이스(100)와 상호작용할 수 있게 하는 시각적 또는 그래픽 사용자 인터페이스("GUI")(180)를 디스플레이하는 데 사용될 수 있다. GUI(180)는, 디스플레이 출력 컴포넌트(112a)의 영역들 전체 또는 일부에 디스플레이될 수 있는, 다양한 계층, 윈도우, 스크린, 템플릿, 요소, 메뉴, 및/또는 현재 실행중인 애플리케이션(예컨대, 애플리케이션(103) 및/또는 애플리케이션(113) 및/또는 애플리케이션(143))의 다른 컴포넌트들을 포함할 수 있다. 예를 들어, 도 3에 도시

된 바와 같이, GUI(180)는 GUI(180)의 하나 이상의 그래픽 요소 또는 아이콘(182)을 갖는 제1 스크린(190)을 디스플레이하도록 구성될 수 있다. 특정 아이콘(182)이 선택되면, 디바이스(100)는 그 아이콘(182)과 연관된 새로운 애플리케이션을 열고 그 애플리케이션과 연관된 GUI(180)의 대응하는 스크린을 디스플레이하도록 구성될 수 있다. 예를 들어, "판매자 앱(Merchant App)" 텍스트 표시자(181)로 라벨링된 특정 아이콘(182)(즉, 특정 아이콘(183))이 디바이스(100)의 사용자에게 의해 선택될 때, 디바이스(100)는 특정 제3자 판매자 애플리케이션을 개시하거나 그렇지 않으면 액세스할 수 있고, 특정 방식으로 디바이스(100)와 상호작용하기 위한 하나 이상의 톨 또는 특징을 포함할 수 있는 특정 사용자 인터페이스의 스크린을 디스플레이할 수 있다(예컨대, 호스트 디바이스(100)의 NFC 컴포넌트(120)의 크리덴셜(예컨대, 크리덴셜 SSD(154a)의 크리덴셜)을 이용하여 결제를 하기 위해 디바이스 사용자에게 의해 사용될 수 있는 임의의 적합한 애플리케이션(호스트 디바이스(100) 상의 카드 관리 애플리케이션(113b) 및/또는 클라이언트 디바이스(100') 상의 판매자 애플리케이션(113'))의 사용 중의 GUI(180)의 그러한 디스플레이들에 대한 특정 예들은 예컨대, 도 3a 내지 도 3h를 참조한다). 각각의 애플리케이션에 대해, 스크린들이 디스플레이 출력 컴포넌트(112a) 상에 디스플레이될 수 있으며 다양한 사용자 인터페이스 요소를 포함할 수 있다. 부가적으로 또는 대안적으로, 각각의 애플리케이션에 대해, 다양한 다른 유형의 비-시각적 정보가 디바이스(100)의 다양한 다른 출력 컴포넌트(112)를 통해 사용자에게 제공될 수 있다.

[0048] 한편, 호스트 디바이스(100)와 관련하여 도 2 및 도 3을 설명하는데 있어서, 도 2 및 도 3의 임의의 하나 이상의 디바이스(100)의 컴포넌트 중 하나, 일부 또는 전부는 클라이언트 디바이스(100')에 의해 유사하게 제공될 수 있음이 이해되어야 한다. 일부 실시예에서, 호스트 디바이스(100)의 하나 이상의 컴포넌트는 클라이언트 디바이스(100')에 의해 제공되지 않을 수 있다(예컨대, 클라이언트 디바이스(100')는 하나 이상의 크리덴셜이 프로비저닝된 보안 요소를 포함하지 않을 수 있는 한편, 다른 실시예들에서, 클라이언트 디바이스(100')는 하나 이상의 네이티브 크리덴셜이 프로비저닝된 보안 요소를 또한 포함할 수 있으면서도, 여전히 클라이언트 디바이스(100')는 비-네이티브 크리덴셜(예컨대, 호스트 디바이스(100)에 네이티브한 크리덴셜)을 사용하여 금융 거래를 용이하게 할 수 있다. 일부 실시예들에서, 클라이언트 디바이스(100')는 GUI를 제공하도록 동작하는 사용자 인터페이스 컴포넌트를 포함하지 않고, 대신에 보다 자동화된 디바이스로 간주될 수 있다. 부가적으로 또는 대안적으로, 호스트 디바이스(100)는 GUI를 제공하도록 동작하는 사용자 인터페이스 컴포넌트를 포함하지 않고, 대신에 거래를 지불하기 위해 결제 크리덴셜의 사용을 선택 및 인증하기 위한 오디오 출력 컴포넌트 및 기계적 또는 다른 적합한 사용자 입력 컴포넌트를 제공할 수 있다.

[0049] 도 4의 설명

[0050] 이제 도 4를 참조하면, 도 4는 시스템(1)의 상업적 엔티티 서브시스템(400)의 특정 실시예들에 관한 추가의 상세사항을 도시한다. 도 4에 도시된 바와 같이, 상업적 엔티티 서브시스템(400)은 보안 플랫폼 시스템일 수 있고, 보안 모바일 플랫폼("SMP") 브로커 컴포넌트(440), SMP 신뢰 서비스 관리자("TSM") 컴포넌트(450), SMP 암호 서비스 컴포넌트(460), 아이덴티티 관리 시스템("IDMS") 컴포넌트(470), 사기 시스템 컴포넌트(fraud system component)(480), 하드웨어 보안 모듈("HSM") 컴포넌트(490), 저장 컴포넌트(420) 및/또는 하나 이상의 서버(410)를 포함할 수 있다. 상업적 엔티티 서브시스템(400)의 하나의, 일부의, 또는 모든 컴포넌트는, 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 하나 이상의 프로세서 컴포넌트, 디바이스(100)의 메모리 컴포넌트(104)와 동일하거나 유사할 수 있는 하나 이상의 메모리 컴포넌트, 및/또는 디바이스(100)의 통신 컴포넌트(106)와 동일하거나 유사할 수 있는 하나 이상의 통신 컴포넌트를 사용하여 구현될 수 있다. 상업적 엔티티 서브시스템(400)의 하나의, 일부의, 또는 모든 컴포넌트는, 금융 기관 서브시스템(350)과 별개이고 그에 독립적일 수 있는 단일 상업적 엔티티(예컨대, 애플 인크.)에 의해 관리되고, 소유되고, 적어도 부분적으로 제어되고 그리고/또는 그렇지 않으면 제공될 수 있다. 상업적 엔티티 서브시스템(400)의 컴포넌트들은 서로 상호작용하거나 새로운 보안 층을 제공하기 위해 그리고/또는 보다 끊임없는 사용자 환경을 제공하기 위해 금융 기관 서브시스템(350) 및/또는 호스트 전자 디바이스(100) 및/또는 클라이언트 전자 디바이스(100') 및/또는 판매자 서브시스템(200)과 집합적으로 상호작용할 수 있다.

[0051] 상업적 엔티티 서브시스템(400)의 SMP 브로커 컴포넌트(440)는 상업적 엔티티 사용자 계정을 이용하여 사용자 인증을 관리하도록 구성될 수 있다. SMP 브로커 컴포넌트(440)는 또한, 디바이스(100) 상의 크리덴셜들의 수명 주기 및 프로비저닝을 관리하도록 구성될 수 있다. SMP 브로커 컴포넌트(440)는 디바이스(100') 및/또는 디바이스(100) 상의 사용자 인터페이스 요소들(예컨대, GUI(180)의 요소들)을 제어할 수 있는 1차 종점(primary endpoint)일 수 있다. 최종 사용자 디바이스의 운영 체제 또는 다른 애플리케이션(예컨대, 애플리케이션(103), 애플리케이션(113), 및/또는 호스트 디바이스(100)의 애플리케이션(143))은 특정 애플리케이션 프로그래밍 인터페이스(application programming interface)("API")들을 호출하도록 구성될 수 있고, SMP 브로커(440)는 그 API

들의 요청들을 프로세싱하고 데이터로 응답하도록 구성될 수 있으며, 이는 디바이스(100)의 사용자 인터페이스를 도출하고 그리고/또는(예컨대, 상업적 엔티티 서브시스템(400)과 전자 디바이스(100) 사이의 통신 경로(65)를 통해) NFC 컴포넌트(120)의 보안 요소와 통신할 수 있는 애플리케이션 프로토콜 데이터 단위(application protocol data unit)("APDU")들로 응답할 수 있다. 그러한 APDU들은 시스템(1)의 신뢰 서비스 관리자("TSM") (예컨대, 상업적 엔티티 서브시스템(400)과 금융 기관 서브시스템(350) 사이의 통신 경로(55)의 TSM)를 통해 금융 기관 서브시스템(350)으로부터 상업적 엔티티 서브시스템(400)에 의해 수신될 수 있다. 상업적 엔티티 서브시스템(400)의 SMP TSM 컴포넌트(450)는, 금융 기관 서브시스템(350)으로부터 디바이스(100) 상의 크리덴셜 프로비저닝 동작들을 이행하는 데 사용될 수 있는 글로벌플랫폼-기반 서비스 또는 임의의 다른 적합한 서비스들을 제공하도록 구성될 수 있다. 글로벌플랫폼, 또는 임의의 다른 적합한 보안 채널 프로토콜은, SMP TSM 컴포넌트(450)로 하여금, 상업적 엔티티 서브시스템(400)과 금융 기관 서브시스템(350) 사이의 안전한 데이터 통신을 위해 TSM과 디바이스(100)의 보안 요소(145) 사이에서 민감한 계정 데이터를 제대로 통신 및/또는 프로비저닝하게 할 수 있다.

[0052]

SMP TSM 컴포넌트(450)는 HSM 컴포넌트(490)를 사용하여 그것의 키들을 보호하고 새로운 키들을 생성하도록 구성될 수 있다. 상업적 엔티티 서브시스템(400)의 SMP 암호 서비스 컴포넌트(460)는, 사용자 인증 및/또는 시스템(1)의 다양한 컴포넌트들 사이의 기밀 데이터 송신에 제공될 수 있는 키 관리 및 암호화 동작들을 제공하도록 구성될 수 있다. SMP 암호 서비스 컴포넌트(460)는 안전한 키 저장 및/또는 불분명한(opaque) 암호화 동작들을 위해 HSM 컴포넌트(490)를 활용할 수 있다. SMP 암호 서비스 컴포넌트(460)의 결제 암호 서비스는 IDMS 컴포넌트(470)와 상호작용하여, 파일-상(on-file) 신용 카드들과 연관된 정보 또는 상업적 엔티티의 사용자 계정들(예컨대, 애플 아이클라우드™ 계정)과 연관된 다른 유형들의 상거래 크리덴셜들을 검색하도록 구성될 수 있다. 그러한 결제암호 서비스는, 그것의 사용자 계정들의 상거래 크리덴셜들(예컨대, 신용 카드 번호들)을 설명하는 암호화되지 않은(clear) 텍스트(즉, 비-해싱된(non-hashed)) 정보를 메모리 내에 가질 수 있는 상업적 엔티티 서브시스템(400)의 유일한 컴포넌트이도록 구성될 수 있다. IDMS 컴포넌트(470)는 (예컨대, 상업적 엔티티 특정 서비스(예컨대, 애플 인크.에 의한 아이메시지™)를 사용하여 아이덴티티 서비스("IDS") 전송과 같은 호스트 디바이스(100)와 클라이언트 디바이스(100') 사이의 임의의 적합한 통신을 인에이블하고/하거나 관리하도록 구성될 수 있다. 예를 들어, 특정 디바이스들이 그러한 서비스를 위해 자동 또는 수동으로 등록될 수 있다(예컨대, 상업적 엔티티(400)의 생태계 내의 모든 디바이스가 서비스를 위해 자동으로 등록될 수 있음). 그러한 서비스는 메시지가 서비스를 사용하여(예컨대, 호스트 디바이스(100)의 IDS 애플리케이션(113d)을 사용하여) 전송될 수 있기 전에 활성 등록을 필요로 할 수 있는 중단 간 암호화 메커니즘을 제공할 수 있다. IDMS 컴포넌트(470) 및/또는 임의의 다른 적합한 서버 또는 상업적 엔티티 서브시스템(400)의 일부는 소정의 사용자 계정 또는 다른 것과 연관된 임의의 전자 디바이스 상에 프로비저닝된 임의의 크리덴셜을 식별 또는 그렇지 않으면 상태를 룩업(lookup)하도록 동작할 수 있으며, 따라서 상업적 엔티티 서브시스템(400)은 특정 사용자 계정과 연관된 특정 클라이언트 디바이스(예컨대, 상업적 엔티티 서브시스템(400)을 갖는 패밀리 계정의 다수의 호스트 디바이스)에 이용가능할 수 있는 하나 이상의 비-네이티브 결제 크리덴셜을 효율적이고 효과적으로 식별하도록 동작할 수 있다. 상업적 엔티티 서브시스템(400)의 상업적 엔티티 사기 시스템 컴포넌트(480)는, 상거래 크리덴셜 및/또는 사용자에게 관하여 상업적 엔티티에 알려진 데이터에 기초하여(예컨대, 상업적 엔티티와의 사용자 계정과 연관된 데이터(예컨대, 상거래 크리덴셜 정보) 및/또는 상업적 엔티티의 제어 하에 있을 수 있는 임의의 다른 적합한 데이터 및/또는 금융 기관 서브시스템(350)의 제어 하에 있지 않을 수 있는 임의의 다른 적합한 데이터에 기초하여), 상거래 크리덴셜에 대해 상업적 엔티티 사기 체크를 실행하도록 구성될 수 있다. 상업적 엔티티 사기 시스템 컴포넌트(480)는 다양한 인자 또는 임계치에 기초하여 크리덴셜에 대한 상업적 엔티티 사기 점수를 결정하도록 구성될 수 있다. 부가적으로 또는 대안적으로, 상업적 엔티티 서브시스템(400)은 저장소(420)를 포함할 수 있으며, 이는 디바이스(100)의 사용자들에 대한 다양한 서비스의 제공자일 수 있다(예컨대, 디바이스(100/100')에 의해 재생되는 미디어를 판매/대여하기 위한 아이튠즈™ 스토어, 디바이스(100/100') 상에서 사용할 애플리케이션들을 판매/대여하기 위한 애플 앱 스토어™, 디바이스(100/100')로부터의 데이터를 저장하고/하거나 다수의 사용자 디바이스들 및/또는 다수의 사용자 프로파일을 서로 연관시키기 위한 애플 아이클라우드™ 서비스, 다양한 애플 제품을 온라인에서 구입하기 위한 애플 온라인 스토어 등). 단지 하나의 예로서, 저장소(420)는 애플리케이션(113)을 관리하고 이를 디바이스(100)에 (예컨대, 통신 경로(65)를 통해) 제공하도록 구성될 수 있으며, 여기서 애플리케이션(113)은 बैंक 애플리케이션, 상업적 판매자 애플리케이션, 이메일 애플리케이션, 텍스트 메시징 애플리케이션, 인터넷 애플리케이션, 카드 관리 애플리케이션, 또는 임의의 다른 적합한 통신 애플리케이션과 같은 임의의 적합한 애플리케이션일 수 있다. 임의의 적합한 통신 프로토콜 또는 통신 프로토콜들의 조합이, 상업적 엔티티 서브시스템(400)의 다양한 컴포넌트들 사이에서 (예컨대, 도

4의 적어도 하나의 통신 경로(495)를 통해) 데이터를 전달하고/하거나 상업적 엔티티 서브시스템(400)과 시스템(1)의 다른 컴포넌트들 사이에서(예컨대, 도 1a의 통신 경로(55)를 통한 금융 엔티티 서브시스템(350) 및/또는 도 1a의 통신 경로(65)를 통한 호스트 전자 디바이스(100) 및/또는 도 1a의 통신 경로(95)를 통한 클라이언트 전자 디바이스(100')) 데이터를 통신하기 위해 상업적 엔티티 서브시스템(400)에 의해 사용될 수 있다.

[0053] 도 5의 설명

[0054] 도 5는 비-네이티브 결제 크리덴셜과 함께 전자 디바이스를 사용하여 금융 거래를 수행하기 위한 예시적인 프로세스(500)의 흐름도이다. 프로세스(500)는 호스트 전자 디바이스(100), 클라이언트 전자 디바이스(100'), 판매자 서브시스템(200), 매입 은행 서브시스템(300), 상업적 엔티티 서브시스템(400) 및 금융 기관 서브시스템(350)에 의해 구현되는 것으로 도시된다. 그러나, 프로세스(500)는 임의의 다른 적합한 컴포넌트들 또는 서브시스템들을 사용하여 구현될 수 있다는 것이 이해되어야 한다. 프로세스(500)는 호스트 디바이스(100)로부터의 결제 크리덴셜을 사용하면서 클라이언트 디바이스(100')를 통해 판매자 서브시스템(200)과의 안전하고 효율적으로 금융 거래를 수행하기 위한 끊임없는 사용자 경험을 제공할 수 있다.

[0055] 프로세스(500)의 단계(502)에서, 잠재 거래 데이터는 판매자 서브시스템(200)으로부터 클라이언트 디바이스(100')에게 통신될 수 있다. 예를 들어, 판매자 애플리케이션(113')을 실행 중인 클라이언트 디바이스(100')와 의 사용자 상호작용 동안의 어떤 시점에서(예컨대, 사용자가 판매자의 상품 또는 서비스에 대해 온라인 쇼핑을 하는 동안), 판매자 서브시스템(200)으로부터 또는 임의의 다른 적합한 엔티티로부터 잠재 거래 데이터가 클라이언트 디바이스(100')에 통신될 수 있으며, 이는 클라이언트 디바이스(100')의 사용자와 판매자 서브시스템(200)의 판매자 사이에 발생할 잠재적 금융 거래와 관련된 임의의 적합한 데이터를 나타낼 수 있는 것으로서, 이에 제한되지는 않으나, 다음을 포함할 수 있다. (i) 특정 판매자 정보, 예컨대, 고유 판매자 식별자, (ii) 특정 거래 정보, 예컨대, 거래를 위해 결제하는 데 사용될 특정 화폐(예컨대, 엔, 파운드, 달러 등)의 식별, 및/또는 거래를 위해 결제될 특정 화폐 금액의 식별, 및/또는 구매 또는 임대 또는 그렇지 않으면 결제될 특정 제품 또는 서비스의 식별, 및/또는 사용될 디폴트 또는 초기 배송 주소의 식별, (iii) 거래를 위해 판매자에게 수령가능한 하나 이상의 유형의 결제 방법을 나타내는 정보(예컨대, 구매에 사용될 수 있는 결제 카드들(예컨대, 비자를 제외한 마스터카드)의 리스트), 및/또는 (iv) 고유 판매자-기반 거래 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행 중인 거래와의 연관을 위해 판매자 서브시스템(200)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열). 그러한 잠재 거래 데이터는, 적어도 금융 거래를 완료하는 데 요구되거나 적어도 사용될 수 있는, 연관 데이터를 갖거나 갖지 않는 임의의 적합한 수 및 유형의 데이터 필드를 포함할 수 있으며, 예컨대, 구매 중인 고객의 연락처 정보 필드들(예컨대, 전화 번호, 이메일 주소, 우편 주소)로서, 일부 필드들은 기입되어(populated) 그러한 잠재 거래 데이터의 일부로서 포함될 수 있고/있거나 일부 필드들은 그러한 잠재 거래 데이터의 일부로서 기입되지 않은 채 프로세스(500) 동안 오픈되어 지정되기를 대기할 수도 있다. 단계(502)의 그러한 잠재 거래 데이터는 본 명세서에서 PKPaymentRequest로 지칭될 수 있다. 대안적으로, 일부 실시예들에서, 사용자는 단계(502)에서 판매자 서브시스템(200)과 연관된 잠재 거래 데이터가 클라이언트 디바이스(100')에 이용가능해지도록 클라이언트 디바이스(100')와 능동적으로 상호작용하지 않을 수 있다. 대신에, 예를 들어, 클라이언트 디바이스(100')는 특정 제품이 구매되어야 하고, 그 특정 제품에 대해 적어도 하나의 특정 판매자로부터 연관된 거래 데이터를 획득하기 위해 하나 이상의 판매자와 상호작용해야 한다고 결정하도록 구성될 수 있으며(예컨대, 클라이언트 디바이스(100')는 가전기기 제품이 구매되어야 한다고 결정하고(예컨대, 세탁기에 더 많은 세탁 세제가 필요하다고 검출하거나, 특정 일자에 더 많은 세제를 구매하도록 사용자에게 의해 미리 설정된 달력 이벤트를 검출하고), 그 제품에 대해 최상의 거래를 제공하는 특정 판매자를 자동으로 식별하고, 해당 판매자로부터 해당 제품을 구매하기 위해 해당 판매자와 자동으로 상호작용하여 거래 데이터를 획득하도록 구성될 수 있는 가전기기일 수 있음), 모든 것이 자동으로 그리고 클라이언트 디바이스(100')의 사용자에게 의한 임의의 능동적 개입이 없이 이루어진다. 단계(502)의 잠재 거래 데이터는 클라이언트 디바이스(100') 또는 클라이언트 디바이스(100')와 연관하여 이용가능한 호스트 디바이스(100)가 잠재 거래 데이터와 연관된 금융 거래를 지불하기 위해 결제 크리덴셜 데이터를 안전하게 생성하여 판매자 서브시스템(200)에 제공하는 데 필요한 모든 데이터를 포함할 수 있다. 그러한 잠재 거래 데이터는 임의의 적합한 방식으로 단계(502)에서 판매자 서브시스템(200)에 의해 클라이언트 디바이스(100')로 통신될 수 있다(예컨대, 그러한 잠재 거래 데이터는 판매자 서브시스템(200)의 서버(210)로부터 임의의 적합한 통신 프로토콜을 사용하여 통신 경로(15)를 통하거나 또는 임의의 적합한 통신 프로토콜을 사용하여 단말기(220)과 NFC 컴포넌트(120') 사이의 비접촉식 근접-기반 통신 채널을 통해 클라이언트 디바이스(100')의 통신 컴포넌트(106')로 송신될 수 있음).

[0056] 프로세스(500)의 단계(504)에서, 단계(502)의 거래 데이터와 연관된 거래와 같은 금융 거래를 잠재적으로 지불하기 위해 적어도 하나의 이용가능한 비-네이티브 결제 소스가 식별될 수 있다. 이것은 단계(502)에서 거래 데이터를 수신하는 것에 응답하여 클라이언트 디바이스(100')에 의해 자동으로 달성될 수 있거나, 또는 거래 데이터의 수신과 독립적으로 주기적으로 달성될 수 있거나, 임의의 적합한 시간에 클라이언트 디바이스(100')의 사용자에게 의해 생성된 요청에 응답하여 달성될 수 있다. 예를 들어, 단계(502)에서 클라이언트 디바이스(100')에 의해 수신된 잠재 거래 데이터에 응답하여, 클라이언트 디바이스(100')는 단계(502)의 거래 데이터와 연관된 금융 거래를 적어도 부분적으로 지불하는데 이용가능할 수 있는 적어도 하나의 호스트 전자 디바이스(예컨대, 보안 요소 상에 결제 크리덴셜 데이터를 생성하도록 구성될 수 있는 호스트 디바이스(100)와 같은 임의의 전자 디바이스)를 식별하도록 시도하도록 동작될 수 있다. 임의의 이용가능한 비-네이티브 결제 소스를 식별하기 위해 임의의 적합한 기술을 사용할 수 있다. 예를 들어, 비콘 신호는 클라이언트 디바이스(100')에 의해 디스커버리 요청으로서 송신될 수 있고 이는 비콘을 수신할 수 있는 임의의 호스트 디바이스로부터 응답을 요청할 수 있다(예컨대, 클라이언트 디바이스(100')와 특정 거리 내에서 비콘의 특정 통신 프로토콜을 사용하여 통신하도록 동작하는 임의의 호스트 디바이스, 또는 비콘은 빠른 응답("QR") 코드 또는 클라이언트 디바이스(100')에 의해 제시되고 하나 이상의 호스트 디바이스의 스캐너에 의해 관독될 수 있는 임의의 적합한 코드일 수 있음). 대안적으로 또는 부가적으로, 클라이언트 디바이스(100')는 임의의 적합한 통신 경로 및 프로토콜을 사용하여 하나 이상의 특정 호스트 디바이스(예컨대, 디바이스(100'))의 연락처 애플리케이션에서 식별되고/되거나 디바이스(100')의 사용자에게 의해(예컨대, 전화 번호 또는 이메일 주소 또는 임의의 적합한 고유 디바이스 식별자(예컨대, 호스트 디바이스(100)의 디바이스 식별자(119)에 의해) 수동으로 식별된 하나 이상의 디바이스)에 디스커버리 요청을 전송할 수 있다. 그러한 디스커버리 요청은 임의의 적합한 정보, 예컨대, 클라이언트 디바이스(100')를 식별하는 정보(예컨대, 클라이언트 디바이스(100')의 디바이스 식별자(119')), 및/또는 잠재적 금융 거래를 지불하기 위해(예컨대, 판매자에 의해) 수령가능할 수 있는 하나 이상의 특정 결제 유형(예컨대, 단계(502)의 잠재 거래 데이터에 의해 식별될 수 있는 결제 유형(들))을 식별하는 정보를 포함할 수 있으며, 응답으로, 임의의 적합한 정보, 예컨대, 응답하는 호스트 디바이스를 식별하는 임의의 적합한 정보(예컨대, 호스트 디바이스(100)의 디바이스 식별자(119)) 및/또는 그 호스트 디바이스에 이용가능할 수 있는 하나 이상의 특정 결제 유형을 식별하는 임의의 적합한 정보(예컨대, 호스트 디바이스(100)의 AID(155aa) 및/또는 AID(155ba), 여기서 응답의 그러한 결제 유형 식별은 디스커버리 요청의 유형과 일치하는 각각의 유형을 단지 포함하거나 응답하는 호스트에 이용가능한 모든 결제 유형을 포함할 수 있음) 및/또는 응답하는 호스트 디바이스의 위치를 식별하는 임의의 적합한 정보 및/또는 호스트 디바이스의 상태(예컨대, 어웨이크 상태, 슬립 상태, 전원 오프 상태, 등)를 식별하는 임의의 적합한 정보를 요청할 수 있다.

[0057] 단계(504)에서, 상업적 엔티티 서브시스템(400) 또는 임의의 다른 엔티티는 클라이언트 디바이스(100')에 의한 호스트 디바이스(100)의 식별에 참여할 수 있다. 예를 들어, 전술한 바와 같이, 상업적 엔티티 서브시스템(400)은 아이클라우드™ 및/또는 아이메시지™ 또는 임의의 다른 적합한 아이덴티티 서비스 전송과 같은 클라이언트 디바이스(100') 및/또는 호스트 디바이스(100)에 이용가능하게 된 임의의 적합한 서비스를 관리하도록 동작할 수 있으며, 상이한 디바이스들 사이의 연관을 짓고/짓거나 다양한 디바이스들의 상태 및/또는 성능을 자동으로 결정하도록 동작할 수 있다(예컨대, 일가족이 클라이언트 디바이스(100') 뿐만 아니라, 호스트 디바이스(100)를 포함하는 다수의 다른 디바이스와 연관될 수 있는 상업적 엔티티 서브시스템(400)의 계좌를 가질 수 있음). 하나의 예로서, 단계(504)는 클라이언트 디바이스(100')에서, 클라이언트 디바이스(100')의 계정과 연관된 모든 다른 디바이스의 상태에 대해 상업적 엔티티 서브시스템(400)에 디스커버리 요청을 전송하는 단계, 및 상업적 엔티티 서브시스템(400)에서, 그러한 디바이스들 중 하나, 일부 또는 각각의 상태를(예컨대, 아이덴티티 서비스 전송 또는 그 외의 것을 사용하여) 획득하고, 이들 상태들 중 각각을 클라이언트 디바이스(100')와 공유하는 단계를 포함할 수 있으며, 상태는 호스트 디바이스(100)의 이용가능성 및 호스트 디바이스(100)에 이용가능한 적어도 하나의 결제 유형의 아이덴티티를 나타낼 수 있다(예컨대, 호스트 디바이스 식별자, AID(들) 및 각각의 결제 애플리케이션의 상태(예컨대, 비자/인앱(Visa/in-app) 인에이블되고, 디스커버/인앱(Discover/in-app) 디스에이블) 및/또는 디바이스 자체의 상태). 각각의 호스트 디바이스는 그러한 요청들 및 잠재 응답들에 대하여 그의 자체 설정을 가질 수 있다(예컨대, 특정 호스트 디바이스는 다만 특정 클라이언트 디바이스들(예컨대, 다만 상업적 엔티티 서브시스템(400)의 동일한 계정과 연관된 디바이스들, 다만 그 특정 호스트 디바이스의 연락처 애플리케이션 내의 연락처와 연관된 디바이스들 등)로부터의 상태 요청에만 응답하도록 구성될 수 있음). 단계(504)에서 하나 이상의 이용가능한 결제 소스의 식별을 인에이블하기 위한 그러한 디스커버리 요청 및/또는 디스커버리 응답은 임의의 적합한 방식으로 통신될 수 있으며, 예컨대, 클라이언트 디바이스(100')와 호스트 디바이스(100) 사이에서(예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(99)를

통해) 직접(예컨대, 피어-투-피어), 또는 클라이언트 디바이스(100')와 상업적 엔티티 서브시스템(400) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(95)를 통해), 및 상업적 엔티티 서브시스템(400)과 호스트 디바이스(100) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(65)를 통해) (예컨대, 아이덴티티 서비스 전송 또는 상업적 엔티티 서브시스템(400)의 임의의 다른 적합한 통신 서비스를 사용하여) 통신될 수 있다.

[0058]

프로세스(500)의 단계(506)에서, 클라이언트 디바이스(100')는 결제 요청 데이터를 적어도 하나의 특정 호스트 전자 디바이스(100)에 통신할 수 있다. 그러한 결제 요청 데이터는 지불될 잠재 거래의 하나 이상의 특정 특성들을 식별하기 위해 클라이언트 디바이스(100')에 의해 제공될 수 있는 임의의 적합한 정보를 포함할 수 있다. 예를 들어, 단계(502)의 잠재 거래 데이터와 마찬가지로, 단계(506)의 결제 요청 데이터는 지불될 잠재적 금융 거래와 관련된 임의의 적합한 데이터를 포함할 수 있으며, 이에 제한되지는 않으나, 다음을 포함할 수 있다. (i) 특정 판매자 정보, 예컨대, 단계(502)의 잠재 거래 데이터의 적어도 일부분을 제공한 특정 판매자 서브시스템(200)을 식별할 수 있는 판매자 식별자의 식별, (ii) 특정 거래 정보, 예컨대, 거래를 위해 결제하는 데 사용될 특정 화폐(예컨대, 엔, 파운드, 달러 등)의 식별, 및/또는 거래를 위해 결제될 특정 화폐 금액의 식별, 및/또는 구매 또는 임대 또는 그렇지 않으면 결제될 특정 제품 또는 서비스의 식별, 및/또는 사용될 디폴트 또는 초기 배송 주소의 식별, (iii) 거래를 위해 판매자에게 수령가능한 하나 이상의 유형의 결제 방법을 나타내는 정보(예컨대, 구매에 사용될 수 있는 결제 카드들(예컨대, 비자를 제외한 마스터카드)의 리스트), (iv) 고유 판매자-기반 거래 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행 중인 거래와의 연관을 위해 판매자 서브시스템(200)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열), (v) 고유 클라이언트-기반 거래 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행 중인 거래와의 연관을 위해 클라이언트 디바이스(100')에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열), 및/또는 (vi) 고유 클라이언트-기반 결제 요청 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 진행 중인 결제 요청과의 연관을 위해 클라이언트 디바이스(100')에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열). 일부 실시예들에서, 그러한 결제 요청 데이터는 목표 호스트 디바이스(100)에 통신되기 전에 상업적 엔티티 서브시스템(400)에 의해 암호화되거나 그렇지 않으면, 포맷 또는 핸들링될 수 있다. 단계(506)의 결제 요청 데이터에 대한 목표 호스트 디바이스(100)는 단계(504)에서 (예컨대, 단계(504)의 임의의 적합한 디스커버리 응답에 기초하여) 임의의 이용가능한 결제 소스의 식별에 기초하여 선택될 수 있거나, 단계(504)에서 이루어진 임의의 식별과 독립적으로 선택될 수 있다. 단계(506)의 결제 요청 데이터는 (예컨대, 단계(504)에서 클라이언트 디바이스(100')에 의해 획득된 임의의 식별 데이터(예컨대, 호스트 디바이스 AID 데이터) 또는 그 외의 것에 기초하여) 목표 호스트 디바이스에 이용가능하도록 클라이언트 디바이스(100')에 의해 공지될 수 있는 특정 결제 유형의 식별자를 포함할 수 있다. 클라이언트 디바이스(100')의 사용자는 단계(504)에서 하나 이상의 결제 소스의 식별에 기초하여 제공될 수 있는 잠재적 목표 호스트 디바이스의 리스트로부터 단계(506)의 결제 요청 데이터에 대한 목표 호스트 디바이스(100)를 선택할 수 있거나, 또는 디바이스(100')는 임의의 적합한 방식으로 임의의 적합한 특정 목표 호스트 디바이스(예컨대, 디바이스(100')의 연락처 애플리케이션 내의 디바이스 및/또는 디바이스(100')의 사용자에 의해(예컨대, 전화 번호 또는 이메일 주소 또는 임의의 적합한 고유 디바이스 식별자에 의해) 수동으로 식별된 디바이스)를 식별할 수 있다. 대안적으로, 단계(506)의 결제 요청 데이터에 대한 목표 호스트 디바이스(100)는 단계(504)에서 클라이언트 디바이스(100')에 의해 획득된 임의의 식별 데이터에 응답하여 클라이언트 디바이스(100')에 의해 자동으로 선택될 수 있다(예컨대, 디바이스(100')는 임의의 적합한 특성에 기초하여 (예컨대, 디바이스(100')의 애플리케이션의 디폴트 또는 주문맞춤화된 설정에 의해 결정될 수 있는 바와 같이) 이용가능한 호스트 디바이스의 그룹으로부터 하나의 호스트 디바이스(예컨대, 클라이언트 디바이스(100')와의 최단 거리를 갖는 호스트 디바이스 또는 이용가능한 호스트 디바이스들 중 최고 우선순위를 갖는 호스트 디바이스 등)를 선택하도록 주문맞춤화되거나 그렇지 않으면 구성될 수 있음). 단계(506)의 그러한 결제 요청 데이터는 본 명세서에서 *PKRemotePaymentRequest*로 지칭될 수 있으며, 이에 제한되지는 않지만, 다음을 포함하는 임의의 적합한 데이터를 포함할 수 있다. (1) 단계(502)의 *PKPaymentRequest*(예컨대, 이는 *PKRemotePaymentRequest* 내에 래핑(wrap)될 수 있음), (2) 본 명세서에서 *PKRemoteDevice*로 지칭될 수 있는, 선택된 목표 호스트 디바이스를 식별하는 임의의 적합한 데이터(예컨대, 단계(504)의 디스커버리 응답에 포함될 수 있는 바와 같은, 호스트 디바이스(100)의 호스트 디바이스 식별자(119)), (3) 본 명세서에서 *SelectedApplicationIdentifier*로 지칭될 수 있는, 목표 호스트 디바이스의 선택되거나 디폴트인 특정 결제 크리덴셜(예컨대, 단계(504)의 디스커버리 응답에 포함될 수 있고, 클라이언트 디바이스(100')에서 자동으로 또는 사용자 선택될 수 있는, 호스트 디바이스(100)의 보안 요소(145)의 AID(155aa))을 식별하는 임의의 적합한 데이터, 및/또는 (4) 본 명세서에서 *RemotePaymentIdentifier*로 지칭될 수 있는, 결제

요청과 연관되는 고유 식별자(예컨대, 클라이언트 및 시스템의 호스트 디바이스를 통해 결제 요청을 식별하는데 사용될 수 있고 클라이언트 디바이스(100) 또는 그 외의 것에 의해 생성될 수 있는 고유 값)를 식별하는 임의의 적합한 데이터. 그러한 결제 요청 데이터는 단계(506)에서 임의의 적합한 방식으로 통신될 수 있으며, 예컨대, 클라이언트 디바이스(100')와 호스트 디바이스(100) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(99)를 통해) 직접(예컨대, 피어-투-피어), 또는 클라이언트 디바이스(100')와 상업적 엔티티 서비스 시스템(400) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(95)를 통해), 및 상업적 엔티티 서비스 시스템(400)과 호스트 디바이스(100) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(65)를 통해) (예컨대, 아이덴티티 서비스 전송 또는 상업적 엔티티 서비스 시스템(400)의 임의의 다른 적합한 통신 서비스를 사용하여) 통신될 수 있다.

[0059]

프로세스(500)의 단계(508)에서, 호스트 결제 크리덴셜 데이터는 호스트 디바이스(100)에 의해 적어도 부분적으로 생성될 수 있고, 이어서, 단계(510)에서, 호스트 결제 크리덴셜 데이터는 호스트 거래 데이터로서 호스트 디바이스(100)에 의해 상업적 엔티티 서비스 시스템(400)에 통신될 수 있다. 예를 들어, 단계(506)에서 결제 요청 데이터를 수신하는 것에 응답하여, 호스트 디바이스(100)는 거래를 지불하려고 시도하는 데 사용되는 보안 요소(145)의 특정 크리덴셜을 (예컨대, 단계(506)의 결제 요청 데이터의 *SelectedApplicationIdentifier*에 기초하여) 식별하도록 동작할 수 있으며, 그 특정 크리덴셜과 연관된 호스트 결제 크리덴셜 데이터가 단계(508)에서 생성되고, 이어서, 단계(510)에서 호스트 거래 데이터(예컨대, *PKPaymentRequest*의 판매자의 식별)로서 단계(506)의 결제 요청 데이터의 적어도 일부와 함께 통신될 수 있다. 그러한 호스트 결제 크리덴셜 데이터는 호스트 디바이스(100)의 특정 보안 요소 크리덴셜(예컨대, SSD(154a)의 크리덴셜)의 적합한 소유권을 안전하게 증명하도록 동작할 수 있는 임의의 적합한 데이터를 포함할 수 있으며, 이에 제한되지는 않으나, 다음을 포함할 수 있다. (i) 토큰 데이터(예컨대, DPAN, DPAN 만료 일자 및/또는 SSD(154a)의 크리덴셜 정보(161a)의 CVV), 및 (ii) 암호화 데이터(예컨대, SSD(154a)와 금융 기관 서비스 시스템(350)의 공유 비밀(예컨대, 키(155a'))을 사용하여 보안 요소(145)에 의해 생성될 수 있는 암호문, 및 공유 비밀을 사용하여 암호화 데이터를 독립적으로 생성하기 위해, (단계(520) 또는 그 외의 단계에서) 호스트 디바이스(100)에 이용가능할 수 있고, 그리고 금융 기관 서비스 시스템(350)에도 이용가능해질 수 있는 임의의 다른 적합한 정보(예컨대, 토큰 데이터의 일부 또는 전부, 호스트 디바이스(100)를 식별하는 정보, 단계(502)의 잠재 거래 데이터의 일부 또는 전부를 식별하는 정보, 예컨대, 비용 및/또는 화폐, 임의의 적합한 카운터 값, 논스(nonce) 등)). 이어서, 호스트 거래 데이터는 단계(510)에서 호스트 디바이스(100)로부터 상업적 엔티티 서비스 시스템(400)에게 통신될 수 있으며, 그러한 호스트 거래 데이터는 단계(508)에서 생성된 특정 호스트 결제 크리덴셜 데이터 뿐만 아니라 (예컨대, 단계(506)의 결제 요청 데이터에 의해 호스트 디바이스(100)에 제공될 수 있는) 지불될 잠재적 금융 거래와 관련된 임의의 다른 적합한 데이터를 포함할 수 있으며, 이는 이에 제한되지는 않으나, 다음을 포함할 수 있다. (i) 특정 판매자 정보, 예컨대, 단계(502)의 잠재 거래 데이터를 제공한 특정 판매자 서비스 시스템(200)을 식별할 수 있는 판매자 식별자의 식별, (ii) 특정 거래 정보, 예컨대, 거래를 위해 결제하는 데 사용될 특정 화폐(예컨대, 엔, 파운드, 달러 등)의 식별, 및/또는 거래를 위해 결제될 특정 화폐 금액의 식별, 및/또는 구매 또는 임대 또는 그렇지 않으면 결제될 특정 제품 또는 서비스의 식별, 및/또는 사용될 디폴트 또는 초기 배송 주소의 식별, (iii) 고유 판매자-기반 거래 식별자(예컨대, 수행 중인 거래와의 연관을 위해 판매자 서비스 시스템(200)에 의해 생성된 바와 같음), (iv) 고유 클라이언트-기반 거래 식별자(예컨대, 수행되는 거래와의 연관을 위해 클라이언트 디바이스(100')에 의해 생성된 바와 같음), (v) 고유 클라이언트-기반 결제 요청 식별자(예컨대, 결제 요청과의 연관을 위해 클라이언트 디바이스(100')에 의해 생성된 바와 같음), 및/또는 (v) 고유 호스트-기반 거래 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행 중인 거래와의 연관을 위해 호스트 디바이스(100)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열). 따라서, 단계(510)에서 호스트 디바이스(100)로부터 상업적 엔티티 서비스 시스템(400)으로 통신된 호스트 거래 데이터는 단계(502)의 잠재 거래 데이터의 및/또는 단계(506)의 결제 요청 데이터(예컨대, 판매자의 식별자)의 일부 또는 전부뿐만 아니라 디바이스(100)의 특정 크리덴셜에 기초하여 데이터의 적어도 2개의 유형 및/또는 분리가능한 부분을 포함할 수 있는, 단계(508)의 호스트 결제 크리덴셜 데이터(예컨대, 금융 기관 서비스 시스템(350)에 의해 수신될 때, 함께 더 안전한 금융 거래(예컨대, 암호문 검증)를 가능하게 할 수 있는 임의의 적합한 토큰 데이터 및 임의의 적합한 암호화 데이터)를 포함할 수 있다.

[0060]

호스트 디바이스(100)는 단계(510)에서 호스트 거래 데이터를 상업적 엔티티 서비스 시스템(400)에 통신하기 전에, 금융 기관 키를 이용하여 호스트 거래 데이터의 호스트 결제 크리덴셜 데이터의 전부 또는 적어도 일부분(예컨대, 호스트 결제 크리덴셜 데이터의 토큰 데이터 및/또는 암호화 데이터)을 암호화할 수 있다. 예를 들어, 보안 요소(145)는 금융 기관 서비스 시스템(350)에 또한 이용가능할 수 있는 요소(145)(예컨대, 크리덴셜 키(155

a'))를 확보하기 위해 이용가능한 임의의 적합한 크리덴셜 키 또는 요소를 이용하여 임의의 적합한 방식으로 호스트 거래 데이터의 적어도 일부분을 암호화 또는 서명할 수 있다. 대안적으로 또는 부가적으로, 호스트 디바이스(100)는 단계(510)에서 호스트 거래 데이터를 상업적 엔티티 서브시스템(400)에 통신하기 전에, (예컨대, 호스트 거래 데이터의 임의의 부분이 금융 기관 키를 이용하여 먼저 암호화된 안되던) 상업적 엔티티 키를 이용하여 호스트 거래 데이터의 전부 또는 호스트 거래 데이터의 적어도 일부분(예컨대, 호스트 결제 크리덴셜 데이터)을 암호화할 수 있다. 예컨대, 보안 요소(145)는 상업적 엔티티 서브시스템(400)에 또한 액세스가능할 수 있는 보안 요소(145)의 액세스 키(155a), 액세스 키(155b), CRS(151k) 및/또는 ISD 키(156k)(예컨대, 호스트 디바이스(100)와 상업적 엔티티 서브시스템(400) 사이의 임의의 공유 비밀)를 이용하여 호스트 거래 데이터의 적어도 일부분을 암호화할 수 있다. 대안적으로 또는 부가적으로, 보안 요소(145)는 상업적 엔티티 서브시스템(400)에 액세스가능할 수 있는 CASD(158k)를 이용하여 호스트 거래 데이터의 적어도 일부분을 서명할 수 있다. 일부 실시예들에서, 그러한 상업적 엔티티 키 또는 액세스 키는 상업적 엔티티 서브시스템(400)의 스킵과 연관된 상업적 엔티티 공개 키일 수 있으며, 상업적 엔티티 서브시스템(400)은 연관된 상업적 엔티티 개인 키에 대한 액세스를 가질 수 있다. 상업적 엔티티 서브시스템(400)은 그러한 상업적 엔티티 공개 키를 금융 기관 서브시스템(350)에 제공할 수 있고, 이어서, 금융 기관 서브시스템(350)은 ((예컨대, 프로세스(600)의 단계(604)에서) 예컨대, 호스트 디바이스(100)에 크리덴셜 데이터를 프로비저닝할 때) 그 상업적 엔티티 공개 키를 호스트 디바이스(100)와 공유할 수 있다. 호스트 거래 데이터는, 임의의 적합한 금융 기관 키 및/또는 임의의 상업적 엔티티 키에 의해 적어도 부분적으로 암호화 및/또는 서명되던 안되던 간에, 단계(510)에서 임의의 적합한 방식으로 호스트 디바이스(100)에 의해 상업적 엔티티 서브시스템(400)에 통신될 수 있다(예컨대, 그러한 호스트 거래 데이터는 임의의 적합한 통신 프로토콜을 사용하여 통신 경로(65)를 통해 상업적 엔티티 서브시스템(400)의 서버(410)로 호스트 디바이스(100)의 통신 컴포넌트(106)로부터 송신될 수 있음).

[0061]

다음으로, 단계(512)에서, 프로세스(500)는 호스트 결제 크리덴셜 데이터가 판매자 서브시스템(200) 이외의 임의의 엔티티와의 거래를 지불하기 위해 활용될 수 없도록, 상업적 엔티티 서브시스템(400)이 판매자 서브시스템(200)과의 공유 비밀을 사용하여 호스트 거래 데이터의 적어도 호스트 결제 크리덴셜 데이터를 암호화함으로써 단계(510)에서 수신된 호스트 거래 데이터를 추가로 보안하는 단계를 포함할 수 있다. 예컨대, 단계(510)의 호스트 거래 데이터가 임의의 상업적 엔티티 키를 이용하여 암호화된다면, 상업적 엔티티 서브시스템(400)은 단계(512)에서 그러한 데이터를 복호화하도록 동작될 수 있다(예컨대, 상업적 엔티티 서브시스템(400)의 서버(410)는 호스트 거래 데이터를 수신하고 이어서 (예컨대, 액세스 키(155a), 액세스 키(155b), CRS(151k), CASD(158k) 및/또는 상업적 엔티티 서브시스템(400)의 ISD 키(156k)를 이용하여) 그 호스트 거래 데이터를 복호화/서명해제(unsign)할 수 있다. 호스트 디바이스(100)와 상업적 엔티티 서브시스템(400) 사이에서 호스트 거래 데이터를 호스트 디바이스(100)와 상업적 엔티티 서브시스템(400) 둘 모두에 공지된 상업적 엔티티 키를 사용하여 암호화/서명된 형태로 통신함으로써, 프로세스(500)는 그 호스트 거래 데이터의 통신이 상업적 엔티티 키에 대한 액세스를 갖지 않는 엔티티에 의해 인터셉트되고 사용되는 것을 방지할 수 있다. 또한, 단계(512)에서, 상업적 엔티티 서브시스템(400)은 판매자 키(예컨대, 특정 거래가 지불되는 중인 판매자 서브시스템(200)과 연관될 수 있는 판매자 키(157) 및/또는 판매자 키(157'))를 이용하여 호스트 거래 데이터의 적어도 일부분을 암호화하거나 그렇지 않으면 재-포맷하도록 동작할 수 있다. 그러한 판매자 키는 테이블(430)을 통해 상업적 엔티티 서브시스템(400)에 의해 결정될 수 있고 액세스가능할 수 있다(예컨대, 단계(510)의 호스트 거래 데이터의 판매자 식별자와 연관된 판매자 키를 식별함에 의한 것으로, 이는 단계(506)의 결제 요청 데이터에 의해 클라이언트 디바이스(100')로부터 호스트 디바이스(100)에 제공된 것일 수 있고, 단계(506)의 결제 요청 데이터는 단계(502)의 잠재 거래 데이터에 의해 판매자 서브시스템(200)으로부터 클라이언트 디바이스(100')에 제공된 것일 수 있음). 예를 들어, 전술한 바와 같이, 일부 실시예들에서, 단계(502)에서 판매자 서브시스템(200)으로부터 클라이언트 디바이스(100')로 통신된 잠재 거래 요청 데이터는 판매자 서브시스템(200)을 나타낼 수 있는 판매자 식별자를 포함할 수 있다. 예를 들어, 판매자 식별자는 단계(502)에서 잠재 거래 데이터를 수신할 때 클라이언트 디바이스(100')에 의해 활용된 온라인 리소스(113')와 연관될 수 있다. 판매자 식별자는 상업적 엔티티 서브시스템(400)에 의해 액세스가능한 많은 판매자 키들 중 특정한 하나(예컨대, 상업적 엔티티 서브시스템(400)의 레버리지 테이블(430)을 통한 판매자 키(157'))를 식별하기 위해 단계(512)에서 상업적 엔티티 서브시스템(400)에 의해 수신 및 활용될 수 있으며, 이어서, 상업적 엔티티 서브시스템(400)은 호스트 거래 데이터의 적어도 일부분(예컨대, 적어도 호스트 거래 데이터의 호스트 결제 크리덴셜 데이터)을 암호화하기 위해 식별된 판매자 키를 사용할 수 있다. 그러한 호스트 결제 크리덴셜 데이터를 그러한 판매자 키(예컨대, 상업적 엔티티 서브시스템(400) 및 판매자 서브시스템(200)에만 공지될 수 있는 키)를 이용하여 암호화함으로써, 그러한 호스트 결제 크리덴셜 데이터는 다른 엔티티에 의해 인터셉트되지 않고 상업적 엔티티 서브시스템(400)으로부터 판

매자 서브시스템(200)으로 안전하게 통신될 수 있고 다른 판매자와의 거래를 지불하는데 사용될 수 있는 그러한 방식으로 보안될 수 있다.

[0062] 다음으로, 단계(514)에서, 프로세스(500)는 단계(512)의 보안 호스트 거래 데이터를 호스트 디바이스(100)에 통신하는 상업적 엔티티 서브시스템(400)을 포함할 수 있다. 예를 들어, 단계(514)에서, 그러한 판매자 키 암호화 호스트 결제 크리덴셜 데이터는 임의의 적합한 통신 프로토콜을 사용하여 통신 경로(65)를 통해 상업적 엔티티 서브시스템(400)으로부터 호스트 디바이스(100)로 보안 호스트 거래 데이터의 적어도 일부로서 송신될 수 있다. 그러한 보안 호스트 거래 데이터는 지불될 거래와 연관된 단계(502) 및/또는 단계(506)의 임의의 적합한 데이터와 같은 판매자 키-암호화된 호스트 결제 크리덴셜 데이터에 부가하여 임의의 적합한 데이터를 포함할 수 있으며, 이는 이에 제한되지는 않으나, 다음을 포함할 수 있다. (i) 특정 판매자 정보, 예컨대, 단계(502)의 잠재 거래 데이터를 제공한 특정 판매자 서브시스템(200)을 식별할 수 있는 판매자 식별자의 식별, (ii) 특정 거래 정보, 예컨대, 거래를 위해 결제하는 데 사용될 특정 화폐(예컨대, 엔, 파운드, 달러 등)의 식별, 및/또는 거래를 위해 결제될 특정 화폐 금액의 식별, 및/또는 구매 또는 임대 또는 그렇지 않으면 결제될 특정 제품 또는 서비스의 식별, 및/또는 사용될 디폴트 또는 초기 배송 주소의 식별, (iii) 고유 판매자-기반 거래 식별자(예컨대, 수행 중인 거래와의 연관을 위해 판매자 서브시스템(200)에 의해 생성된 바와 같음), (iv) 고유 클라이언트-기반 거래 식별자(예컨대, 수행되는 거래와의 연관을 위해 클라이언트 디바이스(100')에 의해 생성된 바와 같음), (v) 고유 클라이언트-기반 결제 요청 식별자(예컨대, 결제 요청과의 연관을 위해 클라이언트 디바이스(100')에 의해 생성된 바와 같음), 및/또는 (vi) 고유 호스트 기반 거래 식별자(예컨대, 호스트 디바이스 거래 데이터를 위해 호스트 디바이스(100)에 의해 생성된 바와 같음). 따라서, 단계(514)에서 상업적 엔티티 서브시스템(400)으로부터 호스트 디바이스(100)로 통신되는 보안 호스트 거래 데이터는 단계(502)의 잠재 거래 데이터의 일부 또는 전부 및/또는 단계(506)의 결제 요청 데이터의 일부 또는 전부뿐만 아니라 보안 호스트 결제 크리덴셜 데이터를 포함할 수 있다.

[0063] 다음으로, 프로세스(500)의 단계(516)에서, 호스트 디바이스(100)는 단계(514)에서 상업적 엔티티 서브시스템(400)으로부터 통신된 보안 호스트 거래 데이터를 수신할 수 있고, 임의의 적합한 방식으로 클라이언트 디바이스(100')와 보안 호스트 거래 데이터를 공유할 수 있다. 예를 들어, 보안 호스트 거래 데이터는 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100')에 공유된 공유 비밀 또는 키를 이용하여 일부 데이터를 암호화하거나 그렇지 않으면 재포맷하는 것을 포함할 수 있는 임의의 적합한 통신 프로토콜(예컨대, 보안 전송 프로토콜(예컨대, 애플 링크.의 아이메시지™) 또는 이메일 또는 임의의 다른 적합한 방법)을 사용하여 통신 경로(99)를 통해 호스트 디바이스(100)와 클라이언트 디바이스(100') 간에 공유될 수 있다. 일부 실시예들에서, 그러한 보안 호스트 거래 데이터는 NFC 컴포넌트(120)와 NFC 컴포넌트(120') 사이의 비접촉 근접 기반 통신을 통해 호스트 디바이스(100)와 클라이언트 디바이스(100') 사이에서 통신될 수 있다. 대안적으로, 도시되지는 않았지만, 그러한 보안 호스트 거래 데이터는 호스트 디바이스(100) 및 단계(514)를 통하는 대신, 임의의 적합한 방식으로(예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(95)를 통해) 상업적 엔티티 서브시스템(400)으로부터 클라이언트 디바이스(100')로 직접 통신될 수 있으며, 상업적 엔티티 서브시스템(400)은 목표 클라이언트 디바이스(100')를 식별하기 위해 단계(510)의 호스트 거래 데이터의 임의의 클라이언트 디바이스 식별자를 레버리지할 수 있다. 대안적으로, 도시되지는 않았지만, 그러한 보안 호스트 거래 데이터는 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100') 및 단계(514 및 516)를 통하는 대신에, 임의의 적합한 방식으로 상업적 엔티티 서브시스템(400)으로부터 판매자 서브시스템(200)으로 직접(예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(85)를 통해) 통신될 수 있으며, 상업적 엔티티 서브시스템(400)은 목표 판매자 서브시스템(200)을 식별하기 위해 단계(510)의 호스트 거래 데이터의 임의의 판매자 식별자를 레버리지할 수 있다. 대안적으로, 도시되지는 않았지만, 그러한 보안 호스트 거래 데이터는 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100') 및/또는 판매자 서브시스템(200) 및 단계들(514 내지 518)을 통하는 대신에, 임의의 적합한 방식으로(예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(55)를 통해) 상업적 엔티티 서브시스템(400)으로부터 금융 기관 서브시스템(350)으로 직접 통신될 수 있다. 단계(516)에서 클라이언트 디바이스(100')에 의해 수신될 수 있는 보안 호스트 거래 데이터는 지불될 거래와 연관된 임의의 적합한 데이터와 같은 판매자 키-암호화된 호스트 결제 크리덴셜 데이터에 부가하여 임의의 적합한 데이터를 포함할 수 있으며, 이에 제한되지는 않으나, 다음을 포함할 수 있다, (i) 특정 판매자 정보, 예컨대, 단계(502)의 잠재 거래 데이터를 제공한 특정 판매자 서브시스템(200)을 식별할 수 있는 판매자 식별자의 식별, (ii) 특정 거래 정보, 예컨대, 거래를 위해 결제하는 데 사용될 특정 화폐(예컨대, 엔, 파운드, 달러 등)의 식별, 및/또는 거래를 위해 결제될 특정 화폐 금액의 식별, 및/또는 구매 또는 임대 또는 그렇지 않으면 결제될 특정 제품 또는 서비스의 식별, 및/또는 사용될 디폴트 또는 초기 배송 주소의 식별, (iii) 고유 판매자-기반 거래 식별자(예컨대, 수행 중인 거래와의 연관을

위해 판매자 서브시스템(200)에 의해 생성된 바와 같음), (iv) 고유 클라이언트-기반 거래 식별자(예컨대, 수행되는 거래와의 연관을 위해 클라이언트 디바이스(100')에 의해 생성된 바와 같음), (v) 고유 클라이언트-기반 결제 요청 식별자(예컨대, 결제 요청과의 연관을 위해 클라이언트 디바이스(100')에 의해 생성된 바와 같음), 및/또는 (vi) 고유 호스트 기반 거래 식별자(예컨대, 호스트 디바이스 거래 데이터를 위해 호스트 디바이스(100)에 의해 생성된 바와 같음). 따라서, 클라이언트 디바이스(100')와 공유되는 보안 호스트 거래 데이터는 단계(502)의 잠재 거래 데이터의 일부 또는 전부 및/또는 단계(506)의 결제 요청 데이터의 일부 또는 전부뿐만 아니라 보안 호스트 결제 크리덴셜 데이터를 포함할 수 있다.

[0064]

다음으로, 프로세스(500)의 단계(518)에서, 클라이언트 디바이스(100')는 단계(516)에서 공유된 보안 호스트 거래 데이터를 사용하여 보안 호스트 거래 데이터의 판매자 키 암호화 호스트 결제 크리덴셜 데이터를 포함할 수 있는 판매자 서브시스템(200)에 클라이언트 거래 데이터를 전송함으로써 판매자 서브시스템(200)과의 거래를 지불할 수 있다. 예를 들어, 그러한 클라이언트 거래 데이터는 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(15)를 통하고/통하거나 NFC 컴포넌트(120')와 판매자 단말기(220) 사이의 비접촉식 근접-기반 통신으로서 클라이언트 디바이스(100')의 통신 컴포넌트(106')로부터 판매자 서브시스템(200)의 서버(210)로 송신될 수 있다. 클라이언트 디바이스(100')에 의해(예컨대, 판매자 리소스(113'))를 사용하여 판매자 서브시스템(200)에 통신될 수 있는 클라이언트 거래 데이터는 지불될 거래와 연관된 임의의 적합한 데이터와 같은, 보안 호스트 거래 데이터의 판매자 키-암호화된 호스트 결제 크리덴셜 데이터에 부가하여 임의의 적합한 데이터를 포함할 수 있으며, 이에 제한되지는 않으나, 다음을 포함할 수 있다. (i) 특정 판매자 정보, 예컨대, 단계(502)의 잠재 거래 데이터를 제공한 특정 판매자 서브시스템(200)을 식별할 수 있는 판매자 식별자의 식별, (ii) 특정 거래 정보, 예컨대, 거래를 위해 결제하는 데 사용될 특정 화폐(예컨대, 엔, 파운드, 달러 등)의 식별, 및/또는 거래를 위해 결제될 특정 화폐 금액의 식별, 및/또는 구매 또는 임대 또는 그렇지 않으면 결제될 특정 제품 또는 서비스의 식별, 및/또는 사용될 디폴트 또는 초기 배송 주소의 식별, (iii) 고유 판매자-기반 거래 식별자(예컨대, 수행 중인 거래와의 연관을 위해 판매자 서브시스템(200)에 의해 생성된 바와 같음), (iv) 고유 클라이언트-기반 거래 식별자(예컨대, 수행되는 거래와의 연관을 위해 클라이언트 디바이스(100')에 의해 생성된 바와 같음), (v) 고유 클라이언트-기반 결제 요청 식별자(예컨대, 결제 요청과의 연관을 위해 클라이언트 디바이스(100')에 의해 생성된 바와 같음), 및/또는 (vi) 고유 호스트 기반 거래 식별자(예컨대, 호스트 디바이스 거래 데이터를 위해 호스트 디바이스(100)에 의해 생성된 바와 같음). 따라서, 판매자 서브시스템(200)과 공유된 클라이언트 거래 데이터는 단계(502)의 잠재 거래 데이터의 일부 또는 전부 및/또는 단계(506)의 결제 요청 데이터 중 일부 또는 전부뿐만 아니라 단계(512)의 보안 호스트 거래 데이터의 적어도 판매자 키-암호화된 호스트 결제 크리덴셜 데이터를 포함할 수 있다. 클라이언트 거래 데이터의 적어도 일부로서 보안 호스트 거래 데이터의 판매자 키-암호화된 호스트 결제 크리덴셜 데이터를 통신함으로써, 프로세스(500)는 금융 거래를 지불하기 위해 판매자 서브시스템(200)이 호스트 디바이스(100) 및/또는 상업적 엔티티 서브시스템(400)과 통신할 필요 없이 판매자 서브시스템(200)에 그러한 판매자 키 암호화 호스트 결제 크리덴셜 데이터의 통신을 인에이블하면서도, 단계(508)에서 호스트 디바이스(100)에 의해 생성된 호스트 결제 크리덴셜 데이터가 판매자 키에 대한 액세스를 가지지 않는 판매자 엔티티에 대한 거래를 지불하기 위해 사용되는 것을 또한 방지할 수 있다(예컨대, 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100')). 대안적으로, 비록 도시되지는 않았지만, 적어도 단계(514)의 보안 호스트 거래 데이터의 판매자 키 암호화 호스트 결제 크리덴셜 데이터는 클라이언트 디바이스(100') 및 추가 단계(518)를 통하는 것이 아니라, 호스트 디바이스(100)가 목표 판매자 서브시스템(200)을 식별하기 위해 단계(506)의 결제 요청 데이터의 임의의 판매자 식별자를 레버리지할 수 있는 임의의 적합한 방식으로, 호스트 디바이스(100)로부터 판매자 서브시스템(200)에 직접 통신될 수 있다. 부가적으로 또는 대안적으로, 도시되지는 않았지만, 호스트 디바이스(100)는 단계(508)의 호스트 결제 크리덴셜 데이터를 상업적 엔티티 서브시스템(400) 대신에 호스트 디바이스(100) 상의 적절한 판매자 키를 이용하여 암호화하도록 동작할 수 있다(예컨대, 그러한 판매자 키가 호스트 디바이스(100)에 액세스가능해진 경우임). 대안적으로, 도시되지는 않았지만, 단계(512)의 보안 호스트 거래 데이터의 적어도 판매자 키-암호화된 호스트 결제 크리덴셜 데이터는, 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100') 및 그에 따라 추가적인 단계(516 및 518)를 통하는 대신에, 상업적 엔티티 서브시스템(400)이 목표 판매자 서브시스템(200)을 식별하기 위해 단계(510)의 호스트 거래 데이터의 임의의 판매자 식별자를 레버리지할 수 있는 임의의 적합한 방식으로 상업적 엔티티 서브시스템(400)으로부터 판매자 서브시스템(200)으로 직접(예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(85)를 통해) 통신될 수 있다. 대안적으로, 도시되지는 않았지만, 단계(512)의 보안 호스트 거래 데이터의 적어도 판매자 키-암호화된 호스트 결제 크리덴셜 데이터는, 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100') 및/또는 판매자 서브시스템(200) 및 단계(514 내지 518)를 통하는 대신에, (예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신

경로(55)를 통해) 임의의 적합한 방식으로 상업적 엔티티 서브시스템(400)으로부터 금융 기관 서브시스템(350)으로 직접 통신될 수 있다. 다른 실시예들에서, 단계(516)에서, 호스트 디바이스(100)는 클라이언트 디바이스(100')를 통하는 대신에 보안 호스트 거래 데이터를 판매자 서브시스템(200)에 직접 통신할 수 있다. 또 다른 실시예들에서, 단계(514)에서, 상업적 엔티티 서브시스템(400)은 호스트 디바이스(100)를 통하는 대신에 보안 호스트 거래 데이터를 클라이언트 디바이스(100')에 직접 통신할 수 있다. 또 다른 실시예들에서, 단계(514)에서, 상업적 엔티티 서브시스템(400)은 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100')를 통하는 대신에, 보안 호스트 거래 데이터를 판매자 서브시스템(200)에 직접 통신할 수 있다.

[0065]

단계(512)의 보안 호스트 거래 데이터의 판매자 키-암호화된 호스트 결제 크리덴셜 데이터가 판매자 서브시스템(200)에 의해 수신된 후, 프로세스(500)는 단계(520)에서, 판매자 서브시스템(200)이 금융 거래를 실행하기 위해 매입 은행(300) 및/또는 금융 기관 서브시스템(350)으로 판매자 키-암호화된 호스트 결제 크리덴셜 데이터를 활용하는 단계를 포함할 수 있다. 예를 들어, 판매자 서브시스템(200)은 판매자 서브시스템(200)에 액세스가능한 판매자 키(예컨대, 판매자 키(157) 및/또는 판매자 키(157'))를 이용하여 판매자 키-암호화된 호스트 결제 크리덴셜 데이터를 복호화하고, 이어서, 호스트 결제 크리덴셜 데이터를 매입 은행(300) 및/또는 금융 기관 서브시스템(350)에게 (예컨대, 통신 경로(25) 및/또는 통신 경로(35)를 통해) 포워드함으로써 해당 호스트 결제 크리덴셜 데이터와 연관된 지불 계좌가 식별되고 금융 거래의 지불을 위해 매입 은행(300) 및/또는 금융 기관 서브시스템(350)에 의해 사용될 수 있다. 다음으로, 그러한 거래가 단계(520)에서 실행된 후, 프로세스(500)는 단계(522)에서 임의의 적합한 확인 정보(예컨대, 임의의 적합한 결제 영수증 데이터 및/또는 임의의 적합한 불충분 지불 메시지 데이터)를 사용하여 클라이언트 디바이스(100')에 거래의 상태(예컨대, 거래의 실행 또는 거부)를 확인하는 판매자 서브시스템(200)을 포함할 수 있다. 이어서, 클라이언트 디바이스(100')는 단계(524)에서 (예컨대, 임의의 적합한 결제 영수증 데이터 및/또는 임의의 적합한 불충분 지불 메시지 데이터와 같은) 그러한 확인된 거래 상태를 호스트 디바이스(100)와 공유하도록 동작할 수 있다. 거래가 성공적이면, 확인 정보는 단계(522)에서 클라이언트 디바이스(100') 및/또는 단계(524)에서 호스트 디바이스(100)에서 거래(예컨대, 결제 요청 데이터의 고유 *RemotePayment Identifier*에 의해 식별된 거래)를 종료하도록 동작할 수 있다. 부가적으로 또는 대안적으로, 거래가 성공적이지 않은 경우, 확인 정보는 거래를 종료하도록 동작할 수 있거나 동작하지 않을 수 있다(예컨대, 유효한 지불금이 이용가능하지 않거나 호스트 디바이스가 허위로 확인되면 거래를 종료하지만, 유효하지 않은 배송 주소로 결정되면 오픈하고 업데이트를 허용함).

[0066]

도 5의 프로세스(500)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 부가적인 단계들이 부가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다. 예를 들어, 일부 실시예들에서, 프로세스(500)와 유사한 프로세스가 상업적 엔티티 서브시스템(400) 없이 이행될 수 있다. 대신에, 호스트 디바이스(100)는 (예컨대, 단계(508)에서, 호스트 디바이스(100)가 단계(512)의 동작을 수행할 수 있도록) 판매자 서브시스템(200)과 연관된 판매자 키에 액세스하고, 판매자 키-암호화된 호스트 결제 크리덴셜 데이터를 유도하도록 동작할 수 있고, 이어서, 거래가 호스트 결제 크리덴셜 데이터를 이용하여 안전하게 지불될 수 있도록 클라이언트 디바이스(100') 및/또는 판매자 서브시스템(200)에 그러한 판매자 키-암호화된 호스트 결제 크리덴셜 데이터를 통신한다. 프로세스(500)는 판매자 키 암호화된 호스트 결제 크리덴셜 데이터를 판매자 서브시스템(200)에 통신함으로써, 클라이언트 디바이스(100')와 판매자 서브시스템(200) 사이에서 개시된 금융 거래가 클라이언트 디바이스(100')에게 비-네이티브인 결제 크리덴셜에 의해서가 아니라, 호스트 디바이스(100)에게 네이티브인 결제 크리덴셜에 의해 적어도 부분적으로 지불되게 할 수 있다. 프로세스(500)는 판매자 서브시스템(200)이 금융 거래를 지불하기 위해 호스트 디바이스(100) 및/또는 상업적 엔티티 서브시스템(400)중 어느 하나의 통신하거나 심지어 그 존재를 인식할 필요없이 판매자 키 암호화된 호스트 결제 크리덴셜 데이터와 판매자 서브시스템(200) 사이의 통신을 가능하게 할 수 있으며, 또한, 단계(508)에서 호스트 디바이스(100)에 의해 생성된 호스트 결제 크리덴셜 데이터가 그러한 판매자 키에 대한 액세스를 갖지 않는 엔티티에 의해 사용되는 것을 방지할 수 있다. 일부 실시예들에서, 호스트 디바이스(100)는 높은 수준의 보안 또는 효율을 가능하게 할 수 있는 소정 데이터를 공유 및/또는 수신하기 위해(예컨대, 단계(510) 내지 단계(514)에서) 상업적 엔티티 서브시스템(400)과 끊임없이, 그리고 호스트 디바이스(100)의 사용자에게 투명하게 통신하도록 구성될 수 있다. 호스트 디바이스(100)의 사용자가 단계(508)에서 결제 요청 데이터에 기초하여 금융 거래를 수행하기 위한 특정 크리덴셜을 활용하는 것을 선택한 후에, 프로세스(500)의 나머지 단계들은 그 사용자에게 투명하게 발생할 수 있다(예컨대, 단계(510) 내지 단계(524)는 호스트 디바이스(100)와의 임의의 추가 사용자 상호작용없이 발생할 수 있고 호스트 디바이스(100)의 사용자에게 순간적으로 보일 수 있음). 호스트 디바이스(100)의 사용자에게 프로세스(500)는 단계(508) 후에 보안 호스트 결제 크리덴셜 데이터가 자동으로 그리고 순간적으로 판매자 서브시스템(200)에 전송되어 금융 거래의 상태가 확인되는 것처럼 보일 수 있다. 부

가적으로 또는 대안적으로, 클라이언트 디바이스(100')의 사용자는 단계(506)에서 결제 요청 데이터가 그것으로 통신되었을 수 있는 특정 결제 소스를 식별할 수 있으며 그런 후에 프로세스(500)의 나머지 단계는 그 사용자에게 투명하게 발생할 수 있다(예컨대, 단계(508) 내지 단계(524)는 클라이언트 디바이스(100')와의 임의의 추가 사용자 상호작용없이 발생할 수 있고 클라이언트 디바이스(100')의 사용자에게는 순간적으로 보일 수 있음). 클라이언트 디바이스(100')의 사용자에게 프로세스(500)는 단계(506) 후에(예컨대, 호스트 디바이스를 선택한 후에), 보안 호스트 결제 크리덴셜 데이터가 자동으로 그리고 순간적으로 판매자 서브시스템(200)에 전송되어 금융 거래의 상태가 확인되는 것처럼 보일 수 있다. 대안적으로, 일부 실시예들에서, 프로세스(500)는 전체적으로 클라이언트 디바이스(100')의 사용자에게 투명하게 발생할 수 있다(예컨대, 클라이언트 디바이스(100')는 금융 거래가 발생해야 할 때를 자동으로 결정하고, 클라이언트 디바이스(100')와의 임의의 활성 클라이언트 디바이스 사용자 상호작용없이 하나 이상의 이용가능한 결제 소스에게 그러한 금융 거래에 대한 결제 요청 데이터를 자동으로 전송하도록 구성될 수 있음).

[0067] 도 6의 설명

[0068] 도 6은 비-네이티브 결제 크리덴셜과 함께 전자 디바이스를 사용하여 금융 거래를 수행하기 위한 예시적인 프로세스(600)의 흐름도이다. 프로세스(600)는 호스트 전자 디바이스(100), 클라이언트 전자 디바이스(100'), 판매자 서브시스템(200), 매입 은행 서브시스템(300), 상업적 엔티티 서브시스템(400) 및 금융 기관 서브시스템(350)에 의해 구현되는 것으로 도시된다. 그러나, 프로세스(600)는 임의의 다른 적합한 컴포넌트들 또는 서브시스템들을 사용하여 구현될 수 있다는 것이 이해되어야 한다. 프로세스(600)는 호스트 디바이스(100)로부터의 결제 크리덴셜을 사용하면서 클라이언트 디바이스(100')를 통해 판매자 서브시스템(200)과의 안전하고 효율적으로 금융 거래를 수행하기 위한 끊임없는 사용자 경험을 제공할 수 있다. 도 6의 프로세스(600)에 따라 금융 거래를 수행하기 위한 시스템(1)의 동작에 관한 다음 논의를 용이하게 하기 위해, 도 1 내지 도 4의 개략도의 시스템(1)의 다양한 컴포넌트 및 도 3 내지 도 3h의 스크린(190 내지 190h)의 정면도가 참조되며, 이들은 거래 동안 호스트 디바이스(HD)(100)의 그래픽 사용자 인터페이스의 대표적 예시(예컨대, 카드 관리 애플리케이션(113b) 또는 호스트 디바이스(100)의 임의의 적합한 결제 애플리케이션에 의해 제공될 수 있는 GUI) 및/또는 클라이언트 디바이스(CD)(100')의 그래픽 사용자 인터페이스의 대표적 예시(예컨대, 클라이언트 디바이스(100')의 판매자 애플리케이션(113') 또는 클라이언트 디바이스(100')의 임의의 적합한 결제 애플리케이션에 의해 제공될 수 있는 GUI)일 수 있다. 기술된 동작들은 매우 다양한 그래픽 요소 및 시각적 기법으로 달성될 수 있다. 따라서, 도 3 내지 도 3h의 실시예들은 본 명세서에서 채택된 정확한 사용자 인터페이스 규약으로 제한되도록 의도되지 않는다. 오히려, 실시예들은 매우 다양한 사용자 인터페이스 양식을 포함할 수 있다.

[0069] 프로세스(600)는 상업적 엔티티 서브시스템(400)에 의한 호스트 디바이스(100)의 보안 요소 상에 호스트 액세스 데이터(652)(예컨대, 도 1b의 호스트 액세스 데이터(652))가 프로비저닝될 수 있는 단계(602)에서 시작될 수 있다. 예컨대, 액세스 SSD(예컨대, SSD(154b))는 호스트 디바이스(100)의 보안 요소(145) 상에 상업적 엔티티 서브시스템(400)의 서버(410)로부터의 액세스 데이터(652)로서 프로비저닝되어 호스트 디바이스(100)가 판매자 서브시스템(200)과의 금융 거래를 보다 안전하게 수행하게 할 수 있다. 언급된 바와 같이, 액세스 SSD(154b)는 상업적 엔티티 서브시스템(400)으로부터 직접 호스트 디바이스(100)의 보안 요소(145) 상에 적어도 부분적으로 프로비저닝될 수 있다(예컨대, 호스트 액세스 데이터(652)로서, 이는 상업적 엔티티 서브시스템(400)의 서버(410)와 호스트 디바이스(100)의 통신 컴포넌트(106) 사이의 통신 경로(65)를 통해 프로비저닝되고, 이어서 통신 컴포넌트(106)로부터 보안 요소(145)로(예컨대, 버스(118)를 통해) 전달될 수 있음). 경로(65)를 통한 호스트 액세스 데이터(652)는 액세스 SSD(154b)의 적어도 일부 또는 전부로서 호스트 디바이스(100)의 보안 요소(145) 상에 프로비저닝될 수 있고, 액세스 애플릿(153b) 및/또는 액세스 키(155b)를 포함할 수 있다. 단계(602)는 호스트 디바이스(100)가 초기에(예컨대, 호스트 디바이스(100)가 사용자에게 판매되기 전에 상업적 엔티티 서브시스템(400)에 의해) 구성될 때 적어도 부분적으로 이행될 수 있다. 대안적으로 또는 부가적으로, 단계(602)는 호스트 디바이스(100)의 사용자가 NFC 컴포넌트(120)의 보안 요소(145)를 초기 설정하는 것에 응답하여 적어도 부분적으로 이행될 수 있다. 부가적으로 또는 대안적으로, 호스트 액세스 데이터(652)는 보안 요소(145)의 ISD(152)에 대한 ISD 키(156k)를 포함할 수 있고, 상업적 엔티티 서브시스템(400)과 호스트 디바이스(100) 사이의 보안 송신을 인에이블하기 위해 액세스 키(155b)에 추가하거나 액세스 키로서 사용될 수 있다. 부가적으로 또는 대안적으로, 호스트 액세스 데이터(652)는 호스트 디바이스(100)의 보안 요소(145)의 CRS(151)의 CRS(151k) 및/또는 CASD(158)의 CASD(158k)를 포함할 수 있고, 상업적 엔티티 서브시스템(400)과 호스트 디바이스(100) 사이의 보안 송신을 인에이블하기 위해(예컨대, 상업적 엔티티 서브시스템(400)과 호스트 디바이스(100) 사이의 임의의 적합한 상업적 엔티티 키 또는 공유 비밀로서 사용하기 위해) 액세스 키(155b) 및/또는

액세스 키(155a) 및/또는 ISD 키(155k)에 부가되거나 대체되어 사용될 수 있다.

[0070]

단계(604)에서, 프로세스(600)는 일부 실시예들에서, 호스트 크리덴셜 데이터(654)(예컨대, 도 1b의 크리덴셜 데이터(654))를 상업적 엔티티 서브시스템(400)을 통해 금융 기관 서브시스템(350)에 의해 호스트 디바이스(100)의 보안 요소 상에 프로비저닝하는 단계를 포함할 수 있다. 예를 들어, 그러한 호스트 크리덴셜 데이터(654)는 금융 기관 서브시스템(350)으로부터 직접 호스트 디바이스(100)의 보안 요소(145) 상에 적어도 부분적으로 프로비저닝될 수 있다(예컨대, 금융 기관 서브시스템(350)과 디바이스(100) 사이의 도 1b의 통신 경로(75)를 통하여, 통신 컴포넌트(106)를 통해 보안 요소(145)로 전달될 수 있음). 부가적으로 또는 대안적으로, 그러한 호스트 크리덴셜 데이터(654)는 상업적 엔티티 서브시스템(400)을 통해 금융 기관 서브시스템(350)으로부터 호스트 디바이스(100)의 보안 요소(145) 상에 적어도 부분적으로 프로비저닝될 수 있다(예컨대, 금융 기관 서브시스템(350)과 상업적 엔티티 서브시스템(400) 사이의 도 1b의 통신 경로(55)를 통하여, 이는 상업적 엔티티 서브시스템(400)의 서버(410)와 호스트 디바이스(100)의 통신 컴포넌트(106) 사이의 도 1b의 통신 경로(65)를 통하여 호스트 크리덴셜 데이터(654)로서 호스트 디바이스(100)에 전달될 수 있고, 이어서, 통신 컴포넌트(106)로부터 보안 요소(145)로 (예컨대, 버스(118)를 통해) 전달될 수 있음). 경로(75) 및/또는 경로(65)를 통한 호스트 크리덴셜 데이터(654)는 크리덴셜 SSD(154a)의 적어도 일부 또는 전부로서 호스트 디바이스(100)의 보안 요소(145) 상에 프로비저닝될 수 있고, 크리덴셜 정보(161a) 및/또는 크리덴셜 키(155a') 및/또는 키(155ak)를 갖는 크리덴셜 애플릿(153a)을 포함할 수 있다. 단계(604)는 호스트 디바이스(100)의 사용자가 호스트 디바이스(100) 상에서 프로비저닝될 특정 크리덴셜을 선택할 때 적어도 부분적으로 이행될 수 있다. 일부 실시예들에서, 호스트 크리덴셜 데이터(654)는 상업적 엔티티 서브시스템(400)으로부터 금융 기관 서브시스템(350)으로 초기에 제공될 수 있고/있거나 상업적 엔티티 서브시스템(400)에 의해 부가될 수 있는 액세스 키(155a)를 또한 포함할 수 있다. 일부 실시예들에서, 그러한 호스트 크리덴셜 데이터(654)는 프로비저닝 중인 결제 크리덴셜의 크리덴셜 정보(예컨대, 애플릿(153a)의 크리덴셜 정보(161a))의 적어도 일부로서의 주 계좌 번호, AID(예컨대, SSD(154a)에서 프로비저닝되는 결제 크리덴셜의 데이터의 애플릿(153a)에 대한 AID(155aa)), SSD 식별자 및/또는 SSD 카운터를 포함할 수 있다.

[0071]

호스트 디바이스(100) 상에 프로비저닝된 크리덴셜 데이터는 그 크리덴셜을 이용하여 결제하는 데 필요한 모든 데이터, 예컨대, 예를 들어, 주 계좌 번호("PAN"), 카드 보안 코드(예컨대, 카드 검증 코드("CVV")), PAN 만료 일자, 크리덴셜과 연관된 이름 등 뿐만 아니라, 호스트 디바이스(100)에 대해 동작하여 적합한 암호화 데이터(예컨대, 임의의 적합한 공유 비밀 및 기능 출력이 공유 비밀에 의해 적어도 부분적으로 결정될 수 있는 임의의 적합한 암호 알고리즘 또는 암호)를 생성할 수 있는 다른 데이터를 포함할 수 있다. 사용자의 "실제" 크리덴셜 또는 실제 PAN 또는 지불 PAN("F-PAN")이 아니라, "가상" 크리덴셜 또는 가상 PAN 또는 디바이스 PAN("D-PAN")이 호스트 디바이스(100) 상에 프로비저닝될 수 있다. 예를 들어, 크리덴셜이 호스트 디바이스(100) 상에 프로비저닝될 것으로 결정되면, 실제 크리덴셜 대신에 가상 크리덴셜이 생성되고, 실제 크리덴셜에 링크되어, 호스트 디바이스(100) 상에 프로비저닝되도록, (예컨대, 금융 기관 서브시스템(350)에 의해, 상업적 엔티티 서브시스템(400)에 의해, 및/또는 호스트 디바이스(100)의 사용자에게 의해) 요청될 수 있다. 가상 크리덴셜과 실제 크리덴셜의 생성 및 링크하기는 금융 기관 서브시스템(350)의 임의의 적합한 컴포넌트에 의해 수행될 수 있다. 예를 들어, 결제 네트워크 서브시스템(360)(예컨대, 실제 크리덴셜의 브랜드와 연관될 수 있는 특정 결제 네트워크 서브시스템(360))은 실제 크리덴셜 및 가상 크리덴셜 사이의 연관을 생성할 수 있는 가상-링크 테이블(312)(예컨대, 도 1b에 도시된 바와 같은)을 정의 및 저장할 수 있으며, 가상 크리덴셜이 판매자 서브시스템(200)과의 금융 거래를 위해 호스트 디바이스(100)에 의해 활용될 때마다(예컨대, 호스트 디바이스(100) 상에 프로비저닝된 후에) 결제 네트워크 서브시스템(360)은 (예컨대, 단계(642)에서, 단계(640)에서 데이터(690)를 수신하는 것에 응답하여) 인증 또는 검증 요청을 수신하거나 그렇지 않으면 그 가상 크리덴셜을 나타내는 임의의 수신된 데이터를 검증하려고 시도하고, 테이블(312)에 의해 결정된 가상 크리덴셜과 연관된 실제 크리덴셜에 비추어 그 검증 시도 요청의 분석을 수행 할 수 있다. 대안적으로, 그러한 테이블은 적절한 발행 은행 서브시스템(370) 또는 금융 기관 서브시스템(350)에 의해 접근가능한 임의의 다른 적합한 서브시스템에 의해 액세스가 가능하고/하거나 유사하게 레버리지될 수 있다. 실제 크리덴셜 대신에 호스트 디바이스(100) 상에 가상 크리덴셜을 프로비저닝함으로써, 특정 거래 동안 결제 네트워크 서브시스템(360)이 가상 크리덴셜을 실제 크리덴셜에 링크하기 위해서만 테이블 (312)을 활용하도록 구성될 수 있기 때문에, 금융 기관 서브시스템(350)은 가상 크리덴셜이 인가되지 않은 사용자에게 의해 인터셉트될 때 발생할 수 있는 사기 활동을 제한하도록 구성될 수 있다.

[0072]

단계(606)에서, 프로세스(600)는 판매자 애플리케이션(113) 또는 판매자 웹사이트와 같은 판매자의 온라인 리소스를 판매자 키(157)와 연관시키는 단계를 포함할 수 있다. 예를 들어, 상업적 엔티티 서브시스템(400)은 판매자 키를 판매자의 리소스와 연관시키도록 테이블(430)을 채울 수 있으며(예컨대, 판매자 키(157)와 호스트 디바

이스(100)의 리소스(113) 및/또는 판매자 키(157')와 클라이언트 디바이스(100')의 리소스(113'))), 따라서 판매자 리소스를 사용하여 (예컨대, 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100'))를 통해 상업적 엔티티 서브시스템(400)과 판매자 서브시스템(200) 사이의 안전한 상거래 크리덴셜 데이터 통신을 인에이블할 수 있다. 판매자 서브시스템(200) 및 상업적 엔티티 서브시스템(400) 둘 모두 그러한 판매자 키의 버전을 (예컨대, 도 1b에 도시된 바와 같이, 판매자 서브시스템(200) 및 상업적 엔티티 서브시스템(400)의 각각의 보안 요소에) 저장할 수 있다. 일부 실시예들에서, 온라인 리소스 결제 프로그램에 참여하기 위해, 판매자는 상업적 엔티티 서브시스템(400)의 상업적 엔티티에 의해 운영되는 프로그램의 회원으로 등록되고/되거나 판매자 인증서를 획득할 필요가 있을 수 있다. 판매자들은 인증서 없이 결제 데이터를 수신할 수 없을 수 있다. 각각의 인증서는 판매자를 해당 판매자의 공개 키(예컨대, 공개 판매자 키(157/157'))에 결합할 수 있는 고유한 상업적 엔티티 판매자 식별자를 포함할 수 있다. 판매자는 다수의 인증서를 얻을 수 있으므로, 하나 초과를 아이덴티티를 보유할 수 있다. 그러한 고유한 상업적 엔티티 판매자 식별자는 판매자 서브시스템(200)에 의해 클라이언트 디바이스(100')에 (예컨대, 단계(610)에서 잠재 거래 데이터(660)의 일부로서 그리고/또는 클라이언트 디바이스(100') 상에 실행 중인 판매자 온라인 리소스(예컨대, 판매자 애플리케이션(113'))의 고유 요소로서) 제공될 수 있으며, 그러한 상업적 엔티티 판매자 식별자는 시도된 거래 동안 (예컨대, 결제 요청 데이터(666) 및/또는 결제 요청 데이터(674)를 통해 단계(628)의 호스트 거래 데이터(678)의 적어도 일부로서) 호스트 디바이스(100)를 통해 클라이언트 디바이스(100')로부터 상업적 엔티티 서브시스템(400)으로 제공될 수 있다. 일부 실시예들에서, 상업적 엔티티 서브시스템(400)은 판매자 온라인 리소스에 대한 판매자 키(예컨대, 애플리케이션(113)에 대한 키(157) 및/또는 애플리케이션(113')에 대한 키(157'))를 생성하거나 그렇지 않으면 할당할 수 있고 그러한 판매자 키를 (예컨대, 경로(85)를 통해) 판매자 서브시스템(200)에 제공할 수 있다. 대안적으로, 판매자 서브시스템(200)은 판매자 온라인 리소스에 대한 판매자 키를 생성 또는 그렇지 않으면 할당하고 그러한 판매자 키를 (예컨대, 경로(85)를 통해) 상업적 엔티티 서브시스템(400)에 제공할 수 있다. 판매자 서브시스템(200) 또는 상업적 엔티티 서브시스템(400) 중 어느 하나는 그러한 키의 생성, 교환, 저장, 사용 및 교체를 포함할 수 있는 임의의 판매자 키의 관리를 담당할 수 있다. 그러한 판매자 키가 생성되고/되거나 관리될 수 있는 방식 또는 위치에 관계없이, 판매자 서브시스템(200) 및 상업적 엔티티 서브시스템(400) 둘 모두는 판매자 키의 버전을(예컨대, 판매자 서브시스템(200) 및 상업적 엔티티 서브시스템(400)의 각각의 보안 요소에) 저장할 수 있다. 이것은 상업적 엔티티 서브시스템(400)과 판매자 서브시스템(200) 사이에서 데이터를 안전하게 통신하기 위해 이들 사이의 공유 비밀을 가능하게 할 수 있다. 일부 실시예들에서, 호스트 디바이스(100)는 그러한 판매자 키가 제공됨으로써 그 키를 이용하여 결제 데이터를 호스트 디바이스(100) 상에 안전하게 암호화할 수 있다.

[0073] 단계(608)에서, 프로세스(600)는 클라이언트 디바이스(100')에 의해 액세스되는 판매자의 리소스(658)(예컨대, 도 1b의 판매자의 제3자 리소스(113'))를 포함할 수 있다. 도 1b에 도시된 바와 같이, 판매자의 리소스 애플리케이션(113')은 상업적 엔티티 서브시스템(400)으로부터(예컨대, 애플리케이션 스토어(420)로부터) 클라이언트 디바이스(100') 상에 로딩될 수 있다. 그러나 예를 들어, 도 3에 도시된 바와 같이, 호스트 디바이스(100)에 관하여, 클라이언트 디바이스(100')의 사용자는 I/O 컴포넌트(114a)의 터치 스크린 입력 컴포넌트(110f)를 사용하여 GUI(180)의 특정 스크린(190)의 "판매자 앱" 아이콘(183)을 선택할 수 있으며, 이러한 선택은 판매자의 제3자 애플리케이션(113')과 상호작용하는 능력을 사용자에게 제공하기 위한 개시 이벤트로서 클라이언트 디바이스(100')에 의해 인식될 수 있다. 대안적으로 또는 부가적으로, 그러한 판매자의 리소스(658)는 판매자 서브시스템(200)으로부터 직접 클라이언트 디바이스(100')에 의해 액세스될 수 있다. 판매자 애플리케이션 아이콘의 그러한 선택에 응답하여, GUI는 클라이언트 디바이스(100')가 사용자가 구매를 위해 판매자로부터의 상업적으로 이용가능한 아이템들을 열람하기 위해 애플리케이션(113')과 상호작용할 수 있게 하는 대화형 스크린을 제공할 수 있다. 대안적으로, 단계(608)는 클라이언트 디바이스(100')가 (예컨대, 판매자 서버(210)를 통해) 판매자 서브시스템(200)으로부터의 판매자의 웹페이지인 판매자의 리소스(658)에 클라이언트 디바이스(100')의 인터넷 애플리케이션을 사용하여 액세스하는 단계를 포함할 수 있으며, 이는 또한 사용자에게 판매자의 제3자 애플리케이션이 아닌 판매자의 웹페이지와 상호작용할 수 있는 능력을 제공하기 위한 "인터넷" 아이콘(예컨대, 도 3의 GUI(180)의 특정 스크린(190)의 아이콘(182))에 의해 선택가능할 수 있다. 대안적으로, 단계(608)는 활성 사용자 입력 없이 리소스(658)가 임의의 적합한 자동 액세스를 하는 단계를 포함할 수 있다(예컨대, 클라이언트 디바이스(100')는, 자율 가전기기 클라이언트 디바이스(100')가 특정 공급이 부족한 것을 검출하는 것과 같은 임의의 적합한 이벤트를 검출하는 것에 응답하여(예컨대, 세탁기 클라이언트 디바이스(100')가 세탁 세제의 낮은 공급을 감지하는 것에 응답하여) 리소스(658)와 자동으로 상호작용하도록 동작할 수 있음).

[0074] 다음으로, 단계(610)에서, 클라이언트 디바이스(100')는 (예컨대, 프로세스(500)의 단계(502)와 관련하여 설명된 바와 같이) 액세스된 판매자 리소스로부터 잠재 거래 데이터(660)를 수신할 수 있다. 예를 들어, 도 1b에

도시된 바와 같이, 잠재 거래 데이터(660)는, 클라이언트 디바이스(100')가 판매자의 리소스(113')(예컨대, 제3자 애플리케이션 또는 웹사이트 또는 판매자 임의의 다른 적합한 온라인 리소스(예컨대, 리소스(658))와 상호작용할 때 판매자 서브시스템(200)으로부터(예컨대, 판매자 서버(210)로부터) 클라이언트 디바이스(100')에 제공될 수 있다. 대안적으로 또는 부가적으로, 잠재 거래 데이터(660)의 적어도 일부분은, 단계(610)에서 데이터가 판매자 서버(210)로부터 클라이언트 디바이스(100')로 능동적으로 전송되는 것이 아니라, 클라이언트 디바이스(100')에 로컬인 애플리케이션(113')을 통해 클라이언트 디바이스(100')에 의해 국부적으로 액세스가능할 수 있다(예컨대, 애플리케이션(113')은 메모리 컴포넌트에 저장되거나 클라이언트 디바이스(100')의 프로세서(102')에 의해 실행될 수 있음). 예를 들어, 애플리케이션(113')이 (예컨대, 단계(608)에서 판매자 리소스(658)로서) 클라이언트 디바이스(100') 상에 초기에 저장될 수 있는 경우, 잠재 거래 데이터(660)의 적어도 일부는, 판매자 서브시스템(200)에 의해 클라이언트 디바이스(100')에 제공된 임의의 추가 정보 없이, 초기에 저장된 애플리케이션(113')에 의해 생성될 수 있다. 잠재 거래 데이터(660)는 클라이언트 디바이스(100')의 사용자와 판매자 서브시스템(200)의 판매자 사이에서 발생할 잠재적 금융 거래의 임의의 적합한 특성을 나타내는 임의의 적합한 데이터를 포함할 수 있으며, 이에 제한되지는 않으나, 다음을 포함할 수 있다, (i) 특정 판매자 정보, 예컨대, 고유 판매자 식별자(예컨대, 매입 은행 판매자 식별자 및/또는 상업적 엔티티 판매자 식별자) 및/또는 사용 중인 특정 판매자 리소스(예컨대, 특정 판매자 애플리케이션(113'))의 식별, (ii) 특정 거래 정보, 예컨대, 거래를 위해 결제하는 데 사용될 특정 화폐(예컨대, 엔, 파운드, 달러 등)의 식별, 및/또는 거래를 위해 결제될 특정 화폐 금액의 식별, 및/또는 구매 또는 임대 또는 그렇지 않으면 결제될 특정 제품 또는 서비스의 식별, 및/또는 사용될 디폴트 또는 초기 배송 주소의 식별, (iii) 거래를 위해 판매자에게 수령가능한 하나 이상의 유형의 결제 방법을 나타내는 정보(예컨대, 구매에 사용될 수 있는 결제 카드들(예컨대, 비자를 제외한 마스터카드)의 리스트), 및/또는 (iv) 고유 판매자-기반 거래 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행 중인 거래와의 연관을 위해 판매자 서브시스템(200)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열). 그러한 잠재 거래 데이터(660)는, 적어도 금융 거래를 완료하는 데 요구되거나 적어도 사용될 수 있는, 연관 데이터를 갖거나 갖지 않는 임의의 적합한 수 및 유형의 데이터 필드를 포함할 수 있으며, 예컨대, 구매 중인 고객의 연락처 정보 필드들(예컨대, 전화 번호, 이메일 주소, 우편 주소)로서, 일부 필드들은 기입되어 그러한 잠재 거래 데이터(660)의 일부로서 포함될 수 있고/있거나 일부 필드들은 그러한 잠재 거래 데이터(660)의 일부로서 기입되지 않은 채 프로세스(600) 동안 오픈되어 지정되기를 대기할 수도 있다. 단계(610)의 그러한 잠재 거래 데이터(660)는 본 명세서에서 *PKPaymentRequest*로 지칭될 수 있다. 대안적으로, 언급된 바와 같이, 사용자는 단계(610)에서 판매자 서브시스템(200)과 연관된 잠재 거래 데이터(660)가 클라이언트 디바이스(100')에 이용가능해지도록 클라이언트 디바이스(100')와 능동적으로 상호작용하지 않을 수 있다.

[0075]

잠재 거래 데이터(660)는 상품 및/또는 서비스의 구매를 위한 결제 토큰을 생성하기 위한 클라이언트 디바이스(100')에 대한 판매자 리소스의 요청을 정의할 수 있고, 예를 들어, 판매자의 결제 프로세싱 능력, 결제할 금액, 및 화폐 코드에 관한 정보를 포함하는 잠재 거래에 관한 임의의 적합한 정보를 캡슐화할 수 있다. 잠재 거래 데이터(660)는 또한 판매자에 의해 지원될 수 있는 하나 이상의 결제 네트워크의 리스트를 포함할 수 있으며, 따라서 클라이언트 디바이스(100')는 그러한 리스트에 오른 하나 이상의 결제 네트워크(예컨대, 결제 네트워크(들)(360)) 중 임의의 결제 네트워크가 인가된 결제 크리덴셜을 클라이언트 디바이스(100') 상에 또는 클라이언트 디바이스(100')에 이용가능한 임의의 적합한 호스트 디바이스 상에 갖는지 여부를 결정하도록 구성될 수 있다. 일부 실시예들에서, 그러한 잠재 거래 데이터(660)가 클라이언트 디바이스(100')에 의해 액세스될 수 있으면, 도 3a에 도시된 바와 같이, 예를 들어, 클라이언트 디바이스(100')의 GUI는 스크린(190a)을 제공할 수 있으며, 판매자의 리소스는 거래 데이터(660)를 사용하여 잠재 거래와 연관된 임의의 적합한 정보, 예컨대, 정보(307a)를 갖는 판매자의 이름(예컨대, "판매자 A"), 정보(307b)를 갖는 제품의 이름(예컨대, "제품 B"), 정보(307c)를 갖는 가격(예컨대, "가격 C") 및/또는 정보(307d)를 갖는 초기 배송 데이터(예컨대, "주소 D")를 클라이언트 디바이스(100')의 사용자에게 보여줄 수 있다. 판매자 서브시스템(200)에 의해 클라이언트 디바이스(100')에 제공될 수 있는 잠재 거래 데이터(660)는 그러한 정보(307a, 307b, 307c 및/또는 307d)를 나타낼 수 있다. 클라이언트 디바이스(100')의 사용자는 디바이스(100') 및 스크린(190a)과 상호작용하여, 그러한 정보의 특정 부분들(예컨대, 배송 주소, 등)을 조정할 수 있으며, 이는 (예컨대, 단계(622)에서) 업데이트된 잠재 거래 데이터가 생성되어 판매자 서브시스템(200)에 의해 공유되도록 요구할 수 있다. 도 3a에 또한 도시되고 보다 상세히 후술되는 바와 같이, 스크린(190a)은 또한 보안 결제 프롬프트(*secure pay prompt*)(309)를 포함할 수 있다. 잠재 거래 데이터(660)의 적어도 일부분은 도 1b의 통신 경로(15)를 통해 판매자 서브시스템(200)으로부터 클라이언트 디바이스(100')로 제공될 수 있고, 클라이언트 디바이스(100')의 통신 컴포넌트(106')에 의해 수신될 수 있다. 통신 컴포넌트(106')는 이러한 잠재 거래 데이터(660)를 (예컨대, (예컨대, 정보(307a 내지 307

d)에 대해) 클라이언트 디바이스(100') 상의 사용자 인터페이스의 일부로서 스크린(190a) 상에 디스플레이하기 위해) 프로세서(102') 및/또는 NFC 컴포넌트(120')에 전달할 수 있다. 예를 들어, NFC 컴포넌트(120')는 클라이언트 디바이스(100')와 판매자 서브시스템(200) 사이의 금융 거래를 안전하게 인에이블하기 위해 그러한 잠재 거래 데이터(660)를 활용할 수 있다. 일부 실시예들에서, 잠재 거래 데이터(660)는 판매자 결제 요청 데이터 및/또는 "URL"(uniform resource locator) 또는 임의의 다른 적합한 기준 문자열 및/또는 쿼리 문자열로 지칭될 수 있다.

[0076]

다음으로, 프로세스(600)의 단계(612)에서, 클라이언트 디바이스(100')는 임의의 적합한 원격 소스에 임의의 적합한 호스트 이용가능성 요청 데이터(662)(예컨대, 디스커버리 요청)를 전송함으로써, 금융 거래, 예컨대, 단계(610)의 잠재 거래 데이터(660)와 연관된 거래를 잠재적으로 지불하기 위한 (예컨대, 적어도 하나의 호스트 디바이스의) 적어도 하나의 비-네이티브 결제 소스를 식별하려고 시도할 수 있고, 이어서, 프로세스(600)의 단계(614)에서, 임의의 송신된 호스트 이용가능성 요청 데이터(662)에 응답하여, 클라이언트 디바이스(100')는 (예컨대, 프로세스(500)의 단계(504)에 관해 설명된 바와 같이) 임의의 적합한 소스로부터 임의의 적합한 호스트 이용가능성 응답 데이터(664)(예컨대, 임의의 적합한 디스커버리 응답)를 수신할 수 있다. 임의의 이용가능한 비-네이티브 결제 소스를 식별하기 위해 임의의 적합한 기술을 사용할 수 있다. 예를 들어, 비콘 신호는 클라이언트 디바이스(100')에 의해 호스트 이용가능성 요청 데이터(662)로서 송신될 수 있고 이는 비콘을 수신할 수 있는 임의의 호스트 디바이스로부터 응답을 요청할 수 있다(예컨대, 클라이언트 디바이스(100')와 특정 거리 내에서 비콘의 특정 통신 프로토콜을 사용하여 통신하도록 동작할 수 있는 임의의 호스트 디바이스, 또는 비콘은 빠른 응답("QR") 코드 또는 클라이언트 디바이스(100')에 의해 제시되고 하나 이상의 호스트 디바이스의 스캐너에 의해 판독되는 임의의 다른 적합한 코드일 수 있음). 대안적으로 또는 부가적으로, 클라이언트 디바이스(100')는 임의의 적합한 통신 경로 및 프로토콜을 사용하여 하나 이상의 특정 호스트 디바이스(예컨대, 디바이스(100')의 연락처 애플리케이션에서 식별되고/되거나 디바이스(100')의 사용자에게 의해(예컨대, 전화 번호 또는 이메일 주소 또는 임의의 적합한 고유 디바이스 식별자(예컨대, 호스트 디바이스(100)의 디바이스 식별자(119)에 의해) 수동으로 식별된 하나 이상의 디바이스)에 호스트 이용가능성 요청 데이터(662)를 전송할 수 있다.

[0077]

그러한 호스트 이용가능성 요청 데이터(662)는 임의의 적합한 정보, 예컨대, 클라이언트 디바이스(100')를 식별하는 정보(예컨대, 클라이언트 디바이스(100')의 디바이스 식별자(119')) 및/또는 잠재적 금융 거래를 지불하기 위해 (예컨대, 판매자에 의해) 수령가능한 수 있는 하나 이상의 특정 결제 유형(예컨대, 단계(610)의 잠재 거래 데이터(660)에 의해 식별될 수 있는 결제 유형(들))을 식별하는 정보를 포함할 수 있고, 응답으로, 임의의 적합한 호스트 이용가능성 응답 데이터(664), 예컨대, 응답하는 호스트 디바이스를 식별할 수 있는 임의의 적합한 정보(예컨대, 호스트 디바이스(100)의 디바이스 식별자(119)) 및/또는 그 호스트 디바이스에 이용가능할 수 있는 하나 이상의 특정 결제 유형을 식별하는 임의의 적합한 정보(예컨대, 호스트 디바이스(100)의 AID(155aa) 및/또는 AID(155ba), 여기서 호스트 이용가능성 응답 데이터(664)의 그러한 결제 유형 식별은 호스트 이용가능성 요청 데이터(662)의 디스커버리 요청의 유형과 일치하는 각각의 유형을 단지 포함하거나 응답하는 호스트에 이용가능한 모든 결제 유형을 포함할 수 있음) 및/또는 응답하는 호스트 디바이스의 위치를 식별하는 임의의 적합한 정보 및/또는 호스트 디바이스의 상태(예컨대, 어웨이크 상태, 슬립 상태, 전원 오프 상태, 등)를 식별하는 임의의 적합한 정보를 요청할 수 있다. 호스트 디바이스에 의해 공유되는 호스트 이용가능성 응답 데이터(664)는 예컨대, 프로토콜 버퍼를 사용하는 것에 의해, 호스트 디스커버리에 요구되는 최소량의(bare minimum amount) 데이터일 수 있다. 단계(612) 및/또는 단계(614)에서, 상업적 엔티티 서브시스템(400) 또는 임의의 다른 엔티티는 클라이언트 디바이스(100')에 의한 호스트 디바이스(100)의 식별에 참여할 수 있다. 예를 들어, 전술한 바와 같이, 상업적 엔티티 서브시스템(400)은 아이클라우드™ 및/또는 아이메시지™ 또는 임의의 다른 적합한 아이덴티티 서비스 전송과 같은 클라이언트 디바이스(100') 및/또는 호스트 디바이스(100)에 이용가능하게 된 임의의 적합한 서비스를 관리하도록 동작할 수 있으며, 상이한 디바이스들 사이의 연관을 짓고/짓거나 다양한 디바이스들의 상태 및/또는 성능을 자동으로 결정하도록 동작할 수 있다(예컨대, 일가족이 클라이언트 디바이스(100') 뿐만 아니라, 호스트 디바이스(100)를 포함하는 다수의 다른 디바이스와 연관될 수 있는 상업적 엔티티 서브시스템(400)의 계좌를 가질 수 있음). 하나의 예로서, 일례로서, 클라이언트 디바이스(100')는 클라이언트 디바이스(100')의 계정과 연관된 모든 다른 디바이스의 상태를 요청하기 위해 상업적 엔티티 서브시스템(400)에 호스트 이용가능성 요청 데이터(662)를 전송할 수 있고, 상업적 엔티티 서브시스템(400)은 그러한 디바이스들 중 하나, 일부 또는 각각의 상태를 획득하고 이들 상태의 각각을 호스트 이용가능성 응답 데이터(664)로서 클라이언트 디바이스(100')와 공유함으로써 응답할 수 있으며, 여기서 상태는 호스트 디바이스(100)의 이용가능성 및 호스트 디바이스(100)에 이용가능한 적어도 하나의 결제 유형의 아이덴티티를 나타낼 수 있다. 각각의 호스트 디바이스는 그러한 요청들 및 잠재 응답들에 대하여 그의 자체 설정을 가질 수 있다(예컨대, 특

정 호스트 디바이스는 다만 특정 클라이언트 디바이스들(예컨대, 다만 상업적 엔티티 서브시스템(400)의 동일한 계정과 연관된 디바이스들, 다만 그 특정 호스트 디바이스의 연락처 애플리케이션 내의 연락처와 연관된 디바이스들, 등)로부터 수신된 호스트 이용가능성 요청 데이터(662)에만 응답하도록 구성될 수 있음). 단계(612) 및 단계(614)에서 하나 이상의 이용가능한 결제 소스의 식별을 인에이블하기 위한 그러한 요청들 및/또는 응답들은 임의의 적합한 방식으로 통신될 수 있으며, 예컨대, 클라이언트 디바이스(100')와 호스트 디바이스(100) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(99)를 통해) 직접, 또는 클라이언트 디바이스(100')와 상업적 엔티티 서브시스템(400) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(95)를 통해), 및 상업적 엔티티 서브시스템(400)과 호스트 디바이스(100) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하는 통신 경로(65)를 통해) 통신될 수 있다. 예를 들어, 도 1b에 도시된 바와 같이, 호스트 이용가능성 요청 데이터(662)는 클라이언트 디바이스(100')로부터 호스트 디바이스(100)로 (예컨대, 임의의 적합한 통신 프로토콜을 사용하여 통신 경로(99)를 통하거나 상업적 엔티티 서브시스템(400)을 통해(예컨대, 임의의 적합한 통신 프로토콜(들)을 사용하여 통신 경로(95) 및 통신 경로(65)를 통해) 또는 상업적 엔티티 서브시스템(400)으로 (예컨대, 임의의 적합한 통신 프로토콜을 사용하여 통신 경로(95)를 통해) 통신될 수 있고, 호스트 이용가능성 응답 데이터(664)는 호스트 디바이스(100)로부터 클라이언트 디바이스(100')로 (예컨대, 임의의 적합한 통신 프로토콜(들)을 사용하여 통신 경로(99)를 통해) 또는 상업적 엔티티 서브시스템(400)을 통해 (예컨대, 임의의 적합한 통신 프로토콜(들)을 이용하여 통신 경로(65) 및 통신 경로(95)를 통해) 또는 상업적 엔티티 서브시스템(400)으로부터 (예컨대, 임의의 적합한 통신 프로토콜을 사용하여 통신 경로(95)를 통해) 통신될 수 있다.

[0078] 호스트 이용가능성 요청 데이터(612)는 잠재 거래 데이터(660)를 수신하는 것에 응답하여, 또는 그러한 거래 데이터(660)의 수신과는 독립적으로 주기에 따라, 또는 임의의 적합한 시간에 클라이언트 디바이스(100')의 사용자에게 의해 주어진 요청에 응답하여, 예컨대, 도 3a의 스크린(190a)의 GUI와 상호작용하는 클라이언트 디바이스(100')의 사용자에게 응답하여, 클라이언트 디바이스(100')에 의해 자동으로 전송될 수 있다. 예를 들어, 잠재 거래 데이터(660)의 상세사항에 따라 판매자로부터 구매를 하기 위해 클라이언트 디바이스(100')의 스크린(190a)의 보안 결제 프롬프트(309)를 사용자가 선택하는 것에 응답하여, 클라이언트 디바이스(100')는 호스트 이용가능성 요청 데이터(662)를 생성하고 송신할 수 있다. 또한, 도 3b에 도시된 바와 같이, 클라이언트 디바이스(100')는 도 3a의 스크린(190a)의 보안 결제 프롬프트(309)의 선택을 수신하는 것에 응답하고, 임의의 적합한 호스트 이용가능성 응답 데이터(664)를 수신하는 것에 응답하여, 스크린(190b)을 제공하도록 구성될 수 있으며, 이는 사용자에게 구매를 하기 위해 클라이언트 디바이스(100')에 이용가능할 수 있는 특정 결제 소스 또는 크리덴셜을 선택하기 위해 하나 이상의 방식으로 클라이언트 디바이스(100')와 상호작용하라고 촉구할 수 있다. 예를 들어, 도시된 바와 같이, 스크린(190b)은 사용자가 클라이언트 디바이스(100')에 이용가능할 수 있는 잠재적으로 다수의 결제 소스들 중 하나를 선택할 수 있게 하는 결제 소스 선택 프롬프트(311)를 포함할 수 있다. 결제 소스 선택 프롬프트(311)는 판매자에 의해 지원되는 결제 네트워크와 연관된 크리덴셜들을 갖는 결제 소스만을 포함할 수 있거나(이는 예컨대, 전술한 바와 같이, 잠재 거래 데이터(660)에 의해 결정될 수 있음), 클라이언트 디바이스(100')에 이용가능한 모든 결제 소스(예컨대, 호스트 이용가능성 응답 데이터(664)로서 수신된 모든 AID(들)와 연관된 모든 소스들)를 보여주되, 다만 수령가능한 결제 네트워크들과 연관된 것들만 사용자에게 의해 선택가능하게 할 수 있다. 결제 소스 선택 프롬프트(311)는, 이에 제한되는 것은 아니나 다음을 포함하는 임의의 적합한 결제 소스들을 포함할 수 있다: 클라이언트 디바이스(100')(도시되지 않음)의 보안 요소에 네이티브한 임의의 적합한 결제 크리덴셜들, 임의의 수신된 호스트 이용가능성 응답 데이터(664)에 의해 식별될 수 있는 임의의 이용가능한 결제 소스들의 임의의 적합한 비-네이티브 결제 크리덴셜들(예컨대, 프롬프트(311)의 결제 옵션 식별자(311a)에 의해 지시될 수 있는 호스트 디바이스(1)의 결제 방법(X), 프롬프트(311)의 결제 옵션 식별자(311b)에 의해 지시될 수 있는 호스트 디바이스(1)의 결제 방법(Y) 등), 및/또는 클라이언트 디바이스(100')에 의해 식별될 수 있는 임의의 적합한 다른 결제 소스(예컨대, 클라이언트 디바이스(100')의 사용자가 결제를 요청하기 위해 임의의 적합한 원격 호스트 디바이스를 (예컨대, 임의의 적합한 고유 호스트 디바이스 식별자, 예컨대, 클라이언트 디바이스(100')에 의해 그 원격 호스트와 통신하는 데 사용될 수 있는 호스트 디바이스의 전화 번호 또는 이메일 주소를 입력함으로써, 또는 클라이언트 디바이스(100')의 연락처 애플리케이션에서 식별될 수 있거나 최근 선택된 호스트 디바이스 또는 그 외의 것으로 식별될 수 있는 호스트 디바이스를 선택함으로써) 수동으로 입력 또는 선택할 수 있게 하는 프롬프트(311)의 결제 옵션 식별자(311c)). 일부 실시예들에서, 결제 소스 선택 프롬프트(311)는 클라이언트 디바이스(100')의 사용자가 특정 결제 소스의 특정 결제 유형(예컨대, 식별자(311a)의 호스트 디바이스(1)의 결제 방법(PM)(X)(예컨대, "계좌 번호가 0096으로 끝나는 아메리칸 익스프레스 카드") 또는 식별자(311b)의 호스트 디바이스(1)의 결제 방법(PM)(Y)(예컨대, "계좌 번호가

0035로 끝나는 마스터카드 카드"))을 선택할 수 있게 하고/하거나 결제 소스 선택 프롬프트(311)는 단순히, (예컨대, 클라이언트 디바이스(100'))에 의해 수신된 호스트 이용가능성 응답 데이터(664)의 특이성에 따라, 또는 클라이언트 디바이스(100'))에 이용가능한 임의의 다른 적합한 데이터에 따라 클라이언트 디바이스(100'))의 사용자가 특정 결제 소스(예컨대, 호스트 디바이스(1) 또는 호스트 디바이스(2))를 선택하지만 그 결제 소스의 특정 결제 유형은 선택하지 않을 수 있게 동작할 수 있다. 일부 실시예들에서, 호스트 이용가능성 응답 데이터(664)는 상업적 엔티티 서브시스템(400) 및/또는 현재 비-응답적일 수 있는 특정 호스트 디바이스(100)(예컨대, 전원 오프되었거나, 단계(612)의 디스커버리 요청에 응답하지 않지만 적합한 결제 크리덴셜을 포함하는 것으로 공지될 수 있는 호스트 디바이스(100))를 위한 클라이언트 디바이스(100'))에 의해 공지된 캐싱된 결제 이용가능성 데이터에 기초할 수 있으며, 프롬프트(311)의 식별자(미도시)는 호스트 디바이스 및 그것의 공지된 결제 크리덴셜 뿐만 아니라 그러한 호스트 디바이스가 현재 전원 오프 상태임을 클라이언트 디바이스(100'))의 사용자에게 경고하는 정보(예컨대, "HD2의 PM Z를 사용을 인에이블하려면 HD2를 켜야합니다.")의 식별을 포함할 수 있다.

[0079]

다음으로, 프로세스(600)의 단계(616)에서, 클라이언트 디바이스(100')는 (예컨대, 프로세스(500)의 단계(506)와 관련하여 설명된 바와 같이) 적어도 하나의 특정 호스트 디바이스(100)에 결제 요청 데이터(666)를 통신할 수 있다. 결제 요청 데이터(666)의 목표 호스트 디바이스(100)는 클라이언트 디바이스(100')에 의해 임의의 적합한 방식으로, 예컨대, 자동으로 또는 도 3b의 결제 소스 선택 프롬프트(311)에 관한 사용자 선택에 응답하여 결정될 수 있고/있거나 그러한 결정은 잠재 거래 데이터(660) 및/또는 호스트 이용가능성 응답 데이터(664)와 같은 임의의 적합한 정보에 기초하여 이루어질 수 있다. 예를 들어, 클라이언트 디바이스(100')의 사용자는 호스트 이용가능성 응답 데이터(664)를 사용하여 하나 이상의 결제 소스의 식별에 기초하여 제공될 수 있는, 도 3b의 결제 소스 선택 프롬프트(311)의 잠재적 목표 호스트 디바이스의 리스트로부터 단계(616)의 결제 요청 데이터(666)에 대한 목표 호스트 디바이스(100)를 선택할 수 있거나(예컨대, 식별자(311a)의 "HD1's PM X" 및 식별자(311b)의 "HD1's PM Y"), 또는 클라이언트 디바이스(100')는 임의의 적합한 특정 목표 호스트 디바이스를 임의의 적합한 방식으로 식별할 수 있다(예컨대, 클라이언트 디바이스(100')의 연락처 애플리케이션 내의 호스트 디바이스 및/또는 (예컨대, 전화 번호 또는 이메일 주소 또는 (예컨대, 도 3b의 식별자(311c)의 옵션을 사용하여) 호스트 디바이스의 임의의 적합한 고유 디바이스 식별자에 의해) 디바이스(100')의 사용자에 의해 수동으로 식별된 호스트 디바이스). 단지 하나의 특정 예로서, 도 3c에 도시된 바와 같이, 클라이언트 디바이스(100')는 도 3b의 결제 소스 선택 프롬프트(311)의 식별자(311a)의 "HD1의 PM X"의 사용자 선택을 수신하는 것에 응답하여 스크린(190c)을 제공하도록 구성될 수 있다. 도 3c의 스크린(190c)은, 예컨대, 도 3c의 요청 호스트 디바이스(HD) 결제 프롬프트(315)의 사용자 선택에 의해, 사용자로 하여금 도 3c의 결제 방법 식별자(313)에 의해 표시된 바와 같이 도 3b의 결제 소스 선택 프롬프트(311)의 선택된 결제 소스에 대한 비-네이티브 호스트 디바이스 결제를 요청하기 위해 하나 이상의 방식으로 클라이언트 디바이스(100')와 상호작용하라고 촉구할 수 있다. 대안적으로, 단계(616)의 결제 요청 데이터(666)에 대해 목표 호스트 디바이스(100)가 단계(614)에서 클라이언트 디바이스(100')에 의해 획득된 임의의 식별 데이터에 응답하여 클라이언트 디바이스(100')에 의해 자동으로 선택될 수 있다(예컨대, 클라이언트 디바이스(100')는 임의의 적합한 특성에 기초하여 이용가능한 호스트 디바이스들의 그룹으로부터 하나의 호스트 디바이스를 선택하도록 주문맞춤화되거나 그렇지 않으면 구성될 수 있음(예컨대, 클라이언트 디바이스(100')와 최단 거리를 갖는 호스트 디바이스 또는 이용가능한 호스트 디바이스의 최고 우선순위를 갖는 호스트 디바이스(예컨대, 이는 디폴트로, 또는 클라이언트 디바이스(100')의 애플리케이션의 주문맞춤화된 설정과 호스트 이용가능성 응답 데이터(664)의 조합 또는 그 외에 의해 결정될 수 있음) 등). 따라서, 단계(616)의 결제 요청 데이터(666)는 (예컨대, 거래 데이터(660) 및/또는 임의의 호스트 이용가능성 응답 데이터(664) 및/또는 (예컨대, 클라이언트 디바이스(100') 상에서 실행 중인 임의의 애플리케이션의) 임의의 애플리케이션 파라미터들에 기초하여) 클라이언트 디바이스(100')와의 임의의 사용자 상호작용 없이 클라이언트 디바이스(100')에 의해 자동으로 생성 및 송신될 수 있다. 단계(616)의 그러한 결제 요청 데이터(666)는 도 1b에 도시된 바와 같이, 단계(616)에서 임의의 적합한 방식으로 통신될 수 있으며, 예컨대, 클라이언트 디바이스(100')와 호스트 디바이스(100) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하여 통신 경로(99)를 통해) 직접 통신되거나, 또는 클라이언트 디바이스(100')와 상업적 엔티티 서브시스템(400) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하여 통신 경로(95)를 통해) 통신되고, 이어서 상업적 엔티티 서브시스템(400)과 호스트 디바이스(100) 사이에서 (예컨대, 임의의 적합한 통신 프로토콜을 사용하여 통신 경로(65)를 통해) 통신될 수 있다. 클라이언트 디바이스(100')는 결제 요청이 이루어질 때 특정 전용 디스커버리 요청 및 응답 사이클이 필요하지 않을 수 있도록, (예컨대, 상업적 엔티티 서브시스템(400)에 의해 일상적으로 수집될 수 있고, 임의의 적합한 시간에 클라이언트 디바이스(100')와 공유될 수 있는 데이터에 기초하여),

클라이언트 디바이스(100')와 연관된 다양한 호스트 디바이스에 이용가능한 다양한 결제 유형의 로컬 캐시(예컨대, 클라이언트 디바이스(100')에 로컬인 메모리)를 유지하도록 동작할 수 있다. (예컨대, 클라이언트 디바이스(100') 상의) 네이티브 크리덴셜들 및/또는 (예컨대, 하나 이상의 호스트 디바이스(100) 상의) 비-네이티브 크리덴셜들로부터 하나 이상의 이용가능한 결제 유형이 클라이언트 디바이스(100')에 의해 결정될 때, 특정 결제 소스의 자동 선택 및/또는 클라이언트 디바이스(100')의 사용자의 선택을 위한 다양한 결제 소스 사이의 우선순위 부여가 인에이블될 수 있다. 예를 들어, 클라이언트 디바이스(100')는 선택한 결제 소스를 포함할 수 있는 클라이언트 디바이스(100')와 호스트 디바이스 사이의 거리에 기초하여 적어도 하나의 이용가능한 결제 소스들 중 하나가 결제 요청 내에 목표화 및 식별되도록 자동으로 선택하거나 우선순위를 부여하도록 동작할 수 있다(예컨대, 이용가능한 결제 소스를 갖는 호스트 디바이스로서 클라이언트 디바이스에 가장 가까운 호스트 디바이스가(예컨대, 이는 디스커버리 응답 내의 거리 데이터로부터 결정되거나 다른 적합한 통신 관련 데이터(예컨대, 검출된 통신 신호 강도 블루투스 등)를 통해 결정될 수 있음) 클라이언트 디바이스의 사용자의 사용의 용이성을 촉진하도록 자동으로 선택될 수 있음). 대안적으로 또는 부가적으로, 클라이언트 디바이스(100')는 판매자에 의해 지원되는 결제 소스들에 기초하여 적어도 하나의 이용가능한 결제 소스들 중 하나가 결제 요청 내에 목표화 및 식별되도록 자동으로 선택하거나 우선순위를 부여하도록 동작할 수 있다(예컨대, 기업 브랜드 결제 크리덴셜은 해당 기업과의 거래에서의 사용에 우선순위가 부여될 수 있음(예컨대, 디즈니 브랜드 비자 카드는 디즈니 판매자와의 거래에서의 사용에 우선순위가 부여되거나 선택될 수 있으며, 그러한 선호는 판매자에 의해 표현되어 클라이언트 디바이스(100')에 이용가능하게 될 수 있음)).

[0080] 결제 요청 데이터(666)는 지불될 잠재 거래의 하나 이상의 특정 특성들을 식별하기 위해 클라이언트 디바이스(100')에 의해 목표 호스트 디바이스(100)에 제공될 수 있는 임의의 적합한 정보를 포함할 수 있다. 예를 들어, 단계(610)의 잠재 거래 데이터(660)와 마찬가지로, 단계(616)의 결제 요청 데이터(666)는 지불될 잠재적 금융 거래와 관련된 임의의 적합한 데이터를 포함할 수 있으며, 이에 제한되지는 않으나, 다음을 포함할 수 있다. (i) 특정 판매자 정보, 예컨대, 판매자(즉, "판매자 A")의 고유 판매자 식별자 및/또는 사용 중인 특정 판매자 리소스(예컨대, 특정 판매자 애플리케이션(113'))의 식별, (ii) 특정 거래 정보, 예컨대, 거래를 위해 결제하는 데 사용될 특정 화폐(예컨대, 엔, 파운드, 달러 등)의 식별, 및/또는 거래를 위해 결제될 특정 화폐 금액의 식별(즉, "금액 C"), 및/또는 구매 또는 임대 또는 그렇지 않으면 지불될 특정 제품 또는 서비스의 식별(즉, "제품 B"), 및/또는 사용될 디폴트 또는 초기 배송 주소의 식별(즉, "배송 D"), (iii) 거래를 위해 판매자에게 수령가능한 하나 이상의 유형의 결제 방법들(예컨대, 구매에 사용될 수 있는 결제 카드들의 리스트(예컨대, 비자를 제외한 마스터 카드)), 또는 클라이언트 디바이스(100')에 의해 선택된 결제 방법들을 나타내는 정보(즉, "HD1의 PM X"), (iv) 고유 판매자-기반 거래 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행 중인 거래와의 연관을 위해 판매자 서브시스템(200)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열), (v) 고유 클라이언트-기반 거래 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행 중인 거래와의 연관을 위해 클라이언트 디바이스(100')에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열), 및/또는 (vi) 고유 클라이언트-기반 결제 요청 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 결제 요청 데이터(666)에 의해 진행 중인 결제 요청과의 연관을 위해 클라이언트 디바이스(100')에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열). 일부 실시예들에서, 결제 요청 데이터(666)는 목표 호스트 디바이스(100)에 통신되기 전에 상업적 엔티티 서브시스템(400)에 의해 암호화되거나 그렇지 않으면, 포맷 또는 핸들링될 수 있다. 그러한 결제 요청 데이터(666)는 본 명세서에서 *PKRemotePaymentRequest*로 지칭될 수 있으며, 이에 제한되지는 않지만, 다음을 포함하는 임의의 적합한 데이터를 포함할 수 있다. (1) 단계(610)의 잠재 거래 데이터(660)의 *PKPaymentRequest*(예컨대, 이는 *PKRemotePaymentRequest* 내에 래핑될 수 있음), (2) 본 명세서에서 *PKRemoteDevice*로 지칭될 수 있는, 선택된 목표 호스트 디바이스를 식별하는 임의의 적합한 데이터(예컨대, 단계(614)의 호스트 이용가능성 응답 데이터(664)에 포함될 수 있는 호스트 디바이스(100)의 호스트 디바이스 식별자(119)), (3) 목표 호스트 디바이스의 선택된 또는 디폴트의 특정 결제 크리덴셜을 식별하는, 본 명세서에서 *SelectedApplicationIdentifier*로 지칭될 수 있는 임의의 적합한 데이터(예컨대, 호스트 디바이스(100)의 보안 요소(145)의 AID(155aa)로서, 단계(614)의 호스트 이용가능성 응답 데이터(664)에 포함될 수 있고/있거나 클라이언트 디바이스(100')에서 자동으로 또는 사용자-선택될 수 있음), 및/또는 (4) 본 명세서에서 *RemotePaymentIdentifier*로 지칭될 수 있는, 결제 요청과 연관된 고유 식별자(예컨대, 클라이언트 및 시스템의 호스트 디바이스를 통해 결제 요청을 식별하는데 사용될 수 있고 클라이언트 디바이스(100) 또는 그 외의 것에 의해 생성될 수 있는 고유 값)를 식별하는 임의의 적합한 데이터.

[0081] 단계(616)에서 클라이언트 디바이스(100')로부터 결제 요청 데이터(666)를 수신하는 것에 응답하여, 목표 호스

트 디바이스(100)는 결제 요청에 따라 조치하기 위해 호스트 디바이스(100)의 사용자에게 임의의 적합한 정보를 제공하도록 동작할 수 있다. 예를 들어, 도 3d에 도시된 바와 같이, 클라이언트 결제 요청이 수신되었다는 것을 식별자(317)를 이용하여 호스트 디바이스(100)의 사용자에게 나타내도록 동작할 수 있는 푸시 알림 스크린(190d)이 호스트 디바이스(100)의 GUI에 의해 제공될 수 있고, 통지를 숨기기 위해 선택될 수 있는 옵션(321) 및/또는 통지에 관한 추가 상세사항을 보기 위해 선택될 수 있는 옵션(319)을 포함할 수 있다. 예를 들어, 추가 상세사항 보기 옵션(319)의 사용자 선택에 응답하여, 또는 스크린(190d) 대신에, 호스트 디바이스(100)의 GUI는 호스트 디바이스(100)의 사용자가 하나 이상의 적합한 방식으로 클라이언트 결제 요청에 응답할 수 있게 하는, 도 3e의 스크린(190e)으로 진행할 수 있다. 도 3e의 스크린(190e)은 호스트 디바이스(100)의 사용자에게, 구매를 하기 위해 프로세스(600)와 유사한 프로세스를 통해 하나 이상의 방식으로 호스트 디바이스(100)와 상호작용하여 호스트 디바이스(100)에 네이티브이거나 디바이스(100)에 비-네이티브이지만 액세스가능한 특정 크리덴셜을 선택할 것을 촉구할 수 있다. 도 3e에 도시된 바와 같이, 단계(616) 이전 및/또는 단계(616)에서, 도 3c의 스크린(190c) 상의 클라이언트 디바이스(100')의 사용자에게 식별된 잠재 거래에 대한 판매자, 제품, 가격 및 배송 정보와 동일하게 호스트 디바이스(100')의 사용자에게 식별해줄 수 있는 식별자(307a 내지 307d)에 부가하여, 스크린(190e)은 사용자가 잠재 거래를 지불하는 데 사용하기 위해 잠재적인 다수의 크리덴셜들 중 호스트 디바이스(100) 상에 프로비저닝될 수 있는 하나(예컨대, 크리덴셜 SSD(154a)의 크리덴셜)를 선택할 수 있게 할 수 있는 크리덴셜 선택 프롬프트(323)를 포함할 수 있다. 프롬프트(323)는 판매자에 의해 지원되는 결제 네트워크들과 연관된 호스트 디바이스(100)에 네이티브인 크리덴셜들(예컨대, 이는 전술한 바와 같이, 결제 요청 데이터(666)에 의해 결정될 수 있음)만을 포함할 수 있다. 도시된 바와 같이, 프롬프트(323)는 호스트 디바이스(100)의 "크리덴셜(X)"와 연관된 제1 네이티브 결제 크리덴셜 옵션(325) 및 호스트 디바이스(100)의 "크리덴셜(Y)"와 연관된 제2 네이티브 결제 크리덴셜 옵션(327)을 포함할 수 있으며, 각각은 (예컨대, 결제 요청 데이터(666)의 임의의 적합한 부분에 기초하여) 잠재 거래의 판매자 서브시스템(200)에 의한 사용을 위해 수령가능한 것일 수 있고/있으며, 적용가능한 경우, 클라이언트 디바이스(100')에 의해 선택된 크리덴셜을 식별하기 위해 임의의 적합한 기술이 사용될 수 있다(예컨대, (예컨대, 도 3b의 스크린(190b)에서) "PM X"가 클라이언트 디바이스(100')에 의해 선택되고, 결제 요청 데이터(666) 내에 구체적으로 식별된다면 "크리덴셜(X)"와 연관된 제1 네이티브 결제 크리덴셜 옵션(325) 다음에 "*"가 제공될 수 있음). 도 3f에 도시된 바와 같이, 호스트 디바이스(100)의 GUI는 도 3e의 스크린(190e)의 크리덴셜 선택 프롬프트(323)로부터 특정 크리덴셜(예컨대, "크리덴셜(X)")에 대한 호스트 디바이스 사용자 선택을 수신하는 것에 응답하여 스크린(190f)을 제공하도록 구성될 수 있다. 도 3f의 스크린(190f)은 크리덴셜 식별자 정보(329)를 이용하여 선택되거나 자동으로 식별된 디폴트 크리덴셜을 식별할 수 있고, 호스트 디바이스(100)의 사용자에게 사용자 및 선택된 크리덴셜을 활용하려는 그의 의도를 입증하기 위해 하나 이상의 방식으로 호스트 디바이스(100)와 상호작용하도록 촉구할 수 있다. 이는 사용자에게 (예컨대, 인증 프롬프트(331)를 이용하여) 개인 식별 번호("PIN") 입력을 통하거나 또는 생체 인식 센서와의 사용자 상호작용을 통해 호스트 디바이스(100)의 보안 요소에 액세스하고, 따라서 구매를 위해 사용될 크리덴셜에 액세스하기 위해 사용자 인증을 입력하도록 촉구하는 것을 포함할 수 있다.

[0082] 단계(616)에서 상이한 예의 결제 요청 데이터(666)가 상이한 목표 호스트 디바이스들(예컨대, 빠른 응답의 가능성을 증가시키기 위해 이용가능한 호스트 디바이스의 그룹(예컨대, 어린이 클라이언트 디바이스로부터 그의 아버지의 호스트 디바이스 및 그의 어머니의 호스트 디바이스까지)로 전송될 수 있다. 슬립 상태의 호스트 디바이스가 목표 호스트 디바이스인 경우, 그 호스트 디바이스에 대한 결제 요청 데이터(666)는 그 목표 호스트 디바이스가 온라인될 때 그와 공유하기 위해 큐잉될 수 있으며(예컨대, 상업적 엔티티 서브시스템(400) 또는 클라이언트 디바이스(100') 그 자체에 의한), 그러한 큐잉은 특정 시간의 기간 동안만 인에이블될 수 있다(예컨대, 그러한 결제 요청 데이터(666)의 생성 이후의 2시간일 수 있고, 그 이후가 되면 그러한 결제 요청 데이터는 만료된 것으로 간주되고 그것의 목표 호스트 디바이스에 제공되지 않을 수 있음). 언급된 바와 같이, 프롬프트(311)는 특정 호스트 디바이스가 온라인이 아니라는 클라이언트 디바이스(100')에 대한 통보를 포함할 수 있으며 - 또는 특정 호스트 디바이스가 결제 요청 데이터에 응답하지 않음을 나타내기 위해 통지가 제공될 수 있다 - 클라이언트 디바이스의 사용자에게 해당 호스트 디바이스를 인에이블하는 단계들을 취하라는 요청을 생성할 수 있는 통지를 생성할 수 있다. 상업적 엔티티 서브시스템(400)은 특정 클라이언트 디바이스로부터의 특정 디스커버리 요청 및/또는 특정 결제 요청이 특정 호스트 디바이스로 가지 않도록 차단하도록 동작할 수 있는 설정을 관리하도록 동작할 수 있거나, 또는 특정 호스트 디바이스는 임의의 적합한 옵션들을 설정하여 특정 클라이언트 디바이스로부터의 그러한 요청들을 차단하도록 동작할 수 있다.

[0083] 호스트 디바이스(100)의 사용자가, 단계(616)에서 수신된 결제 요청 데이터(666)에 응답하여 잠재 거래를 지불하는 용도로서 특정 결제 크리덴셜을 기꺼이 선택 또는 확인한다거나 그렇게 할 수 있다면, 프로세스(600)는 단

계(625)로 진행하고, 프로세스(600)는, (예컨대, 도 3f의 인증 프롬프트(331)의 사용자 선택을 통해) 잠재 거래 데이터(666)에 기초하여 특정 판매자, 제품, 가격 및 배송 목적지에 대한 잠재 거래를 이행하기 위해 특정 크리덴셜을 활용하겠다는 호스트 디바이스(100)의 사용자에게 의한 의도 및 인증을 수신하는 단계를 포함할 수 있다. 액세스 SSD(154b)는 호스트 디바이스(100)의 애플릿(153b)을 레버리지하여, 상거래 크리덴셜 데이터 통신에서 그 크리덴셜 정보를 인에이블하기 위해 다른 SSD(154)들(예컨대, 크리덴셜 SSD(154a))이 사용되도록 허용하기 전에 그러한 인증이 발생했는지 여부를 결정할 수 있다. 단계(625)의 단지 하나의 예로서, 액세스 SSD(154b)의 애플릿(153b)은 (예컨대, 디바이스(100)의 임의의 애플리케이션(예컨대, 호스트 디바이스(100)의 카드 관리 애플리케이션(113b))과 상호작용하는 사용자에게 의해 사용될 수 있는, 도 3의 생체인식 입력 컴포넌트(110i)와 같은 하나 이상의 입력 컴포넌트(110)를 통해) 호스트 디바이스(100)의 사용자의 의도 및 로컬 인증을 결정하도록 구성될 수 있고, 그러한 결정에 응답하여 (예컨대, 크리덴셜 SSD(154a)의 크리덴셜을 이용하여) 결제 거래를 수행하기 위해 다른 특정 SSD를 인에이블하도록 구성될 수 있다. 일부 실시예들에서, 그러한 결정 후에, 그러나 그러한 인에이블을 하기 전에, 호스트 디바이스(100)의 GUI는, (예컨대, 도 3g의 프롬프트(333)와 유사한 프롬프트를 이용하여) 호스트 디바이스(100)의 사용자에게 최종적으로는 선택 및 인증된 크리덴셜을 사용하여 결제를 개시하기 위한 하나 이상의 방식으로 호스트 디바이스(100)와 상호작용하도록 촉구할 수 있는 다른 스크린(예컨대, 도 3g의 스크린(190g)과 유사함)을 제공하도록 구성될 수 있다.

[0084]

호스트 디바이스(100)의 사용자는 단계(625)에서, 단계(616)의 결제 요청 데이터(666)에 의해 식별된, 잠재 거래를 지불하기 위한, 호스트 디바이스(100)에 네이티브한 특정 결제 크리덴셜 정보의 사용에 대한(예컨대, 스크린들(190c 및 190e)의 "판매자 A" 및 "제품 B" 및 "가격 C" 및 "배송 D"에 대한) 의도 및 인증을 제공할 수 있으며, 따라서 단계(625)는 단계(616) 직후에 발생할 수 있다. 그러나, 대안적으로, 프로세스(600)는 임의의 의도 및 인증이 단계(625)에서 제공되기 전에 호스트 디바이스(100)의 사용자가 잠재 거래의 하나 이상의 특성을 조정할 수 있게 할 수 있다. 예를 들어, 단계(616)에서 결제 요청 데이터(666)를 수신한 후에, 호스트 디바이스(100)는 거래를 위한 배송 주소, 거래를 위한 배송 방법 및/또는 거래를 위한 결제 방법과 같은 잠재 거래의 임의의 적합한 특성을 자동으로 또는 호스트 디바이스(100)와의 (예컨대, 스크린(190e)을 이용한) 임의의 적합한 사용자 상호작용에 응답하여 조정하도록 동작할 수 있다. 프로세스(600)는 단계(616)에서 단계(625)로 진행하기보다는, 단계(618)를 포함할 수 있으며, 이에 의해 호스트 디바이스(100)는 결제 요청 데이터(666)에 응답하여 호스트 응답 데이터(668)를 클라이언트 디바이스(100')로 다시 전송할 수 있다. 그러한 호스트 응답 데이터(668)는 호스트 디바이스(100)에 의해 적어도 부분적으로 정의될 수 있는 임의의 적합한 잠재 거래 데이터를 나타내는 임의의 적합한 데이터를 포함할 수 있다. 예를 들어, 도 3e의 스크린(190e)과의 상호작용을 통해, 호스트 디바이스(100)의 사용자는 제1 네이티브 결제 크리덴셜 옵션(325)의 "크리덴셜 X"를 선택할 수 있을 뿐만 아니라(예컨대, 결제 요청 데이터(666)에 의해 식별된 것과 동일하거나 상이한 결제 방법), 잠재 거래가 "제품 B"를 클라이언트 디바이스(100')의 스크린(190c) 및 결제 요청 데이터(666)에 의해 식별되었을 수 있는 초기 "배송 주소 D"보다는 새로운 "배송 주소 E"로 배송하도록 선택할 수도 있다. 따라서, 호스트 디바이스가 결제 요청 데이터의 배송 주소 정보 또는 임의의 다른 적합한 부분을 업데이트한 것에 응답하여 - 이는 프로세스(600)가 거래의 지불을 가능하게 하기 전에, 클라이언트 디바이스(100') 및/또는 판매자 서브시스템(200)의 프로세싱될 필요가 있을 수 있음 -, 호스트 디바이스(100)는 단계(618)에서, 업데이트된 배송 정보를 나타내는 호스트 응답 데이터(668)를 생성하여 (예컨대, 상업적 엔티티 서브시스템(400)을 통하거나 그렇지 않으면 프로세스(600) 동안 호스트 디바이스(100)와 클라이언트 디바이스(100') 사이에서 통신되는 임의의 다른 정보와 유사하게) 클라이언트 디바이스(100')에 전송하도록 동작할 수 있다. 그러한 호스트 응답 데이터(668)는 결제 요청 데이터(666)와 실질적으로 유사할 수 있지만, 호스트 디바이스(100)에 의해 식별된 모든 변경(예컨대, "배송 주소 D"에서 "배송 주소 E"로의 변경)을 나타낼 수 있다. 다음으로, 클라이언트 디바이스(100')는 단계(618)에서 그러한 호스트 응답 데이터(668)를 수신하고, 단계(620)에서 그러한 호스트 응답 데이터(668)의 적어도 일부분을 업데이트된 거래 요청 데이터(670)로서 판매자 서브시스템(200)에 통신할 수 있으며, 업데이트된 거래 요청 데이터(670)는 잠재 거래 데이터(660)에 대한 임의의 하나 이상의 요구되는 업데이트를 판매자 서브시스템(200)에게 식별해줄 수 있다(예컨대, 호스트 디바이스(100)에 의해 식별된 바와 같은 "배송 주소 D"에서 "배송 주소 E"로의 변경, 또는 단계(610) 이후 및/또는 단계(618) 이후이되 단계(620) 이전에 클라이언트 디바이스(100')에 의해 국부적으로 이루어진 임의의 변경)(예컨대, 클라이언트 디바이스(100')의 사용자에게 의한 스크린(190b)에서의 특정 결제 방법(311a)의 선택은 업데이트된 거래 요청 데이터(670)를 생성할 수 있음).

[0085]

그러한 업데이트된 거래 요청 데이터(670)의 수신 및 프로세싱에 응답하여, 판매자 서브시스템(200)은 단계(622)에서 클라이언트 디바이스(100')에 임의의 적합한 업데이트된 잠재 거래 데이터(672)를 생성 및 송신하도록 동작할 수 있으며, 이는 잠재 거래 데이터(660)와 실질적으로 유사할 수 있으나, 클라이언트 디바이스(100')

및/또는 호스트 디바이스(100)에 의해 행해진 임의의 업데이트들(예컨대, "배송지 주소 D"에서 "배송지 주소 E"로 변경) 뿐만 아니라, 그러한 결과로서 판매자 서브시스템(200)에 의해 변경되었을 수 있는 임의의 부가적 잠재 거래 정보를 나타낼 수 있다(예컨대, 가격이 잠재 거래 데이터(660)의 "가격 C"에서 새로운 "가격 C*"로 변경되었을 수 있는데, 이는 "배송 주소 D"에서 "배송 주소 E"로의 변경과 연관된 상이한 배송 비용으로 인한 것일 수 있음). 다른 예로서, 클라이언트 디바이스(100')가 결제 방법 옵션(311a)을 선택한 후에 결제 방법 옵션(311b)을 선택하고 (예컨대, 스크린(190c)에서 요청 결제 프롬프트(315)를 선택하는 것 이전에) 적합한 업데이트된 거래 요청 데이터(670)를 전송하는 것에 응답하여, 판매자 서브시스템(200)은 단계(622)에서 임의의 적합한 업데이트된 잠재 거래 데이터(672)를 생성하여 클라이언트 디바이스(100')에 송신하도록 동작할 수 있으며, 이는 잠재 거래 데이터(660)와 실질적으로 유사할 수 있지만, 클라이언트 디바이스(100')에 의해 이루어진 업데이트(예컨대, 옵션(311a)의 "결제 방법 X"에서 옵션(311b)의 "결제 방법 Y"로의 변경) 뿐만 아니라 그 결과로서 판매자 서브시스템(200)에 의해 변경될 수 있는 임의의 부가적인 잠재 거래 정보를 나타낼 수 있다(예컨대, 가격은 잠재 거래 데이터(660)의 "가격 C"로부터 새로운 "가격 C*"로 변경될 수 있고, 이는 상이한 결제 방법이 선택되는 것에 기인한 것일 수 있음(예컨대, 판매자 브랜드 결제 방법의 선택은 판매자에 의해 브랜드화되지 않은 결제 방법의 선택에 비해 가격 절감을 실현할 수 있음)). 그러한 업데이트된 잠재 거래 데이터(672)는 클라이언트 디바이스(100')에 의해 수신되어 (예컨대, 업데이트된 스크린(190c)을 제공함으로써) 프로세싱될 수 있고/있거나 클라이언트 디바이스(100')는 단계(624)에서 업데이트된 결제 요청 데이터(674)를 생성하여 호스트 디바이스(100)에 전송할 수 있다. 결제 요청 데이터(666), 호스트 응답 데이터(668) 및 업데이트된 결제 요청 데이터(674) 각각은, 그러한 데이터 간에 변동되는 소정의 다른 정보(예컨대, 배송 주소 정보 및/또는 결제 방법 정보 및/또는 가격 정보)가 있음에도 불구하고, 동일한 고유 판매자-기반 거래 식별자 및/또는 동일한 고유 클라이언트-기반 거래 식별자 및/또는 동일한 고유 클라이언트-기반 결제 요청 식별자(예컨대, *RemotePayment Identifier*)와 연관될 수 있거나 포함될 수 있다. 따라서, 클라이언트 디바이스(100')에 의한 잠재 거래 데이터(660)의 임의의 적합한 부분에 대한 임의의 변경에 응답하여 및/또는 호스트 디바이스(100)에 의한 결제 요청 데이터(666)의 임의의 적합한 부분에 대한 임의의 변경, 예컨대, 결제 방법의 변경(예컨대, 제1 결제 크리덴셜에서 제2 결제 크리덴셜로의 변경) 및/또는 배송 방법의 변경(예컨대, 지상 배달 방법에서 2일 항공 배달 방법에서의 변경) 및/또는 배송 주소의 변경(예컨대, 제1 배송 주소에서 제2 배송 주소로의 변경) 및/또는 임의의 다른 적합한 데이터 유형에 대한 변경에 응답하여, 업데이트된 거래 요청이 업데이트된 거래 데이터(672)를 생성할 수 있고 이는 업데이트된 결제 요청 데이터(674)를 생성할 수 있으며, 이는 단계(624)에서 호스트 디바이스(100)로 전송될 수 있으며, 다만 거래 식별자는 일관되게 유지된다. 클라이언트 디바이스(100') 및 호스트 디바이스(100) 중 어느 하나, 또는 둘 모두는 각각의 디바이스의 사용자 인터페이스의 성능에 의존하여 거래 정보의 적어도 일부분(예컨대, 배송 방법, 배송지 주소, 결제 방법 등)을 변경하도록 동작할 수 있거나, 아무것도 그러지 않을 수 있다. 임의의 적합한 요청/응답 모델이 어느 하나의 디바이스에 의한 임의의 적합한 변경에 기초하여 업데이트 요청들 및 응답들의 적합한 생성을 가능하게 하기 위해 채용될 수 있다. 예를 들어, 업데이트된 잠재 거래 데이터(672) 및/또는 업데이트된 결제 요청 데이터(674)는 업데이트를 확인하고 결제 요약 항목들, 배송 방법들, 결제 상태 및/또는 기타를 포함할 수 있는 업데이트된 정보를 제공할 수 있다. 예를 들어, 업데이트 거래 요청 데이터(670)에 응답하여, 업데이트된 총합계 및 배송 방법, 또는 "무효 배송 주소"의 결제 상태를 포함할 수 있는 업데이트된 잠재 거래 데이터(672)가 발생할 수 있다. 디바이스들 사이의 임의의 적합한 기본 통신 프로토콜(예컨대, 클라이언트 디바이스(100')와 호스트 디바이스(100) 사이의 아이덴티티 서비스 전송 계층)은, 다른 디바이스가 업데이트를 수신하고 프로세싱된 때를 각각의 디바이스가 알고 있도록 보장하도록 동작할 수 있는 완료 핸들러를 제공하도록 동작할 수 있다(예컨대, 아이메시지™ 또는 기타 적합한 미디어 메시징 프로토콜의 "수신 확인"과 유사). 예를 들어, 결제 연속성 서비스는 클라이언트와 호스트 디바이스 사이의 결제 요청 및 결제 응답의 보안 통신을 가능하게 하기 위해 제공될 수 있으며, 클라이언트 디바이스 및 호스트 디바이스 각각은 그 서비스의 메시징 전송을 사용할 수 있을 수 있다. (예컨대, 상업적 엔티티 서브시스템(400)의 IDMS 컴포넌트(470) 또는 그 외의 것)(예컨대, 호스트 디바이스(100)의 IDS 애플리케이션(113d)과 같은 IDS 전송) 그러한 데이터를 통신하기 위한 임의의 적합한 메커니즘들, 예컨대, 애플 링크.에 의한 핸드오프™(Handoff™)(예컨대, 디바이스들 간의 애플리케이션 데이터의 끊임없는 공유) 또는 애플 링크.에 의한 에어드롭™(AirDrop™)(예컨대, 보안 애드 호크 전송 프로토콜) 또는 애플 링크.에 의한 Continuity™ SMS/MMS 등이 채용될 수 있다. 또한, 디바이스는 어느 것이든 요청을 취소하도록 동작할 수 있으며(예컨대, 클라이언트 디바이스(100')는 단계(612) 이후 및/또는 단계(624) 이후에 송신된 요청을 취소할 수 있고/있거나 호스트 디바이스(100)는 단계(612) 및/또는 단계(624) 이후에 수신된 요청을 취소할 수 있음), 이는 각각의 디바이스 상의 데이터의 체시를 업데이트하도록 동작할 수 있다(예컨대, 업데이트 스크린들 (190c, 190e)). 특정 거래를 위한 모든 요청/응답의 공통인 *RemotePayment Identifier* 는 각각의 디바이스에 의해 각각의 디바이스가

동일한 특정 거래와 관련하여 통신하고 있음을 확인하는 데 사용될 수 있다. 예를 들어, 특정 *RemotePaymentIdentifier*를 갖는 가장 최근에 수신된 결제 요청은 호스트 디바이스에 의해, 동일한 특정 *RemotePaymentIdentifier*를 가지고 임의의 이전에 수신된 결제 요청보다 앞서 사용될 수 있다.

[0086]

다음으로, 단계(625)에서, 특정 결제 요청 데이터(예컨대, 단계(616)의 결제 요청 데이터(666) 또는 단계(624)의 업데이트된 결제 요청 데이터(674))를 수신하는 것에 응답하여 특정 결제 크리덴셜에 대해 의도 및 인증이 수신되면, 프로세스(600)의 단계들(626 내지 628)은 호스트 디바이스(100)가 상업적 엔티티 서브시스템(400)에 의한 사용을 위해 호스트 거래 데이터(678)를 생성, 암호화 및 송신하는 단계를 포함할 수 있다(예컨대, 프로세스(500)의 단계들(508 및 510)과 관련하여 설명된 바와 같음). 호스트 디바이스(100)의 보안 요소(145) 상의 크리덴셜 SSD(154a)의 크리덴셜이 금융 거래에서의 사용을 위해 선택되고, 인증 및/또는 인에이블되면(예컨대, 단계(625), 호스트 디바이스(100)의 보안 요소(145)(예컨대, NFC 컴포넌트(120)의 프로세서 모듈(142))는 상업적 엔티티 서브시스템(400)에 의한 사용을 위해 그 선택된 크리덴셜의 특정 크리덴셜 데이터를 생성 및 암호화할 수 있다. 예를 들어, 단계(626)에서, 크리덴셜 SSD(154a)의 호스트 결제 크리덴셜 데이터(675)(예컨대, SSD(154a)의 결제 카드 데이터(예컨대, 선택된 "크리덴셜 X"와 연관될 수 있음)), 예컨대, 토큰 데이터 및 암호화 데이터(예컨대, 프로세스(500)의 단계(508)에 관해 상술한 바와 같음)가 생성되고/되거나 크리덴셜 키(155a')를 이용하여 적어도 토큰 데이터 및 암호화 데이터를 포함하는 호스트 결제 크리덴셜 데이터(676)로 적어도 부분적으로 암호화되어, 그러한 암호화된 호스트 결제 크리덴셜 데이터(676)는 호스트 결제 크리덴셜 데이터(675)를 액세스하기 위해 그 크리덴셜 키(155a')에 대한 액세스를 갖는 엔티티(예컨대, 금융 기관 서브시스템(350)에 의해서만 복호화될 수 있다. 그 호스트 결제 크리덴셜 데이터(675)는 그 크리덴셜로 결제하는데 필요한 모든 데이터, 예컨대, 기본 계좌 번호(예컨대, 실제 F-PAN 또는 가상 D-PAN), 카드 보안 코드(예컨대, 카드 검증 코드("CVV")), 만료 날짜, 크리덴셜과 연관된 이름, 연관된 암호화 데이터(예컨대, 보안 요소(145)와 금융 기관 서브시스템(350) 사이의 공유 비밀을 사용하여 생성된 암호문 및 임의의 다른 적합한 정보) 및/또는 기타를 포함할 수 있다. 일부 실시예들에서, 크리덴셜 SSD(154a)의 호스트 결제 크리덴셜 데이터(675)의 일부 또는 전부가 단계(626)에서 크리덴셜 키(155a')를 이용하여 암호화된 호스트 결제 크리덴셜 데이터(676)로서 암호화되면, 그 암호화된 호스트 결제 크리덴셜 데이터(676)는, 단계(627)에서, 단독으로 또는 적용 가능한 결제 요청 데이터(666/674)의 제1 부분(또는 전부)과 함께(예컨대, 판매자의 식별, 가격 금액의 식별, 화폐 및/또는 배송 및/또는 제품의 식별, 및/또는 고유 판매자-기반 거래 식별자 및/또는 고유 클라이언트-기반 거래 식별자 및/또는 고유 클라이언트-기반 결제 요청 및/또는 기타를 포함할 수 있는 잠재 거래 데이터(660/672)의 일부 또는 전부) 및/또는 임의의 다른 적합한 정보(예컨대, 호스트 디바이스(100) 자신을 식별하는 임의의 정보(예컨대, 호스트 디바이스 식별자(119), 임의의 특정 호스트 디바이스-기반 거래 식별자 및/또는 기타)는 액세스 정보에 의해(예컨대, SSD(154a)의 액세스 키(155a), 액세스 SSD(154b)의 액세스 키(155b), ISD 키(156k) 및/또는 CRS(151k)에 의해 그리고/또는 CASD(158k)에 의해 서명됨) 암호화된 호스트 결제 데이터(677)로서 암호화될 수 있다. 예를 들어, 호스트 디바이스(100)의 보안 요소(145)(예컨대, NFC 컴포넌트(120)의 프로세서 모듈(142))는 액세스 정보를 사용하여 데이터(660/666/672/674)로부터 판매자의 식별(예컨대, 판매자 또는 그의 구매 용도의 리소스, 예컨대, 애플리케이션(113')의 식별)과 데이터(660/666/672/674)로부터 구매 및/또는 화폐 코드의 금액의 식별 뿐만 아니라 SSD(154a)의 암호화된 호스트 결제 크리덴셜 데이터(675)(예컨대, 암호화된 호스트 결제 크리덴셜 데이터(676))를 암호화된 호스트 결제 데이터(677)로 암호화할 수 있다. 일부 실시예들에서, 크리덴셜 SSD(154a)의 호스트 결제 크리덴셜 데이터(675)(예컨대, 토큰 데이터 및 암호화 데이터와 같은 SSD(154a)의 결제 카드 데이터)는 (예컨대, 프로세스(500)의 단계(508)에 관해 상술한 바와 같이) 생성되긴 하되, (예컨대, 단계 627에서 데이터(677)로서) 상업적 엔티티 키 또는 액세스 키를 이용하여 암호화되기 전에 (예컨대, 단계(626)에서 데이터(676)로서) 크리덴셜 키를 이용하여 암호화되지는 않으며, 그 대신에, 그러한 호스트 결제 크리덴셜 데이터(675)는 (예컨대, 단계(627)에서 데이터(677)로서) 상업적 엔티티 키 또는 액세스 키를 이용하여 암호화될 수 있고, 따라서 그러한 실시예들에서, 데이터(676)에 대한 임의의 그 이후로의 참조는 임의의 크리덴셜 키를 이용하여 암호화되지 않은 데이터(675)를 참조할 수도 있다. 일부 실시예들에서, 그러한 상업적 엔티티 키 또는 액세스 키는 상업적 엔티티 서브시스템(400)의 스킴과 연관된 상업적 엔티티 공개 키일 수 있으며, 상업적 엔티티 서브시스템(400)은 연관된 상업적 엔티티 개인 키에 대한 액세스를 가질 수 있다. 상업적 엔티티 서브시스템(400)은 그러한 상업적 엔티티 공개 키를 금융 기관 서브시스템(350)에 제공할 수 있고, 이어서, 금융 기관 서브시스템(350)은 ((예컨대, 프로세스(600)의 단계(654)에서) 예컨대, 호스트 디바이스(100)에 크리덴셜 데이터를 프로비저닝할 때) 그 상업적 엔티티 공개 키를 호스트 디바이스(100)와 공유할 수 있다.

[0087]

다음으로, 암호화된 호스트 결제 데이터(677)는 임의의 부가적 정보, 예컨대, 결제 요청 데이터(666/674)의 적어도 일부(예컨대, 판매자의 식별, 가격 금액의 식별, 화폐의 식별, 고유 판매자-기반 거래 식별자, 제품/서비

스의 식별 및/또는 기타) 및/또는 임의의 다른 적합한 정보(예컨대, 호스트 디바이스(100) 자체를 식별하는 임의의 정보, 고유 호스트 디바이스 기반 거래 식별자 및/또는 기타)와 함께, 단계(628)에서 호스트 디바이스(100)로부터 상업적 엔티티 서브시스템(400)으로 호스트 거래 데이터(678)로서 함께 송신될 수 있다(예컨대, 프로세스(500)의 단계(510)와 관련하여 설명된 바와 같음). 그러므로, 호스트 거래 데이터(678)의 적어도 일부(예컨대, 암호화된 호스트 결제 데이터(677))는 호스트 거래 데이터(678)의 암호화된 호스트 결제 데이터(677)를 생성한 암호화에 사용된 액세스 정보(예컨대, 액세스 키(155a), 액세스 키(155b), ISD 키(156k), CRS(151k) 및/또는 CASD(158k))에 대한 액세스를 갖는 엔티티(예컨대, 상업적 엔티티 서브시스템(400))에 의해서만 복호화될 수 있다. 그러한 호스트 거래 데이터(678)는 단계들(626 내지 628)에서 생성되고 이어서 단계(628)에서(예컨대, NFC 컴포넌트(120)의 보안 요소(145)로부터 통신 컴포넌트(106) 및 통신 경로(65)를 통해) 상업적 엔티티 서브시스템(400)에 송신될 수 있다. 단계들(626, 627, 및 628)은 호스트 디바이스(100)의 보안 요소(145)로부터 호스트 거래 데이터(678)의 일부로서 생성되고 송신된 임의의 크리덴셜 데이터가 호스트 디바이스(100)의 다른 부분에 의해 복호화될 수 없는 그러한 방식으로 처음에 암호화되도록(예컨대, 프로세서(102)에 의해) 보장할 수 있다. 즉, 호스트 거래 데이터(678)의 호스트 결제 크리덴셜 데이터(675)는 호스트 디바이스(100)의 보안 요소 외부의 임의의 부분에 노출되지 않거나 그에 의해 액세스가능하지 않을 수 있는 크리덴셜 키(155a')를 이용하여 암호화된 호스트 결제 크리덴셜 데이터(676)로서 암호화될 수 있다. 또한, 호스트 거래 데이터(678)의 그러한 암호화된 호스트 결제 크리덴셜 데이터(676)는 액세스 키(예컨대, 액세스 키(155a, 155b, 156k, 151k 및/또는 158k))(예컨대, 본 명세서에서 "액세스 정보"로 지칭됨))를 이용하여 암호화된 호스트 결제 데이터(677)로 암호화될 수 있으며, 이는 호스트 디바이스(100)의 보안 요소 외부의 임의의 부분에 노출되지 않거나 그에 의해 액세스가능할 수 없을 수 있다.

[0088]

다음으로, 단계(630)에서, 프로세스(600)는 호스트 거래 데이터(678)의 적어도 일부분을 수신 및 복호화하는 상업적 엔티티 서브시스템(400)을 포함할 수 있다. 예컨대, 상업적 엔티티 서브시스템(400)은 호스트 거래 데이터(678)를 수신할 수 있고 이어서 상업적 엔티티 서브시스템(400)에 이용가능한 액세스 정보(예컨대, 155a, 155b, 156k, 151k 및/또는 158k)를 사용하여 호스트 거래 데이터(678)의 암호화된 호스트 결제 데이터(677)를 복호화할 수 있다. 이는 상업적 엔티티 서브시스템(400)이(예컨대, 복호화된 호스트 결제 데이터(677)로부터) 판매자의 암호화되지 않은 식별을 결정하는 한편, 호스트 결제 크리덴셜 데이터(675)를 암호화된 상태로(예컨대, 암호화된 호스트 결제 크리덴셜 데이터(676)로서) 또한 유지할 수 있게 하는데, 왜냐하면 상업적 엔티티 서브시스템(400)은 단계(626)에서 호스트 디바이스(100)의 보안 요소(145)가 그러한 호스트 결제 크리덴셜 데이터(675)를 암호화된 호스트 결제 크리덴셜 데이터(676)로서 암호화하는데 이용한 크리덴셜 키(155a')에 대한 액세스를 가질 수 없기 때문이다. 부가적으로 또는 대안적으로, 판매자는 암호화된 호스트 결제 데이터(677)와 함께 호스트 거래 데이터(678)에 포함되었을 수 있는 부가 데이터에 의해 식별될 수 있다. 호스트 거래 데이터(678)는 호스트 디바이스(100) 또는 적어도 그 보안 요소를 식별하는 정보를 포함할 수 있으므로, 호스트 거래 데이터(678)가 상업적 엔티티 서브시스템(400)에 의해 수신될 때, 상업적 엔티티 서브시스템(400)은 단계(630)에서 어떤 액세스 정보(예컨대, 어떤 액세스 정보(155a, 155b, 156k, 151k, 및/또는 158k))를 사용할 지 알 수 있다. 예를 들어, 상업적 엔티티 서브시스템(400)은 다수의 액세스 키(155a/155b) 및/또는 다수의 ISD 키(156k)에 액세스를 가질 수 있으며, 각각의 키는 특정 호스트 디바이스(100) 또는 특정 보안 요소에 특정될 수 있다.

[0089]

다음으로, 단계(631)에서, 프로세스(600)는 상업적 엔티티 서브시스템(400)이, 결제 요청 데이터(666/674)에 의해, 그리고 따라서 호스트 거래 데이터(678)에 의해 식별되었을 수 있는 판매자와 연관된 판매자 키(예컨대, 판매자 키(157'))를 식별하고, 이어서 그 판매자 키를 사용하여 호스트 거래 데이터(678)의 적어도 일부분을 재-암호화하는 단계를 포함할 수 있다. 즉, 단계(630)에서 적합한 액세스 정보를 사용하여 호스트 거래 데이터(678)의 적어도 일부분을 복호화한 후에(예컨대, 암호화된 호스트 결제 데이터(677)를 복호화하여 암호화된 호스트 결제 크리덴셜 데이터(676) 및 암호화된 호스트 결제 데이터(677) 내에 암호화되었을 수 있는 임의의 다른 정보를 구현한 후), 상업적 엔티티 서브시스템(400)은 이어서 단계(631)에서 호스트 거래 데이터(678)의 적어도 일부분을(예컨대, 암호화된 호스트 결제 크리덴셜 데이터(676)의 토큰 데이터 및/또는 암호화 데이터를), 호스트 거래 데이터(678)에서 식별된 판매자 정보와 연관될 수 있는 적합한 판매자 키를 이용하여 재-암호화할 수 있다. 예컨대, 그러한 판매자 키(예컨대, 판매자 키(157'))는 호스트 거래 데이터(678)에서 식별된 상업적 엔티티 판매자 정보를 도 1b의 테이블(430)의 데이터와 비교함으로써 결정될 수 있다. 이와 같이 적절한 판매자 키가 결정되면, 상업적 엔티티 서브시스템(400)은 그 판매자 키(예컨대, 판매자 키(157'))를 이용하여 호스트 거래 데이터(678)의 적어도 일부분을(예컨대, 암호화된 호스트 결제 크리덴셜 데이터(676)의 토큰 데이터 및/또는 암호화 데이터를) 암호화된 판매자 크리덴셜 데이터(681)로서 재-암호화할 수 있다. 예를 들어, 암호화된

판매자 크리덴셜 데이터(681)는 호스트 거래 데이터(678)로부터의 적어도 암호화된 호스트 결제 크리덴셜 데이터(676) 뿐만 아니라 임의의 적합한 거래 데이터, 예컨대, 호스트 거래 데이터(678) 및/또는 결제 요청 데이터(666/674)로부터의 또는 그에 기초한 구매량 데이터 또는 기타 적합한 거래 데이터(예컨대, 잠재 거래 데이터(660/672)에 의해 초기에 식별되었을 수 있는 데이터)를 포함할 수 있다. 호스트 거래 데이터(678)로부터의 판매자 식별 정보는 암호화된 판매자 크리덴셜 데이터(681)에 포함될 필요가 없을 수 있는데, 왜냐하면 그 판매자 식별은 단계(631)에서 판매자 크리덴셜 데이터(681)를 암호화하는데 이용될 수 있는 판매자 키를 결정하기 위해 이미 사용되었을 수 있기 때문이다. 암호화된 판매자 크리덴셜 데이터(681)는 상업적 엔티티 서브시스템(400)에 의해 서명됨으로써, 판매자 서브시스템(200)에 의해 수신될 때, 상업적 엔티티 서브시스템(400)을 그러한 암호화된 판매자 크리덴셜 데이터(681)의 생성자로서 설정할 수 있고/있거나 판매자 서브시스템(200)이 그러한 암호화된 판매자 크리덴셜 데이터(681)가 서명된 후에 수정되지 않도록 보장하게 할 수 있다. 그러한 암호화된 판매자 크리덴셜 데이터(681)는 단계(631)에서 생성되고, 이어서 단계(632)에서 보안 호스트 거래 데이터(682)와 같은 임의의 다른 적합한 데이터와 함께 호스트 디바이스(100)에 송신될 수 있다(예컨대, 상업적 엔티티 서브시스템(400)의 서버(410)로부터도 1b의 경로(65)를 통해 호스트 디바이스(100)의 통신 컴포넌트(106)로 송신됨).

[0090] 단계들(631, 632)은 도 1b의 보안 호스트 거래 데이터(682)의 일부로서 상업적 엔티티 서브시스템(400)으로부터 송신되는 크리덴셜 데이터(예컨대, 암호화된 판매자 크리덴셜 데이터(681)의 토큰 데이터 및/또는 암호화 데이터)가 호스트 디바이스(100)의 보안 요소(145) 이외의 부분에 의해 복호화될 수 없도록 암호화되는 것을 보장하도록 동작될 수 있다. 즉, 보안 호스트 거래 데이터(682)의 크리덴셜 데이터(예컨대, 토큰 데이터 및/또는 암호화된 판매자 크리덴셜 데이터(681)의 암호화 데이터)는 호스트 디바이스(100)의 임의의 부분 - 임의의 부분은 일부 실시예들의 경우 보안 요소(145)를 포함함 - 에 노출되지 않거나 액세스가능하지 않을 수 있는 판매자 키(예컨대, 판매자 키(157'))를 이용하여 암호화될 수 있다. 또한, 보안 호스트 거래 데이터(682)의 크리덴셜 데이터(예컨대, 토큰 데이터 및/또는 암호화된 판매자 크리덴셜 데이터(681)의 암호화 데이터)는 호스트 디바이스(100)의 보안 요소(145) 외부의 임의의 부분에 노출되지 않거나 액세스가능하지 않을 수 있는 크리덴셜 키(155a')를 이용하여 암호화될 수 있다.

[0091] 단계(634)에서, 보안 호스트 거래 데이터(682)는 (예컨대, 통신 경로(99)를 통해 그리고/또는 임의의 적합한 프로토콜(들)을 사용하여 상업적 엔티티 서브시스템(400)을 통해) 보안 호스트 거래 데이터(684)로서 (예컨대, 프로세스(500)의 단계(516)와 관련하여 설명된 바와 같이) 클라이언트 디바이스(100')로 포워드될 수 있다. 이어서 클라이언트 디바이스(100')는 단계(636)에서, (예컨대, 통신 경로(15)를 통해 또는 비접촉식 근접-기반 통신(5)을 통해) 보안 호스트 거래 데이터(684)의 적어도 암호화된 판매자 크리덴셜 데이터(681)를 클라이언트 거래 데이터(686)로서 판매자 서브시스템(200)에게 (예컨대, 프로세스(500)의 단계(518)와 관련하여 설명된 바와 같이) 포워드하도록 동작할 수 있다. 일부 실시예들에서, 단계(634)와 단계(636) 사이에, 클라이언트 디바이스(100')의 GUI는 도 3g의 다른 스크린(190g)을 제공하도록 구성될 수 있으며, 이는 프롬프트(333)를 이용하여 클라이언트 디바이스(100')의 사용자에게 호스트 디바이스(100)로부터 선택 및 인증된 크리덴셜을 (예컨대, 보안 호스트 거래 데이터(682/684)의 암호화된 판매자 크리덴셜 데이터(681) 내에 암호화된 암호화된 호스트 결제 크리덴셜 데이터(676)로서) 사용하여 결제를 검토 및 거부하고/하거나 최종적으로 개시하기 위한 하나 이상의 방식으로 클라이언트 디바이스(100')와 상호작용하라고 촉구할 수 있다. 대안적으로, 단계(636)는 클라이언트 디바이스(100')의 사용자에게 투명하게 발생할 수 있다. 대안적으로, 판매자 크리덴셜 데이터(681)는 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100')를 통해 통신되지 않고 상업적 엔티티 서브시스템(400)으로부터 판매자 서브시스템(200)에게 통신될 수 있다. 잠재 거래 데이터(660/672)의 하나, 일부 또는 전체 부분은 클라이언트 디바이스(100') 및/또는 호스트 디바이스(100) 및/또는 상업적 엔티티 서브시스템(400)을 통해 결제 요청 데이터(666/674)로부터 호스트 거래 데이터(678) 및/또는 보안 호스트 거래 데이터(682) 및/또는 보안 호스트 거래 데이터(684) 및/또는 클라이언트 거래 데이터(686)로 전달될 수 있음에 따라, 잠재 거래의 특정 식별자는 프로세스(600) 동안 이에 제한되지는 않으나, 다음을 포함하는 엔티티 각각에 의해 식별될 수 있다. (i) 특정 판매자 정보, 예컨대, 판매자(즉, "판매자 A")의 고유 판매자 식별자 및/또는 사용 중인 특정 판매자 리소스(예컨대, 특정 판매자 애플리케이션(113'))의 식별, (ii) 특정 거래 정보, 예컨대, 거래를 위해 결제하는 데 사용될 특정 화폐(예컨대, 엔, 파운드, 달러 등)의 식별, 및/또는 거래를 위해 결제될 특정 화폐 금액의 식별(즉, "금액 C" 및/또는 "금액 C*"), 및/또는 구매 또는 임대 또는 그렇지 않으면 지불될 특정 제품 또는 서비스의 식별(즉, "제품 B"), 및/또는 사용될 디폴트 또는 초기 배송 주소의 식별(즉, "배송 D" 및/또는 "배송 E"), (iii) 거래를 위해 판매자에게 수령가능한 하나 이상의 유형의 결제 방법들(예컨대, 구매에 사용될 수 있는 결제 카드들의 리스트(예컨대, 비자를 제외한 마스터 카드)), 또는 클라이언트 디바이스(100')에 의해 선택된 결제 방법

들을 나타내는 정보(즉, "HD1의 PM X"), (iv) 고유 판매자-기반 거래 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행 중인 거래와의 연관을 위해 판매자 서브시스템(200)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열), (v) 고유 클라이언트-기반 거래 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행 중인 거래와의 연관을 위해 클라이언트 디바이스(100')에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열), (vi) 고유 클라이언트-기반 결제 요청 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 결제 요청 데이터(666/674)에 의해 진행 중인 결제 요청과의 연관을 위해 클라이언트 디바이스(100')에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열, 및/또는 (vi) 고유 호스트-기반 결제 요청 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 호스트 디바이스(100)에 의해 지불 중인 결제 요청과의 연관을 위해 호스트 디바이스(100)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 문자의 영숫자 문자열). 그러한 전달된 데이터는 *PKRemotePaymentRequest*의 적어도 일부분을 포함할 수 있으며, 이에 제한되지는 않지만, 다음을 포함하는 임의의 적합한 데이터를 포함할 수 있다. (1) 단계(610) 및/또는 단계(622)의 *PKPaymentRequest*(예컨대, 이는 *PKRemotePaymentRequest* 내에 래핑될 수 있음), (2) 본 명세서에서 *PKRemoteDevice*로 지칭될 수 있는, 선택된 목표 호스트 디바이스를 식별하는 임의의 적합한 데이터(예컨대, 단계(614)의 디스커버리 응답에 포함될 수 있는 바와 같은, 호스트 디바이스(100)의 호스트 디바이스 식별자(119)), (3) 본 명세서에서 *SelectedApplicationIdentifier*로 지칭될 수 있는, 목표 호스트 디바이스의 선택되거나 디폴트인 특정 결제 크리덴셜(예컨대, 단계(614)의 디스커버리 응답에 포함될 수 있고, 클라이언트 디바이스(100')에서 자동으로 또는 사용자 선택될 수 있는, 호스트 디바이스(100)의 보안 요소(145)의 AID(155aa))를 식별하는 임의의 적합한 데이터, 및/또는 (4) 본 명세서에서 *RemotePaymentIdentifier*로 지칭될 수 있는, 결제 요청과 연관된 고유 식별자(예컨대, 클라이언트 및 시스템의 호스트 디바이스를 통해 결제 요청을 식별하는데 사용될 수 있고 클라이언트 디바이스(100) 또는 그 외의 것에 의해 생성될 수 있는 고유 값)를 식별하는 임의의 적합한 데이터. 다른 실시예들에서, 단계(634)에서, 호스트 디바이스(100)는 클라이언트 디바이스(100')를 통하는 대신에 보안 호스트 거래 데이터(684)를 판매자 서브시스템(200)에 직접 통신할 수 있다. 또 다른 실시예들에서, 단계(632)에서, 상업적 엔티티 서브시스템(400)은 호스트 디바이스(100)를 통하는 대신에, 보안 호스트 거래 데이터(682)를 클라이언트 디바이스(100')에 직접 통신할 수 있다. 또 다른 실시예들에서, 단계(621)에서, 상업적 엔티티 서브시스템(400)은 호스트 디바이스(100) 및/또는 클라이언트 디바이스(100')를 통하는 대신에, 보안 호스트 거래 데이터(632)를 판매자 서브시스템(200)에 직접 통신할 수 있다.

[0092]

보안 호스트 결제 크리덴셜 데이터(675/676)를 포함하는 판매자 크리덴셜 데이터(681)가 (예컨대, 단계(636)에서 클라이언트 거래 데이터(686)로서) 판매자 서브시스템(200)에 의해 수신되면, 프로세스(600)는 판매자 서브시스템(200)이 결제 데이터(688)를 생성하여 (예컨대, 도 1b의 판매자 서브시스템(200)과 매입 은행 서브시스템(300) 사이의 통신 경로(25)를 통해) 매입 은행 서브시스템(300)에 송신하도록 구성될 수 있는 단계(638)를 또한 포함할 수 있으며, 데이터(688)는 호스트 디바이스(100)의 보안 호스트 결제 크리덴셜 데이터 및 제품 또는 서비스에 대한 판매자의 구매 가격을 나타낼 수 있는 결제 정보 및 인가 요청을 포함할 수 있다(예컨대, 이는 클라이언트 거래 데이터(686)에 포함되거나 그렇지 않으면 클라이언트 거래 데이터(686)와 연관되거나, 그렇지 않으면 (예컨대, 고유한 거래 식별자에 기초하여)(예컨대, 잠재 거래 데이터(660/672)에 의해) 판매자 서브시스템(200)에 의해 공지된 거래와 연관될 수 있음). 예컨대, 단계(638)에서, 판매자 서브시스템(200)이 클라이언트 거래 데이터(686)의 판매자 크리덴셜 데이터(681)를 적어도 부분적으로 복호화하기 위해 그것의 알려진 판매자 키(157')를 레버리지함으로써, 결제 데이터(688)는 그것의 크리덴셜 키(155a')를 이용하여 암호화된 크리덴셜 SSD(154a)의 보안 호스트 결제 크리덴셜 데이터(예컨대, 암호화된 결제 크리덴셜 데이터(676))를 포함하지만, 금융 기관 서브시스템(350)에 이용가능하지 않은 키를 이용하여 암호화되지 않는다.

[0093]

단계(638)에서, 결제 데이터(688)가 획득 은행 서브시스템(300)에 송신되면, 이어서 단계(640)에서, 매입 은행 서브시스템(300)은 결제 데이터(688)로부터의 인증 요청 정보를 (예컨대, 도 1b의 매입 은행 서브시스템(300)과 금융 기관 서브시스템(350) 사이의 통신 경로(35)를 통해) 인증 요청 데이터(690)로서 금융 기관 서브시스템(350)에 포워드할 수 있다. 다음으로, 단계(642)에서, 금융 기관 서브시스템(350)의 발행 은행 서브시스템(370)이 (예컨대, 단계(640)의 데이터(690)로서 매입 은행 서브시스템(300)으로부터 직접적으로, 또는 데이터(405)로서 결제 네트워크 서브시스템(360)을 통해 간접적으로) 인가 요청을 수신할 때, 결제 정보(예컨대, 호스트 디바이스(100)의 보안 요소(145)에 의해 크리덴셜 키(155a')에 의해 암호화된 호스트 디바이스(100)의 호스트 결제 크리덴셜 데이터(675)(예컨대, 암호화된 호스트 결제 크리덴셜 데이터(676)) 및 구매 금액 - 이들은 각각은 인증 요청 데이터(690) 뿐만 아니라 데이터(684, 686 및/또는 688)에 포함될 수 있음 - 은 (예컨대, 금융 기관 서브시스템(350)에서 크리덴셜 키(155a')를 사용하여) 복호화되고 분석되어 상거래 크리덴셜과 연관된 계정이 구매 금액을 충당하기에 충분한 크레디트를 갖는지 여부를 결정할 수 있다. 충분한 지불금이 존재하지 않으면

면, 발행 은행 서브시스템(370)은 매입 은행 서브시스템(300)에 부정적인 인가 응답을 송신함으로써 요청된 거래를 거절할 수 있다. 그러나, 충분한 지불금이 존재하는 경우, 발행 은행 서브시스템(370)은 매입 은행 서브시스템(300)에 긍정적인 인증 응답을 송신함으로써 요청된 거래를 승인할 수 있고, 금융 거래가 완료될 수 있다. 어느 한 유형의 인증 응답은 프로세스(600)의 단계(642)에서, 사용자 금융 서브시스템(350)에 의해 인증 응답 거래 상태 데이터(692)로서 (예컨대, 발행 은행 서브시스템(370)으로부터 통신 경로(35)를 통해 매입 은행 서브시스템(300)으로 직접 또는 도 1b의 통신 경로(45)를 통해 발행 은행 서브시스템(370)으로부터 결제 네트워크 서브시스템(360)에 제공될 수 있는 인증 응답 데이터(415)에 기초하여 결제 네트워크 서브시스템(360)으로부터 매입 은행 서브시스템(300)으로 직접) 매입 은행 서브시스템(300)에 제공될 수 있다. 다음으로, 단계(642)에서, 인증 응답 거래 상태 데이터(692)를 수신하는 것에 응답하여, 프로세스(600)는 또한 단계(644)에서, 매입 은행 서브시스템(300) 또는 임의의 다른 적합한 서브시스템이 그러한 인증 응답 거래 상태 데이터를 인증 응답 거래 상태 데이터(694)로서 판매자 서브시스템(200)과 공유하는 단계를 포함할 수 있으며, 이는 이어서, 단계(646)에서, (예컨대, 프로세스(500)의 단계(522)와 관련하여 설명된 바와 같이) (예컨대, 판매자 리소스 또는 다른 리소스를 사용하여) 확인된 거래 상태 데이터(696)로서 클라이언트 디바이스(100')와 공유될 수 있고/있거나, 단계(648)에서, (예컨대, 프로세스(500)의 단계(524)와 관련하여 설명된 바와 같이) 확인된 거래 상태 데이터(698)로서 호스트 디바이스(100)와 공유될 수 있다. 그러한 확인된 거래 상태 데이터는 도 3h의 스크린(190h)의 확인 데이터(335)와 같은 임의의 적합한 확인 데이터를 디바이스(100 및/또는 100')에 제공하도록 구성될 수 있다. 거래가 성공적이면, 확인된 거래 상태 데이터는 단계(646)에서 클라이언트 디바이스(100') 및/또는 단계(648)에서 호스트 디바이스(100)에서 거래(예컨대, 결제 요청 데이터의 고유 *RemotePaymentIdentifier*에 의해 식별된 거래)를 종료하도록 동작할 수 있다. 부가적으로 또는 대안적으로, 거래가 성공적이지 않은 경우, 확인된 거래 상태 데이터는 거래를 종료하도록 동작할 수 있거나 동작하지 않을 수 있다(예컨대, 유효한 지불금이 이용가능하지 않거나 호스트 디바이스가 허위로 식별되면 거래를 종료하지만, 유효하지 않은 배송 주소로 결정되면 오픈하고 업데이트를 허용함). 임의의 비-거래-종결 거래 상태 데이터는 프로세스가 애플리케이션에 의해 취소되거나, 프로세스가 사용자에게 의해 취소되거나, 또는 프로세스가 완료될 때까지 결제 프로세스를 계속되도록 허용할 수 있다.

[0094]

따라서, 판매자 서브시스템(200)은 임의의 적합한 방식으로 클라이언트 거래 데이터(686) 또는 판매자 크리덴셜 데이터(681)의 임의의 다른 캐리어를 프로세싱하도록 구성될 수 있다. 예를 들어, 판매자 크리덴셜 데이터(681)로부터 호스트 결제 크리덴셜 데이터를 획득하기 위해, 판매자 서브시스템(200)은 수신된 판매자 크리덴셜 데이터(681)의 서명 특성이 유효하고 상업적 엔티티 서브시스템(400)이 그 서명의 서명자인 것을 검증할 수 있다. 판매자 서브시스템(200)은 상업적 엔티티 서브시스템(400)에 의해 어떤 판매자 키(예컨대, 어떤 판매자 공개 키(157'))가 판매자 크리덴셜 데이터(681)를 구성하는 데 사용될 수 있었는지를 결정하기 위해 임의의 적합한 기술을 사용할 수 있다. 이어서, 판매자 서브시스템(200)은 대응되는 판매자 개인 키(예컨대, 판매자 서브시스템(200)에서의 판매자 개인 키(157'))를 검색하고, 그 검색된 키를 사용하여 암호화된 판매자 크리덴셜 데이터(681)를 비-캡슐화(de-encapsulate) 및/또는 복호화하여 암호화된 호스트 결제 크리덴셜 데이터(676)를 복구할 수 있다. 이어서, 그러한 데이터(676)는 적절한 결제 네트워크(360)에 제공될 수 있으며, 적절한 결제 네트워크(360)는 금융 기관 서브시스템(350)의 적절한 크리덴셜 키(155a')를 레버리지하여 암호화된 호스트 결제 크리덴셜 데이터(676)를 비-캡슐화 및/또는 복호화하여 호스트 결제 크리덴셜 데이터(675)를 복구할 수 있다(예컨대, 호스트 결제 크리덴셜 데이터(675)를 검증하기 위해 호스트 결제 크리덴셜 데이터(675)의 토큰 데이터 및/또는 암호화 데이터를 복구함(예컨대, 수신된 호스트 결제 크리덴셜 데이터(675)의 토큰 데이터에 기초하여 암호화 데이터를 독립적으로 생성하고, 생성된 암호화 데이터를 수신된 호스트 결제 크리덴셜 데이터(675)의 암호화 데이터와 비교하여, 비교에 기초하여 거래를 검증하거나 거절하기 위함)).

[0095]

도 6의 프로세스(600)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 부가적인 단계들이 추가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다. 일부 실시예들에서, (예컨대, 잠재 거래 데이터(660) 또는 잠재 거래 데이터(672)에 의해 식별되는) 잠재 거래는 2개의 상이한 결제 크리덴셜에 의해 적어도 부분적으로 지불될 수 있다. 예를 들어, 클라이언트 디바이스(100')는 제 1 호스트 거래 데이터(예컨대, 제1 호스트 거래 데이터(684)) - 이는 거래의 제1 부분을 지불하도록 동작할 수 있음 - 의 생성을 개시하기 위해 제1 호스트 디바이스에 제1 결제 요청(예컨대, 제1 결제 요청 데이터(666))을 생성 및 송신할 뿐만 아니라, 제2 호스트 거래 데이터(예컨대, 제2 호스트 거래 데이터(684)) - 이는 거래의 제2 부분을 지불하도록 동작할 수 있음 - 의 생성을 개시하기 위해 제2 호스트 디바이스에 제2 결제 요청(예컨대, 제2 결제 요청 데이터(666))을 생성 및 송신하도록 동작할 수 있으며, 호스트 거래 데이터의 각각의 인스턴스는 거래를 지불하기 위해 클라이언트 디바이스(100')에 의해 공유될 수 있다. 대안적으로, 거래의 제2 부분은 클

라이언트 디바이스(100')에 네이티브한 크리덴셜 데이터에 의해 지불될 수 있다. 도시되지는 않았지만, 보안 호스트 거래 데이터는 상업적 엔티티 서브시스템(400)으로부터 직접(예컨대, 호스트 디바이스(100)를 통하지 않고 통신 경로(95)를 통해) 클라이언트 디바이스(100')로 또는 직접(예컨대, 호스트 디바이스(100)를 통하지 않고/않거나 클라이언트 디바이스(100')를 통하지 않고 통신 경로(85)를 통해) 판매자 서브시스템(200)으로 또는 직접(예컨대, 호스트 디바이스(100)를 통하지 않고/않거나 클라이언트 디바이스(100')를 통하지 않고 및/또는 판매자 서브시스템(200)을 통하지 않고 통신 경로(55)를 통해) 금융 기관 서브시스템(350)으로 통신될 수 있다. 부가적으로 또는 대안적으로, 도시되지는 않았지만, 보안 호스트 거래 데이터는 호스트 디바이스(100)로부터 판매자 서브시스템(200)으로 직접(예컨대, 클라이언트 디바이스(100')를 통하지 않고) 또는 금융 기관 서브시스템(350)으로 직접(예컨대, 클라이언트 디바이스(100')를 통하지 않고/않거나 판매자 서브시스템(200)을 통하지 않고 통신 경로(75)를 통해) 통신될 수 있다. 부가적으로 또는 대안적으로, 비록 도시되지는 않았지만, 클라이언트 거래 데이터는 클라이언트 디바이스(100')로부터 금융 기관 서브시스템(350)으로 직접(예컨대, 판매자 서브시스템(200)을 통하지 않고) 통신될 수 있다. 언급한 바와 같이, 클라이언트 디바이스(100')는 특정 제품에 대한 적어도 하나의 특정 판매자로부터 연관된 잠재 거래 데이터를 클라이언트 디바이스(100')의 사용자에게 의해 임의의 활성 상호작용없이 모두 자동으로 획득하기 위해, 특정 제품을 구매해야 한다고 결정하고 하나 이상의 판매자와 상호작용하도록 구성될 수 있다(예컨대, 클라이언트 디바이스(100')는 어플라이언스 제품이 구매되어야 한다고 결정하도록 구성(예컨대, 세탁기에 의해 더 많은 세탁 세제가 필요하다는 것을 검출하거나, 특정 일자에 더 많은 세제를 구매하는 데 사용자에게 의해 사전 설정된 달력 이벤트를 검출 함)될 수 있는 가전 제품일 수 있고, 그 제품에 대해 최상의 거래를 제공하는 특정 판매자를 자동으로 식별할 수 있고, 해당 판매자로부터 해당 제품을 구매하기 위해 해당 판매자와 자동으로 상호작용하여 잠재 거래 데이터를 획득할 수 있음). 그 후, 클라이언트 디바이스(100')는 결제 요청(예컨대, 결제 요청 데이터(666))을 하나 이상의 특정 목표 호스트 디바이스에 자동으로 생성하고 푸시하도록 동작할 수 있다. 예를 들어, 그러한 클라이언트 디바이스(100')는 (예컨대, 애플 인크.의 홈킷™(HomeKit™)와 같은 가정 자동화 플랫폼을 사용하여) 생태계 내의 하나 이상의 호스트 디바이스(100)와 페어링될 수 있는 자동화된 장치일 수 있으며, 그러한 결제 요청은 적어도 부분적으로 미리 기입되거나 그렇지 않으면 임의의 적합한 미리 정의된 설정에 따라 기입될 수 있다(예컨대, 호스트 디바이스(X)로부터 새로운 세탁 세제에 대한 결제를 요청하고 호스트 디바이스(Y)로부터 새로운 건조기 시트에 대한 결제를 요청하거나, 호스트 디바이스(X)로부터 \$G 초과, 호스트 디바이스(Y)로부터 \$G 미만의 임의의 구매에 대한 결제를 요청하는 등).

[0096] 프로세스(600)의 호스트 디바이스(100)와 클라이언트 디바이스(100') 사이의 하나, 일부 또는 각각의 데이터 통신(예컨대, 데이터(662, 664, 666, 668, 674, 684 및/또는 698) 중 하나, 일부 또는 각각의 통신)은 피어-투-피어 배열로 직접적으로 또는 상업적 엔티티 서브시스템(400) 또는 임의의 다른 적합한 엔티티를 통하는 것과 같은, 임의의 적합한 통신 프로토콜(들)을 사용하는 임의의 적합한 통신 경로(들)를 통하거나 임의의 적합한 방식으로 암호화되거나 전혀 암호화되지 않을 수 있는 임의의 적합한 전송 메커니즘을 이용하여 이루어질 수 있다. 그러한 데이터 통신은 임의의 적합한 온라인 메시징, 인스턴트 메시징, 이메일 메시징, 텍스트 메시징, 임의의 적합한 근접-기반 메시징, NFC, Bluetooth™ 및/또는 기타를 통해 이루어질 수 있으며, 전화 번호, 이메일 주소, 고유 디바이스 식별자, 위치 기반 비콘 등과 같은 임의의 적합한 디바이스 어드레싱 방식을 이용하여 인에이블될 수 있다. 각각의 호스트 디바이스 및 각각의 클라이언트 디바이스는 랩탑, 셀룰러 전화, 가전 제품, 판매자 액세스리 디바이스(예컨대, 가솔린 판매자에 의해 가스 펌프에 제공되는 디바이스), 사용자 액세스리(예컨대, 스마트 시계와 같은 착용형 디바이스) 등과 같은 사용자에게 대한 임의의 적합한 UI 및 I/O 능력을 갖는 임의의 적합한 디바이스일 수 있다. 네이티브 결제 크리덴셜을 갖는 임의의 호스트 디바이스가 자체적으로 네이티브 결제 크리덴셜 갖거나 갖지 않을 수 있는 임의의 다른 적합한 디바이스(예컨대, 그 자신의 네이티브 결제 크리덴셜을 사용하거나 사용하지 않는 클라이언트 디바이스)로부터의 결제 요청을 (예컨대, 공용 인터넷을 통하거나 임의의 다른 적합한 방식을 통해) 수신하고 이에 응답할 수 있게 함으로써, 시스템(1)과 프로세스(600)는 많은 보안 및 효과적인 사용 사례 및 사용자 경험을 가능하게 할 수 있다.

[0097] 예를 들어, 사용자는 클라이언트 디바이스(100')(예컨대, 보안 요소 또는 임의의 네이티브 결제 크리덴셜을 가지지 않을 수 있는 랩톱 컴퓨터) 상의 판매자 서브시스템(200)의 온라인 판매자 리소스(예컨대, 애플리케이션(113'))를 사용하여 온라인 쇼핑하고, 구매할 특정 제품(예컨대, "제품 B")을 식별하기 위해 온라인 리소스와 상호작용한다. 해당 제품의 식별에 응답하여(예컨대, 사용자가 "보안 크리덴셜 결제"(예컨대, 애플 인크.의 애플페이™)를 이용하여 구매"를 선택하는 것에 응답하여), 온라인 리소스는 클라이언트 디바이스(100') 상에 사용자가 특정 배송 주소 또는 다른 가변 데이터를 입력할 수 있게 할 수 있는 결제 시트나 임의의 적합한 UI를 제시하도록 동작할 수 있다(예컨대, 스크린(190a)에 의해 도시된 바와 같이, 그리고 다른 정보를 업데이트 할

있는 단계들(620 및 622)의 하나 이상의 반복을 통해 클라이언트 디바이스(100')의 사용자에게 의해 업데이트될 수 있음(예컨대, 클라이언트 디바이스(100')의 사용자가 정보(307d)의 배송 주소를 변경하는 것에 응답하여, 정보(307c)의 가격이 업데이트될 수 있음)). 어떤 시점에서, 클라이언트 디바이스(100')의 사용자는 스크린(190a)의 "보안 결제" 옵션(309)을 선택할 수 있는데, 이에 따라 디스커버리 프로세스(예컨대, 단계(662 및 664)가 자동적으로(예컨대, 클라이언트 디바이스(100')의 사용자의 임의의 추가의 상호작용 없이), 클라이언트 디바이스(100')는 (예컨대, 잠재 거래 데이터(660)에 의해 표시된 수령가능한 결제 옵션에 기초하여), 스크린(190a)의 결제 시트의 구매 지불에 적합한 네이티브 결제 크리덴셜들을 가지고 있지 않다는 것과, "HD1"의 PM X"(즉, 호스트 디바이스(1)의 결제 방법(X))이 유일하게 사용에 적합한 이용가능하거나 선호되는 비-네이티브 결제 크리덴셜인 것을 식별할 수 있다(예컨대, 선호도는 클라이언트 디바이스에 대한 각각의 이용가능한 호스트 디바이스의 근접성 또는 디스커버리 프로세스를 통해 클라이언트 디바이스(100')에 액세스가능할 수 있는 임의의 다른 적합한 특성들에 기초하여 자동적으로 결정될 수 있음). 그러한 식별 후에, 클라이언트 디바이스(100')는 그 호스트 디바이스에 적절한 결제 요청을 전송하기 위해 사용자가 도 3c의 옵션(315)을 선택할 수 있게 하기 위해 도 3c의 스크린(190c)을 클라이언트 디바이스(100')의 사용자에게 자동적으로 제시하도록 동작할 수 있거나, 또는, 프로세스(600)는 사용자를 대신하여(예컨대, 디스커버리 프로세스의 식별에 응답하여 이용가능한 목표 호스트 디바이스(1)(즉, 그 호스트 디바이스(100))에 적절한 결제 요청 데이터(666/674)를 자동적으로 전송함으로써) 그 선택을 자동적으로 수행할 수 있으며, 이는 호스트 디바이스(100)에 의해 도 3d의 스크린(190d) 또는 도 3e의 스크린(190e)이 자동적으로 제시되게 할 수 있다(예컨대, 클라이언트 디바이스(100') 상에 제시된 결제 시트와 유사할 수 있는 호스트 디바이스(100) 상의 결제 시트를 제시함). 호스트 디바이스(100)는 클라이언트 디바이스(100')에 의해 개시된 거래를 지불하기에 적합한 적어도 하나의 네이티브 결제 크리덴셜을 갖는 보안 요소를 포함할 수 있는 이동 전화 또는 임의의 다른 디바이스일 수 있다. 클라이언트 디바이스(100')의 사용자는 클라이언트 디바이스(100') 뿐만 아니라 호스트 디바이스(100)에도 근접할 수 있으며, (예컨대, 도 3f의 스크린(190f)의 인증 옵션(331)을 선택함으로써) 클라이언트 디바이스(100') 및 판매자 서브시스템(200)에 의해 개시되거나 다른 방식으로 수행되는 거래를 지불하기 위해, 호스트 디바이스(100)에 네이티브한 특정 결제 크리덴셜의 사용을 인증하기 위해 호스트 디바이스(100)의 스크린들(190d 내지 190f) 중 하나의 GUI와 상호작용할 수 있을 것이다. 호스트 디바이스(100)에 대한 그러한 인증에 응답하여, 호스트 디바이스(100)에 네이티브한 크리덴셜에 대한 호스트 결제 크리덴셜 데이터가 거래를 지불하려고 시도하기 위해 금융 기관 서브시스템(350)에 제공될 수 있고 (예컨대, 프로세스(600)의 단계들(625 내지 640)), 이어서, 거래의 확인 상태가 클라이언트 디바이스(100') 및/또는 호스트 디바이스(100)에서의 사용자와 공유될 수 있다 (예컨대, 도 3h의 스크린(190h)에 의해). 대안적인 실시예에서, 다수의 호스트 디바이스가 이용가능한 것으로 식별될 수 있고, 결제 요청은 클라이언트 디바이스(100')로부터 이용가능한 호스트 디바이스들 각각에 전송될 수 있어, 호스트 결제 크리덴셜 데이터를 이용하여 응답하는 첫 번째 호스트 디바이스가 거래를 지불할 수 있거나, 각각의 호스트 디바이스가 호스트 결제 크리덴셜 데이터를 이용하여 응답하여 거래의 특정 부분을 지불할 수 있다.

[0098]

다른 예로서, 홈 자동화 플랫폼(예컨대, 애플 인크.의 홈킷™)을 사용하여 통신 네트워크에 통신 가능하게 연결될 수 있는 사용자의 가전기기 클라이언트 디바이스(100')(예컨대, 세탁기)는 그것이 적절하게 동작하는데 필요한 리소스가 거의 없음을 결정하도록 동작할 수 있다(예컨대, 세탁기 클라이언트 디바이스(100')는 세탁 세제의 보유량이 20% 용량인 것을 자동적으로 결정하도록 동작할 수 있음). 그러한 결정에 응답하여, 가전기기 클라이언트 디바이스(100')는 그 리소스를 더 많이 구매할 기회를 자동적으로 식별하도록 동작할 수 있다(예컨대, 가전기기 클라이언트 디바이스(100')는 최적의 가격 또는 다른 적합한 측정치로 구매하기 위해 필요한 세탁 세제를 식별하기 위해 하나 이상의 온라인 리소스를 통해 하나 이상의 판매자 서브시스템과 상호작용할 수 있도록 동작될 수 있음). 따라서, 그러한 구매 기회에 대한 잠재 거래 데이터(660/672)가 클라이언트 디바이스(100')에 의해 획득될 수 있고, 클라이언트 디바이스(100')는 (예컨대, 단계(662/664)의 디스커버리 프로세스를 통해) 그 거래를 지불하기 위해 이용가능할 수 있는 적어도 하나의 호스트 디바이스를 자동적으로 디스커버리하도록 동작할 수 있고, 적절한 결제 요청 데이터(666/674)를 적어도 하나의 디스커버리된 호스트 디바이스들 - 예컨대, 가전기기 클라이언트 디바이스(100')를 포함하는 가정 자동화 플랫폼 에코시스템과 연관된 적어도 하나의 사용자의 호스트 디바이스 - 의 각각과 자동적으로 공유할 수 있다. 호스트 디바이스(100)는 그러한 결제 요청 데이터를 수신할 수 있고, 가전기기 클라이언트 디바이스(100')에 의해 식별된 거래를 지불하는데 사용하기 위해 그 호스트 디바이스에 네이티브한 결제 크리덴셜을 선택하고 인증할 수 있는 능력을 호스트 디바이스(100)의 사용자에게 제시할 수 있다(예컨대, 클라이언트 디바이스(100')에서 임의의 활성 사용자 상호작용없이 식별됨). 이는 가전기기 클라이언트 디바이스(100')에 대한 임의의 적합한 위치에 있는 사용자 및 호스트 디바이스(100)가 가전기기 클라이언트 디바이스(100')로부터 고유 결제 요청을 수신하고 고유 결제 요청과 연관된 거래를 지불하는

데 사용하기 위해 호스트 디바이스에 네이티브한 결제 크리덴셜에 대한 호스트 거래 데이터를 가전기기 클라이언트 디바이스(100')에 제공할 수 있게 한다(예컨대, 호스트 디바이스(100) 및 그 사용자는 가전기기 클라이언트 디바이스(100')로부터 국내의 다른 쪽에 위치될 수 있지만, (예컨대, 임의의 적합한 인터넷 통신 경로(들) 또는 임의의 다른 적합한 통신 경로(들)를 통해) 여전히 가전기기 클라이언트 디바이스(100')로부터 결제 요청을 수신하고 호스트 결제 크리덴셜 데이터를 이용하여 응답할 수 있음). 대안적으로, 가전기기 클라이언트 디바이스(100')는 인터넷을 통해 먼 거리에 걸쳐 통신하는 대신에, 클라이언트 디바이스(100')의 디스플레이 상에 근접 호스트 디바이스(100)의 센서에 의해 스캐닝되고 특정 결제 요청 데이터를 식별하도록 프로세싱될 수 있는 QR 코드를 제시할 수 있거나, 클라이언트 디바이스(100') 및 호스트 디바이스(100)는 블루투스™ 또는 임의의 다른 적합한 로컬 통신 프로토콜을 통해 통신할 수 있다.

[0099] 일부 실시예들에서, 프로세스(500 및/또는 600) 및/또는 본 개시의 임의의 다른 프로세스의 적어도 일부분은 호스트 디바이스(100)의 사용자와 클라이언트 디바이스(100')의 사용자 사이에 대금을 송금하도록 동작할 수 있다(예컨대, 클라이언트 디바이스(100')는 클라이언트 디바이스(100')와 판매자 서브시스템 사이의 임의의 거래와 독립적으로 호스트 디바이스(100)로부터 지불금을 요청할 수 있음). 일부 실시예들에서, 이는 매입 은행 및/또는 금융 기관 서브시스템(350)의 하나 이상의 엔티티에 의해 인에이블되어, 임의의 판매자 서브시스템에 대한 필요 없이, 호스트 거래 데이터가 호스트 디바이스 상의 크리덴셜과 연관된 계정과 클라이언트 디바이스의 사용자와 연관된 계정 사이에서 지불금의 송금을 용이하게 하도록 인에이블될 수 있다. 대안적으로, 호스트 디바이스 상의 선불 카드 및/또는 클라이언트 디바이스 상의 선불 카드는 호스트와 클라이언트 사이에 지불금을 전송하기 위해 레버리지될 수 있다(예컨대, 호스트 디바이스에 네이티브인 선불 크리덴셜(예컨대, 호스트 디바이스(100)의 보안 요소(145) 상의 크리덴셜)로부터, 클라이언트 디바이스에 네이티브인 선불 크리덴셜(예컨대, 클라이언트 디바이스(100')의 보안 요소 상의 크리덴셜)로 지불금을 전송하는 것). 예컨대, 클라이언트 디바이스(100')는 호스트 디바이스(100)가 호스트 디바이스(100) 상의 선불 크리덴셜로부터 화폐 금액을 차감하고 클라이언트 디바이스(100')의 선불 크리덴셜에 적절한 화폐 금액을 부가하도록 동작할 수 있는 클라이언트 디바이스(100)에 임의의 적절한 APDU 명령을 전송하도록 요청하도록 동작할 수 있는 호스트 디바이스(100)에 결제 요청을 통신할 수 있다(예컨대, 따라서 클라이언트 디바이스(100')와 공유되는 호스트 거래 데이터는 그러한 APDU 명령을 포함할 수 있고/있거나 실제 암호화 화폐를 포함할 수 있음).

[0100] 클라이언트 디바이스(100')가 판매자에 특정된 클라이언트 디바이스(100') 상의 네이티브 애플리케이션을 통해 판매자 서브시스템(200)과 통신하는 경우, 판매자 애플리케이션(113c)은 그러한 애플리케이션에 의해 제공될 수 있다. 그러나, 클라이언트 디바이스(100')가, 판매자에 특정된 것이 아니라 (예컨대, 판매자 제어 하의 서버 상의) 판매자에 의해 관리되는 웹사이트를 가리킬 수 있는 인터넷 브라우저를 통해 판매자 서브시스템(200)과 통신 중인 경우, 판매자 애플리케이션(113c)은 (예컨대, 통신 컴포넌트(106)를 통해) 판매자의 웹사이트로 통신을 포워드할 수 있는 레이아웃 엔진 소프트웨어 컴포넌트(예컨대, 웹킷(WebKit))일 수 있다. 예를 들어, 클라이언트 디바이스(100')의 그러한 애플리케이션(113c)은 판매자 서브시스템(200)에 제공될 임의의 호스트 거래 데이터에 대한 도판이 될 수 있다. 대안적으로, 그러한 호스트 거래 데이터는 클라이언트 디바이스(100')를 통하는 대신에, (예컨대, 잠재 거래 데이터 및 클라이언트 디바이스 결제 요청 데이터에서 판매자에 의해 제공된 판매자 식별자 또는 주소를 사용하여) 호스트 디바이스(100) 또는 상업적 엔티티 서브시스템(400)으로부터 직접적으로 판매자 서브시스템(200)에 통신될 수 있다.

[0101] 도 7의 설명

[0102] 도 7은 상업적 엔티티 서브시스템, 클라이언트 전자 디바이스, 및 호스트 전자 디바이스 - 호스트 전자 디바이스는 보안 요소 및 보안 요소 상에 프로비저닝된 호스트 크리덴셜 애플리케이션을 포함함 - 를 사용하여 판매자 서브시스템과의 금융 거래를 수행하기 위한 예시적인 프로세스(700)의 흐름도이다. 프로세스(700)의 단계(702)에서, 호스트 전자 디바이스는 판매자 서브시스템을 식별하는 판매자 서브시스템 식별자 정보 및 호스트 크리덴셜 애플리케이션을 식별하는 호스트 크리덴셜 애플리케이션 식별자 정보를 포함하는 결제 요청 데이터를 클라이언트 전자 디바이스로부터 수신할 수 있다. 예를 들어, 호스트 전자 디바이스(100)는 판매자 서브시스템(200)의 식별자 및 호스트 전자 디바이스(100)의 크리덴셜 결제 애플릿(153a)의 식별자를 포함할 수 있는 결제 요청 데이터(662)를 수신할 수 있다. 프로세스(700)의 단계(704)에서, 호스트 전자 디바이스는 수신된 결제 요청 데이터에 의해 식별된 호스트 크리덴셜 애플리케이션을 사용하여 보안 요소 상에, 호스트 결제 크리덴셜 데이터를 포함하는 제1 데이터를 생성할 수 있다. 예를 들어, 결제 요청 데이터(666)에 의해 식별된 크리덴셜 결제 애플릿(153a)은 호스트 결제 크리덴셜 데이터(675)를 생성할 수 있다. 프로세스(700)의 단계(706)에서, 호스트 전자 디바이스는 호스트 전자 디바이스의 보안 요소 상에, 제1 데이터 및 수신된 결제 요청 데이터의 판매

자 서브시스템 식별자 정보를 제1 키를 이용하여 암호화함으로써 제2 데이터를 생성할 수 있다. 예를 들어, 호스트 전자 디바이스(100)는 호스트 결제 데이터(677)로서 액세스 키를 이용하여 판매자 서브시스템(200)의 식별자를 포함하는 결제 요청 데이터 및 호스트 결제 크리덴셜 데이터(675)를 암호화할 수 있다. 프로세스(700)의 단계(708)에서, 호스트 전자 디바이스는 호스트 전자 디바이스로부터 상업적 엔티티 서브시스템으로 제2 데이터를 송신할 수 있다. 예를 들어, 호스트 전자 디바이스(100)는 호스트 결제 데이터(678)를 상업적 엔티티 서브시스템(400)에 송신할 수 있다. 프로세스(700)의 단계(710)에서, 호스트 전자 디바이스는 판매자 서브시스템 식별자 정보와 연관된 제2 키를 이용하여, 암호화된 제1 데이터를 포함하는 제3 데이터를 수신할 수 있다. 예를 들어, 호스트 전자 디바이스(100)는 판매자 서브시스템(200)과 연관된 판매자 키를 이용하여, 암호화된 호스트 결제 크리덴셜 데이터(675/676)를 포함할 수 있는 보안 호스트 거래(682)를 수신할 수 있다. 프로세스(700)의 단계(712)에서, 호스트 전자 디바이스는 수신된 제3 데이터를 송신하여 금융 거래의 적어도 일부를 지불할 수 있다. 예를 들어, 호스트 전자 디바이스(100)는 (예컨대, 판매자 서브시스템(200)에 대한) 금융 거래의 적어도 일부를 지불하기 위해 보안 호스트 거래 데이터(684)를 송신할 수 있다.

[0103] 도 7의 프로세스(700)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 부가적인 단계들이 추가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다.

[0104] 도 8의 설명

[0105] 도 8은 클라이언트 전자 디바이스 및 호스트 전자 디바이스를 사용하여 판매자 서브시스템과의 금융 거래를 수행하기 위한 예시적인 프로세스(800)의 흐름도이다. 프로세스(800)의 단계(802)에서, 클라이언트 전자 디바이스는 판매자 서브시스템으로부터 금융 거래를 나타내는 잠재 거래 데이터를 수신할 수 있다. 예를 들어, 클라이언트 전자 디바이스(100')는 판매자 서브시스템(200)으로부터 금융 거래를 나타내는 잠재 거래 데이터(660)를 수신할 수 있다. 프로세스(800)의 단계(804)에서, 클라이언트 전자 디바이스는 클라이언트 전자 디바이스로부터 호스트 전자 디바이스로, 수신된 잠재 거래 데이터에 기초하여 결제 요청 데이터를 송신할 수 있다. 예를 들어, 클라이언트 전자 디바이스(100')는 잠재 거래 데이터(660/672)에 기초하여, 결제 요청 데이터(666/674)를 호스트 전자 디바이스(100)에 송신할 수 있다. 프로세스(800)의 단계(806)에서, 클라이언트 전자 디바이스는, 클라이언트 전자 디바이스에서, 송신된 결제 요청 데이터에 기초하여, 호스트 전자 디바이스에 의해 생성된 호스트 결제 크리덴셜 데이터를 포함하는 호스트 거래 데이터를 수신할 수 있다. 예를 들어, 호스트 전자 디바이스(100)에 의해 생성된 호스트 결제 크리덴셜 데이터(675)를 포함하는 보안 호스트 거래 데이터(684)는 클라이언트 전자 디바이스(100')에 의해 수신될 수 있다. 프로세스(800)의 단계(808)에서, 클라이언트 전자 디바이스는 클라이언트 전자 디바이스로부터 판매자 서브시스템으로, 수신된 호스트 거래 데이터의 호스트 결제 크리덴셜 데이터를 송신하여 금융 거래의 적어도 일부를 지불할 수 있다. 예를 들어, 클라이언트 전자 디바이스(100')는 (예컨대, 판매자 서브시스템(200)에 대한) 금융 거래의 적어도 일부를 지불하기 위해 판매자 서브시스템(200)에 호스트 결제 크리덴셜 데이터(675)를 포함하는 클라이언트 거래 데이터(686)를 송신할 수 있다.

[0106] 도 8의 프로세스(800)에 도시된 단계들은 단지 예시적인 것이며, 존재하는 단계들은 수정되거나 생략될 수 있고, 부가적인 단계들이 추가될 수 있고, 특정 단계들의 순서가 변경될 수 있다.

[0107] 도 9의 설명

[0108] 도 9는 상업적 엔티티 서브시스템, 클라이언트 전자 디바이스, 및 호스트 전자 디바이스 - 호스트 전자 디바이스는 보안 요소 및 보안 요소 상에 프로비저닝된 호스트 크리덴셜 애플리케이션을 포함함 - 를 사용하여 판매자 서브시스템과의 금융 거래를 수행하기 위한 예시적인 프로세스(900)의 흐름도이다. 프로세스(900)의 단계(902)에서, 상업적 엔티티 서브시스템은 금융 거래를 지불하기 위해 판매자 서브시스템에 수령가능한 적어도 하나의 결제 유형을 식별하는 호스트 이용가능성 요청을 클라이언트 전자 디바이스로부터 수신할 수 있다. 예를 들어, 상업적 엔티티 서브시스템(400)은 (예컨대, 잠재 거래 데이터(660)에 기초하여) 금융 거래를 지불하기 위해 판매자 서브시스템(200)에 수령가능한 적어도 하나의 결제 유형을 식별하는 클라이언트 디바이스(100')로부터 호스트 이용가능성 요청 데이터(662)를 수신할 수 있다. 프로세스(900)의 단계(904)에서, 상업적 엔티티 서브시스템은, 상업적 엔티티 서브시스템에서, 호스트 전자 디바이스가 클라이언트 전자 디바이스와 연관되는지를 결정할 수 있다. 예컨대, 상업적 엔티티 서브시스템(400)은 호스트 전자 디바이스(100)가 클라이언트 전자 디바이스(100')와 연관되는지(예컨대, 두 디바이스가 상업적 엔티티 서브시스템의 동일한 특정 사용자 계정과 연관되는지) 결정하도록 동작할 수 있다. 프로세스(900)의 단계(906)에서, 상업적 엔티티 서브시스템은 호스트 전자 디바이스가 클라이언트 전자 디바이스와 연관된다는 결정에 기초하여, 호스트 전자 디바이스의 보안 요소 상에 프로비저닝된 호스트 크리덴셜 애플리케이션이 수신된 호스트 이용가능성 요청의 식별된 적어도 하나의 결

제 유형을 만족시킨다고 결정할 수 있다. 예컨대, 상업적 엔티티 서브시스템(400)은 결제 크리덴셜 애플릿(153a)이 판매자 서브시스템(200)에 수령가능한 결제 방법(예컨대, 비자 신용 카드)과 연관될 수 있는지를 결정하도록 동작할 수 있다. 프로세스(900)의 단계(908)에서, 상업적 엔티티 서브시스템은 호스트 크리덴셜 애플리케이션이 식별된 적어도 하나의 결제 유형을 만족시킨다는 결정에 기초하여, 상업적 엔티티 서브시스템으로부터 클라이언트 전자 디바이스로, 호스트 전자 디바이스를 식별하는 호스트 이용가능성 응답을 송신할 수 있다. 예를 들어, 상업적 엔티티 서브시스템(400)은 호스트 전자 디바이스(100)를 (예컨대, 이용가능한 비-네이티브 결제 소스로서) 식별할 수 있는 클라이언트 전자 디바이스(100')에 호스트 이용가능성 응답 데이터(664)를 송신하도록 동작할 수 있다.

[0109] 도 9의 프로세스(900)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 부가적인 단계들이 부가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다.

[0110] 도 10의 설명

[0111] 도 10은 클라이언트 전자 디바이스 및 호스트 전자 디바이스를 사용하여 서비스 제공자 서브시스템과의 거래를 수행하기 위한 예시적인 프로세스(1000)의 흐름도이다. 프로세스(1000)의 단계(1002)에서, 클라이언트 전자 디바이스는 서비스 제공자 서브시스템의 제품에 대한 액세스를 구매하기 위해 거래의 적어도 일부분을 정의하기 위해 서비스 제공자 서브시스템과 통신할 수 있다. 예를 들어, 클라이언트 전자 디바이스(100')는 판매자 서브시스템(200)으로부터 금융 거래를 나타내는 잠재 거래 데이터(660)를 수신할 수 있다. 프로세스(1000)의 단계(1004)에서, 클라이언트 전자 디바이스는 호스트 전자 디바이스가 거래를 지불하기 위한 거래 크리덴셜을 생성하는 것을 수반할 수 있다. 예를 들어, 클라이언트 전자 디바이스(100')는 잠재 거래 데이터(660/672)에 기초하여, 결제 요청 데이터(666/674)를 호스트 전자 디바이스(100)에 송신할 수 있다.

[0112] 도 10의 프로세스(1000)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 부가적인 단계들이 부가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다.

[0113] 도 1, 도 1a, 도 1b, 도 2, 도 2a 및 도 3의 추가 설명

[0114] 호스트 디바이스(100)의 보안 요소의 크리덴셜(예컨대, NFC 컴포넌트(120)의 크리덴셜 SSD(154a)의 인에이블된 애플릿(153a)과 연관된 상거래 크리덴셜 데이터)이 호스트 거래 데이터의 호스트 결제 크리덴셜 데이터로서(예컨대, 판매자 단말기(220)에 대한 비접촉식 근접-기반 통신 및/또는 판매자 서버(210)에 대한 온라인 기반 통신으로서) 제공되도록 적절하게 인에이블될 때, 매입 은행 서브시스템(300)은 금융 기관 서브시스템(350)과의 금융 거래를 완료하기 위해 그러한 호스트 결제 크리덴셜 데이터를 활용할 수 있다. 예를 들어, 클라이언트 디바이스(100')의 사용자가 구매를 위한 제품을 선택하고, 호스트 디바이스(100)의 사용자가 결제를 위해 디바이스(100)의 특정 크리덴셜이 사용되도록 적절히 인에이블한 후, 판매자 서브시스템(200)은 특정 크리덴셜에 대한 결제 크리덴셜 데이터를 나타내는 호스트 결제 크리덴셜 데이터를 수신할 수 있다. 판매자 서버(210) 및/또는 판매자 단말기(220)는, 디바이스(100)가 (예컨대, 클라이언트 디바이스(100'))를 통해 호스트 결제 크리덴셜 데이터를 제공하는 것에 응답하여, 임의의 적합한 판매자 또는 최종 사용자 전자 디바이스의 사용자에게 제품 또는 서비스를 제공할 수 있는 판매자 서브시스템(200)의 판매자 에이전트에 의해 제공될 수 있다. (예컨대, 데이터(686)로서) 그러한 수신된 호스트 결제 크리덴셜 데이터에 기초하여, 판매자 서브시스템(200)은 데이터(688)를 생성하고 (예컨대, 판매자 서브시스템(200)과 매입 은행 서브시스템(300) 사이의 통신 경로(25)를 통해) 매입 은행 서브시스템(300)에 송신하도록 구성될 수 있으며, 데이터(688)는 호스트 결제 크리덴셜 데이터 및 호스트 디바이스 결제 크리덴셜 및 제품 또는 서비스에 대한 판매자의 구매 가격을 나타낼 수 있는 인증 요청을 포함할 수 있다. 결제 프로세서 또는 매입자(acquirer)로도 알려진 매입 은행 서브시스템(300)은 판매자 서브시스템(200)과 연관된 판매자의 은행 파트너일 수 있고, 매입 은행 서브시스템(300)은 금융 기관 서브시스템(350)과 협력하여, 호스트 결제 크리덴셜 데이터로 호스트 디바이스(100)에 의해 지불되도록 시도된 크리덴셜 거래들을 승인 및 결제하도록 구성될 수 있다. 이어서, 매입 은행 서브시스템(300)은 결제 데이터(688)로부터의 인증 요청을 (예컨대, 매입 은행 서브시스템(300)과 금융 기관 서브시스템(350) 사이의 통신 경로(35)를 통해) 금융 기관 서브시스템(350)으로 인증 데이터(690)로서 포워드할 수 있다.

[0115] 결제 네트워크 서브시스템(360) 및 발행 은행 서브시스템(370)은 단일 엔티티 또는 별개의 엔티티들일 수 있다. 예를 들어, 아메리칸 익스프레스는 결제 네트워크 서브시스템(360) 및 발행 은행 서브시스템(370) 둘 다일 수 있다. 그에 반해, 비자 및 마스터카드의 결제 네트워크(360)일 수 있고, 체이스(Chase), 웰스 파코(Wells Fargo), 뱅크 오브 아메리카(Bank of America) 등과 같은 발행 은행(370)과 협력하여 동작할 수 있다. 금융 기관 서브시스템(350)은 또한 매입 은행 서브시스템(300)과 같은 하나 이상의 매입 은행을 포함할 수 있다. 예를

들어, 매입 은행 서브시스템(300)은 발행 은행 서브시스템(370)과 동일한 엔티티일 수 있다. 매입 은행 서브시스템(300)의 하나의, 일부의, 또는 모든 컴포넌트는, 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 하나 이상의 프로세서 컴포넌트, 디바이스(100)의 메모리 컴포넌트(104)와 동일하거나 유사할 수 있는 하나 이상의 메모리 컴포넌트, 및/또는 디바이스(100)의 통신 컴포넌트(106)와 동일하거나 유사할 수 있는 하나 이상의 통신 컴포넌트를 사용하여 구현될 수 있다. 결제 네트워크 서브시스템(360)의 하나의, 일부의, 또는 모든 컴포넌트는, 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 하나 이상의 프로세서 컴포넌트, 디바이스(100)의 메모리 컴포넌트(104)와 동일하거나 유사할 수 있는 하나 이상의 메모리 컴포넌트, 및/또는 디바이스(100)의 통신 컴포넌트(106)와 동일하거나 유사할 수 있는 하나 이상의 통신 컴포넌트를 사용하여 구현될 수 있다. 발행 은행 서브시스템(370)의 하나의, 일부의, 또는 모든 컴포넌트는, 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 하나 이상의 프로세서 컴포넌트, 디바이스(100)의 메모리 컴포넌트(104)와 동일하거나 유사할 수 있는 하나 이상의 메모리 컴포넌트, 및/또는 디바이스(100)의 통신 컴포넌트(106)와 동일하거나 유사할 수 있는 하나 이상의 통신 컴포넌트를 사용하여 구현될 수 있다. 결제 네트워크 서브시스템(360)과 발행 은행 서브시스템(370)이 개별 엔티티들인 경우, 결제 네트워크 서브시스템(360)은 매입 은행 서브시스템(300)으로부터 데이터(690)를 수신할 수 있고, 이어서 발행 은행 서브시스템(370)으로 (예컨대, 결제 네트워크 서브시스템(360)과 발행 은행 서브시스템(370) 사이의 통신 경로(45)를 통해) 데이터(405)로서 요청을 포워드할 수 있다. 결제 네트워크 서브시스템(360)과 발행 은행 서브시스템(370)이 동일한 엔티티인 경우, 매입 은행 서브시스템(300)은 데이터(690)를 발행 은행 서브시스템(370)에 직접 제출할 수 있다. 또한, 결제 네트워크 서브시스템(360)은 발행 은행 서브시스템(370)을 대신하여 (예컨대, 결제 네트워크 서브시스템(360)과 발행 은행 서브시스템(370) 사이에서 합의된 조건에 따라) 매입 은행 서브시스템(300)에 응답할 수 있다. 매입 은행 서브시스템(300)과 발행 은행 서브시스템(370) 사이에서 인터페이싱함으로써, 결제 네트워크 서브시스템(360)은 매입 은행 서브시스템(300) 및 각각의 발행 은행 서브시스템(370)이 직접 상호작용해야 할 수 있는 엔티티의 수를 감소시킬 수 있다. 즉, 금융 기관 서브시스템(350)의 직접적인 통합 지점들을 최소화하기 위해, 결제 네트워크 서브시스템(360)은 다양한 발행 은행(370) 및/또는 다양한 매입 은행(300)에 대한 통합관리자(aggregator)로서 작용할 수 있다. 금융 기관 서브시스템(350)은 또한 매입 은행 서브시스템(300)과 같은 하나 이상의 매입 은행을 포함할 수 있다. 예를 들어, 매입 은행 서브시스템(300)은 발행 은행 서브시스템(370)과 동일한 엔티티일 수 있다.

[0116] 발행 은행 서브시스템(370)이 (예컨대, 매입 은행 서브시스템(300)으로부터 데이터(690)로서 직접적으로, 또는 결제 네트워크 서브시스템(360)을 통해 데이터(405)로서 간접적으로) 인증 요청을 수신하면, 결제 정보(예컨대, 디바이스(100)의 상거래 크리덴셜 정보) 및 인증 요청에 포함된 구매 금액은 분석되어 상거래 크리덴셜과 연관된 계정이 구매 금액을 충당하기에 충분한 크레디트를 갖는지를 결정할 수 있다. 충분한 지불금이 존재하지 않으면, 발행 은행 서브시스템(370)은 매입 은행 서브시스템(300)에 부정적인 인가 응답을 송신함으로써 요청된 거래를 거절할 수 있다. 그러나, 충분한 지불금이 존재하는 경우, 발행 은행 서브시스템(370)은 매입 은행 서브시스템(300)에 긍정적인 인증 응답을 송신함으로써 요청된 거래를 승인할 수 있고, 금융 거래가 완료될 수 있다. 어느 한 유형의 인증 응답이 사용자 금융 서브시스템(350)에 의해 인증 응답 데이터 또는 거래 상태 데이터(692)로서 매입 은행 서브시스템(300)으로 제공될 수 있다(예컨대, 거래 상태 데이터(692)는 발급 은행 서브시스템(370)으로부터 통신 경로(35)를 통해 매입 은행 서브시스템(300)으로 직접 제공될 수 있거나, 거래 상태 데이터(692)는 결제 네트워크 서브시스템(360)으로부터 통신 경로(45)를 통해 발행 은행 서브시스템(370)으로부터 결제 네트워크 서브시스템(360)에 제공될 수 있는 인증 응답 데이터 또는 거래 상태 데이터(415)에 기초하여 매입 은행 서브시스템(300)으로 제공될 수 있음).

[0117] 언급한 바와 같이, 그리고 도 2에 도시된 바와 같이, 호스트 전자 디바이스(100)는, 음악 재생기(예컨대, 미국 캘리포니아주 쿠파티노 소재의 애플 인크.에 의해 입수가 가능한 아이팟™), 비디오 재생기, 스틸 이미지 재생기, 게임 재생기, 기타 미디어 재생기, 음악 레코더, 영화 또는 비디오 카메라 또는 레코더, 스틸 카메라, 기타 미디어 레코더, 라디오, 의료 장비, 가전기기 또는 상업기기 제품, 배송 차량 기구, 악기, 계산기, 셀룰러 전화기(예컨대, 애플 인크.에 의해 입수가 가능한 아이폰™), 기타 무선 통신 디바이스, 개인 휴대 단말기, 리모콘, 무선 호출기, 컴퓨터(예컨대, 데스크톱, 랩톱, 태블릿(예컨대, 애플 인크.에 의해 입수가 가능한 아이패드™), 서버 등), 모니터, 텔레비전, 스테레오 장치, 셋업 박스(set up box), 셋톱 박스(set-top box), 붐 박스, 모뎀, 라우터, 프린터, 또는 이들의 임의의 조합을 포함할 수 있지만, 이들로 제한되지 않는다. 일부 실시예들에서, 전자 디바이스(100)는 단일 기능을 수행할 수 있고(예컨대, 금융 거래를 이행하는 것에 전용되는 디바이스), 다른 실시예들에서, 전자 디바이스(100)는 다수의 기능을 수행할 수 있다(예컨대, 금융 거래를 이행하고, 음악을 재생하고, 전화 통화를 수신 및 송신하는 디바이스). 전자 디바이스(100)는 사용자가 어디로 이동하든지 금융 거

래를 이행하도록 구성될 수 있는 임의의 휴대용, 모바일, 핸드헬드, 또는 소형 전자 디바이스일 수 있다. 일부 소형 전자 디바이스들은 아이팟™과 같은 핸드헬드 전자 디바이스의 폼 팩터보다 작은 폼 팩터를 가질 수 있다. 예시적인 소형 전자 디바이스들은, 시계(예컨대, 애플 인크.의 애플 워치™), 반지, 목걸이, 벨트, 벨트용 액세서리, 헤드셋, 신발용 액세서리, 가상현실 디바이스, 안경, 다른 착용가능 전자장치, 스포츠 장비용 액세서리, 체력단련 기구용 액세서리, 키 체인, 또는 이들의 임의의 조합을 포함할 수 있지만 이들로 제한되지 않는 다양한 물체 내에 통합될 수 있다. 대안적으로, 호스트 전자 디바이스(100)는 휴대용이 전혀 아닐 수도 있고, 오히려 대체적으로 고정형일 수도 있다.

[0118] 도 2에 도시된 바와 같이, 예를 들어, 전자 디바이스(100)는 프로세서(102), 메모리(104), 통신 컴포넌트(106), 전원 공급장치(108), 입력 컴포넌트(110), 출력 컴포넌트(112), 안테나(116), 및 근거리 통신("NFC") 컴포넌트(120)를 포함할 수 있다. 전자 디바이스(100)는 또한, 디바이스(100)의 다양한 다른 컴포넌트들로, 그것들로부터, 또는 그것들 사이에서 데이터 및/또는 전력을 전송하기 위한 하나 이상의 유선 또는 무선 통신 링크 또는 경로를 제공할 수 있는 버스(118)를 포함할 수 있다. 일부 실시예들에서, 전자 디바이스(100)의 하나 이상의 컴포넌트는 조합되거나 생략될 수 있다. 또한, 전자 디바이스(100)는 도 2에서 조합되거나 포함되지 않은 다른 컴포넌트들을 포함할 수 있다. 예를 들어, 전자 디바이스(100)는 임의의 다른 적합한 컴포넌트들 또는 도 2에 도시된 컴포넌트들의 여러 예들을 포함할 수 있다. 단순화하기 위하여, 컴포넌트들 각각 중 단지 하나만이 도 2에 도시된다.

[0119] 메모리(104)는, 예를 들어, 하드 드라이브, 플래시 메모리, 판독전용 메모리("ROM")와 같은 영구 메모리, 랜덤 액세스 메모리("RAM")와 같은 반-영구 메모리, 임의의 다른 적합한 유형의 저장 컴포넌트, 또는 이들의 임의의 조합을 포함하는, 하나 이상의 저장 매체를 포함할 수 있다. 메모리(104)는, 전자 디바이스 애플리케이션들을 위한 데이터를 임시로 저장하는 데 사용되는 하나 이상의 다른 유형의 메모리일 수 있는 캐시 메모리를 포함할 수 있다. 메모리(104)는 전자 디바이스(100) 내에 고정되게 임베드될 수 있거나, 전자 디바이스(100) 안으로 반복적으로 삽입되고 그로부터 제거될 수 있는 하나 이상의 적합한 유형의 카드(예컨대, 가입자 아이덴티티 모듈("SIM") 카드 또는 시큐어 디지털("SD") 메모리 카드) 상에 통합될 수 있다. 메모리(104)는 미디어 데이터(예컨대, 음악 및 이미지 파일), (예컨대, 디바이스(100) 상에서 기능들을 구현하기 위한) 소프트웨어, 펌웨어, 선호도 정보(예컨대, 미디어 재생 선호도), 생활방식 정보(예컨대, 음식 선호도), 운동 정보(예컨대, 운동 모니터링 장비에 의해 획득된 정보), 거래 정보(예컨대, 신용 카드 정보와 같은 정보), 무선 접속 정보(예컨대, 디바이스(100)가 무선 접속을 설정할 수 있게 하는 정보), 가입 정보(예컨대, 사용자가 가입한 팟캐스트들 또는 텔레비전 쇼들 또는 다른 미디어의 추적을 유지하는 정보), 연락처 정보(예컨대, 전화번호들 및 이메일 주소들), 달력 정보, 임의의 다른 적합한 데이터, 또는 이들의 조합을 저장할 수 있다.

[0120] 통신 컴포넌트(106)는, 디바이스(100)가 임의의 적합한 통신 프로토콜을 사용하여 하나 이상의 다른 전자 디바이스 또는 서버 또는 서브시스템(예컨대, 시스템(1)의 하나 이상의 서브시스템 또는 다른 컴포넌트들)과 통신할 수 있게 하기 위해 제공될 수 있다. 예를 들어, 통신 컴포넌트(106)는 Wi-Fi(예컨대, 802.11 프로토콜), ZigBee(예컨대, 802.15.4 프로토콜), WiDi™, 이더넷(Ethernet), 블루투스(Bluetooth)™, 블루투스™ 저전력(Bluetooth™ Low Energy, "BLE"), 고주파수 시스템들(예컨대, 900 Mhz, 2.4 GHz, 및 5.6 GHz 통신 시스템들), 적외선, 전송 제어 프로토콜/인터넷 프로토콜("TCP/IP")(예컨대, TCP/IP 계층들 각각에서 사용되는 임의의 프로토콜), 스트림 제어 전송 프로토콜("SCTP"), 동적 호스트 구성 프로토콜("DHCP"), 하이퍼텍스트 전송 프로토콜("HTTP"), 비트토렌트(BitTorrent)™, 파일 전송 프로토콜("FTP"), 실시간 전송 프로토콜("RTP"), 실시간 스트리밍 프로토콜("RTSP"), 실시간 제어 프로토콜("RTCP"), 원격 오디오 출력 프로토콜("RAOP"), 실시간 데이터 전송 프로토콜™("RDTP"), 사용자 데이터그램 프로토콜("UDP"), 보안 셸 프로토콜("SSH"), 무선 분산 시스템("WDS") 브리징, 무선 및 셀룰러 전화 및 개인용 이메일 디바이스에 의해 사용될 수 있는 임의의 통신 프로토콜(예컨대, 모바일 통신용 글로벌 시스템("GSM"), "EDGE"(GSM plus Enhanced Data rates for GSM Evolution), 코드 분할 다중 접속("CDMA"), 직교 주파수-분할 다중 접속("OFDMA"), 고속 패킷 접속("HSPA"), 다중-대역 등), 저전력 무선 근거리 개인 통신망("6LoWPAN") 모듈에 의해 사용될 수 있는 임의의 통신 프로토콜, 임의의 다른 통신 프로토콜, 또는 이들의 임의의 조합을 지원할 수 있다. 통신 컴포넌트(106)는 또한, 디바이스(100)가 다른 디바이스(예컨대, 호스트 컴퓨터 또는 액세서리 디바이스)에 통신가능하게 연결되고 무선으로 또는 유선 접속을 통해(예컨대, 커넥터 포트를 사용하여) 그 다른 디바이스와 통신할 수 있게 하는, 임의의 적합한 송수신기 회로(예컨대, 버스(118)를 통한 송수신기 회로 또는 안테나(116))를 포함하거나 그에 전기적으로 연결될 수 있다. 통신 컴포넌트(106)는 임의의 적합한 데이터를 임의의 원격 서버 또는 다른 적합한 엔티티(예컨대, 임의의 적합한 인터넷 접속)에 통신하도록 동작할 때 온라인 통신 컴포넌트로서 지칭될 수 있다. 통신 컴포넌트(106)는 전자 디바이스(100)의 지리적 위치를 결정하도록 구성될 수 있다. 예를 들어, 통신 컴포넌트(106)는 위성

위치확인 시스템("GPS"), 또는 기지국 위치확인 기술 또는 Wi-Fi 기술을 사용할 수 있는 지역적 또는 사이트-적(site-wide) 위치확인 시스템을 활용할 수 있다.

[0121] 전원 공급장치(108)는 전력을 수신 및/또는 생성하기 위한, 그리고 그러한 전력을 전자 디바이스(100)의 다른 컴포넌트들 중 하나 이상에 공급하기 위한 임의의 적합한 회로를 포함할 수 있다. 예를 들어, 전원 공급장치(108)는 전력망에 연결될 수 있다(예컨대, 디바이스(100)가 휴대용 디바이스로서 동작하고 있지 않은 경우, 또는 디바이스의 배터리가 전력 발전소에 의해 생성된 전력으로 전기 콘센트에서 충전되고 있는 경우). 다른 예로서, 전원 공급장치(108)는 천연 소스로부터 전력을 생성하도록 구성될 수 있다(예컨대, 태양전지를 이용한 태양열 발전). 다른 예로서, 전원 공급장치(108)는 전력을 제공하기 위한 하나 이상의 배터리를 포함할 수 있다(예컨대, 디바이스(100)가 휴대용 디바이스로서 동작하고 있는 경우). 예를 들어, 전원 공급장치(108)는 배터리(예컨대, 겔, 니켈 수소 합금(nickel metal hydride), 니켈 카드뮴, 니켈 수소, 납축전지, 또는 리튬이온 배터리), 무정전 또는 연속적 전원 공급장치(uninterruptible 또는 continuous power supply, "UPS" 또는 "CPS"), 및 전력 생성원으로부터 수신된 전력(예컨대, 전력 발전소에서 생성되고, 전기 소켓 또는 그 외의 것을 통해 사용자에게 전달되는 전력)을 프로세싱하기 위한 회로 중 하나 이상을 포함할 수 있다. 전력은 전원 공급장치(108)에 의해 교류 또는 직류로서 제공될 수 있으며, 전력을 변환하거나 수신된 전력을 특정 특성들로 제한하도록 프로세싱될 수 있다. 예를 들어, 전력은 직류로 또는 직류로부터 변환되고, 평균 전력, 유효 전력, 피크 전력, 펄스당 에너지, 전압, (예컨대, 암페어로 측정되는) 전류, 또는 수신된 전력의 임의의 다른 특성 중 하나 이상의 값으로 제한될 수 있다. 전원 공급장치(108)는, (예컨대, 배터리가 이미 충전되어 있을 때보다 배터리를 충전시킬 때 더 많은 전력을 요청하기 위하여) 예를 들어, 전자 디바이스(100) 또는 전자 디바이스(100)에 연결될 수 있는 주변 디바이스들의 요구들 또는 요건들에 기초하여, 상이한 시간들에서 특정한 전력 양들을 요청하거나 제공하도록 동작할 수 있다.

[0122] 하나 이상의 입력 컴포넌트(110)는, 사용자가 디바이스(100)와 상호작용하거나 그와 인터페이싱하는 것을 허용하기 위해 제공될 수 있다. 예를 들어, 입력 컴포넌트(110)는 터치 패드, 다이얼, 클릭 휠, 스크롤 휠, 터치스크린, 하나 이상의 버튼(예컨대, 키보드), 마우스, 조이스틱, 트랙볼, 마이크로폰, 카메라, 스캐너(예컨대, 바코드 스캐너, 또는 바코드, QR 코드 등과 같은 코드로부터 제품 식별 정보를 획득할 수 있는 임의의 다른 적합한 스캐너), 근접 센서, 광 검출기, 모션 센서, 생체인식 센서(예컨대, 사용자를 인증하기 위해 전자 디바이스(100)에 액세스가능할 수 있는 특징-프로세싱 애플리케이션과 공조하여 동작할 수 있는, 지문 판독기 또는 다른 특징 인식 센서), 및 이들의 조합들을 포함하지만 이들로 제한되지 않는, 다양한 형태를 취할 수 있다. 각각의 입력 컴포넌트(110)는 동작하는 디바이스(100)와 연관된 커맨드들을 발행하거나 선택들을 행하는, 하나 이상의 전용 제어 기능을 제공하도록 구성될 수 있다.

[0123] 전자 디바이스(100)는 또한, 정보(예컨대, 그래픽, 청각적 및/또는 촉각적 정보)를 디바이스(100)의 사용자에게 제시할 수 있는 하나 이상의 출력 컴포넌트(112)를 포함할 수 있다. 예를 들어, 전자 디바이스(100)의 출력 컴포넌트(112)는 오디오 스피커, 헤드폰, 오디오 라인-출력, 시각적 디스플레이, 안테나, 적외선 포트, 햅틱 출력 컴포넌트(예컨대, 럼블러(rumbler), 진동기 등), 또는 이들의 조합들을 포함하지만 이들로 제한되지 않는, 다양한 형태를 취할 수 있다.

[0124] 특정 예로서, 전자 디바이스(100)는 출력 컴포넌트(112)로서 디스플레이 출력 컴포넌트를 포함할 수 있다. 그러한 디스플레이 출력 컴포넌트는 시각적 데이터를 사용자에게 제시하기 위한 임의의 적합한 유형의 디스플레이 또는 인터페이스를 포함할 수 있다. 디스플레이 출력 컴포넌트는 디바이스(100)에 임베드되거나 디바이스(100)에 연결된 디스플레이(예컨대, 탈착가능한 디스플레이)를 포함할 수 있다. 디스플레이 출력 컴포넌트는, 예를 들어, 액정 디스플레이("LCD"), 발광 다이오드("LED") 디스플레이, 유기 발광 다이오드("OLED") 디스플레이, 면전도 전자총 디스플레이("SED"), 탄소 나노튜브 디스플레이, 나노크리스탈 디스플레이, 임의의 다른 적합한 유형의 디스플레이, 또는 이들의 조합을 포함할 수 있다. 대안적으로, 디스플레이 출력 컴포넌트는, 예를 들어, 비디오 프로젝터, 전방 디스플레이(head-up display), 또는 3차원(예컨대, 홀로그래픽) 디스플레이와 같은, 전자 디바이스(100)로부터 멀리 떨어진 표면 상에 콘텐츠의 디스플레이를 제공하기 위한 이동가능한 디스플레이 또는 프로젝션 시스템을 포함할 수 있다. 다른 예로서, 디스플레이 출력 컴포넌트는, 컴팩트 디지털 카메라, 반사 카메라, 또는 임의의 다른 적합한 스틸 또는 비디오 카메라에서 발견되는 유형의 뷰파인더와 같은, 디지털 또는 기계적 뷰파인더를 포함할 수 있다. 디스플레이 출력 컴포넌트는 디스플레이 드라이버 회로, 디스플레이 드라이버들을 구동하기 위한 회로, 또는 둘 다를 포함할 수 있으며, 그러한 디스플레이 출력 컴포넌트는, 프로세서(102)의 지시 하에 있을 수 있는 콘텐츠(예컨대, 미디어 재생 정보, 전자 디바이스(100) 상에서 구현되는 애플리케이션들을 위한 애플리케이션 스크린들, 진행중인 통신 동작들에 관한 정보, 유입 통신 요청들에 관

한 정보, 디바이스 동작 스크린들 등)를 디스플레이하도록 동작할 수 있다.

[0125] 하나 이상의 입력 컴포넌트 및 하나 이상의 출력 컴포넌트는 때때로 본 명세서에서 총칭하여 입력/출력("I/O") 컴포넌트 또는 I/O 인터페이스로서 지칭될 수 있음을 유의해야 한다(예컨대, I/O 컴포넌트 또는 I/O 인터페이스(114)로서의 입력 컴포넌트(110) 및 출력 컴포넌트(112)). 예를 들어, 입력 컴포넌트(110) 및 출력 컴포넌트(112)는 때때로, 사용자의 디스플레이 스크린의 터치를 통해 입력 정보를 수신할 수 있고 또한 그 동일한 디스플레이 스크린을 통해 사용자에게 시각적 정보를 제공할 수 있는, 터치 스크린과 같은, 단일 I/O 컴포넌트(114)일 수 있다.

[0126] 전자 디바이스(100)의 프로세서(102)는 전자 디바이스(100)의 하나 이상의 컴포넌트의 동작들 및 성능을 제어하도록 동작할 수 있는 임의의 프로세싱 회로를 포함할 수 있다. 예를 들어, 프로세서(102)는 입력 컴포넌트(110)로부터 입력 신호들을 수신하고/하거나 출력 컴포넌트(112)를 통해 출력 신호들을 구동할 수 있다. 도 2에 도시된 바와 같이, 프로세서(102)는 애플리케이션(103), 애플리케이션(113) 및/또는 애플리케이션(143)과 같은 하나 이상의 애플리케이션을 실행하는 데 사용될 수 있다. 각각의 애플리케이션(103/113/143)은, 하나 이상의 운영 체제 애플리케이션, 펌웨어 애플리케이션, 미디어 재생 애플리케이션, 미디어 편집 애플리케이션, NFC 저전력 모드 애플리케이션, 생체인식 특징-프로세싱 애플리케이션, 또는 임의의 다른 적합한 애플리케이션들을 포함할 수 있지만 이들로 제한되지 않는다. 예를 들어, 프로세서(102)는, 입력 컴포넌트(110) 또는 디바이스(100)의 다른 컴포넌트를 통해 수신된 명령어들 또는 데이터가, 정보가 저장되고/되거나 출력 컴포넌트(112)를 통해 사용자에게 제공될 수 있는 방식을 어떻게 조작할 수 있는지를 결정하기 위해, 사용자 인터페이스 프로그램으로서 애플리케이션(103/113/143)을 로딩할 수 있다. 애플리케이션(103/113/143)은 임의의 적합한 소스로부터, 예컨대 메모리(104)로부터(예컨대, 버스(118)를 통해) 또는 다른 디바이스 또는 서버로부터(예컨대, 통신 컴포넌트(106)를 통해), 프로세서(102)에 의해 액세스될 수 있다. 프로세서(102)는 단일 프로세서 또는 다수의 프로세서를 포함할 수 있다. 예를 들어, 프로세서(102)는 적어도 하나의 "범용" 마이크로프로세서, 범용 및 전용 마이크로프로세서들의 조합, 명령어 세트 프로세서, 그래픽 프로세서, 비디오 프로세서, 및/또는 관련된 칩셋, 및/또는 전용 마이크로프로세서를 포함할 수 있다. 프로세서(102)는 또한 캐싱 목적을 위해 온보드 메모리(on board memory)를 포함할 수 있다.

[0127] 전자 디바이스(100)는 또한 근거리 통신("NFC") 컴포넌트(120)를 포함할 수 있다. NFC 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200)(예컨대, 판매자 결제 단말기(220)) 사이에서 비접촉식 근접-기반 거래들 또는 통신들을 가능하게 할 수 있는 임의의 적합한 근접-기반 통신 메커니즘일 수 있다. NFC 컴포넌트(120)는 비교적 낮은 데이터 레이트들(예컨대, 424 kbps)에서 가까운 범위의 통신을 허용할 수 있으며, ISO/IEC 7816, ISO/IEC 18092, ECMA-340, ISO/IEC 21481, ECMA-352, ISO 14443, 및/또는 ISO 15693과 같은 임의의 적합한 표준들을 따를 수 있다. 대안적으로 또는 부가적으로, NFC 컴포넌트(120)는 비교적 높은 데이터 레이트들(예컨대, 370 Mbps)에서 가까운 범위의 통신을 허용할 수 있으며, 트랜스퍼젯(TransferJet)TM 프로토콜과 같은 임의의 적합한 표준들을 따를 수 있다. NFC 컴포넌트(120) 또는 NFC 컴포넌트(120')와 판매자 서브시스템(200) 사이의 통신은 NFC 컴포넌트와 판매자 서브시스템(200) 사이의 임의의 적합한 가까운 범위의 거리(예컨대, NFC 컴포넌트(120')와 판매자 결제 단말기(220) 사이의 도 1a 및 도 1b의 거리 D를 참조) 내에서, 예컨대 대략 2 내지 4 센티미터의 범위 내에서 일어날 수 있으며, 임의의 적합한 주파수(예컨대, 13.56 MHz)에서 동작할 수 있다. 예를 들어, NFC 컴포넌트의 그러한 가까운 범위의 통신은 자기장 유도를 통해 발생할 수 있으며, 이는 NFC 컴포넌트가 다른 NFC 디바이스들과 통신하고/하거나 무선 주파수 식별("RFID") 회로를 갖는 태그들로부터 정보를 검색하게 할 수 있다. 그러한 NFC 컴포넌트는 상품 정보를 획득하고, 결제 정보를 전송하고, 그렇지 않으면 외부 디바이스와 통신(예컨대, NFC 컴포넌트(120')와 판매자 단말기(220) 사이 및/또는 NFC 컴포넌트(120')와 NFC 컴포넌트(120) 사이에서 통신)하는 방식을 제공할 수 있다.

[0128] NFC 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200) 사이에서 비접촉식 근접-기반 통신을 인에이블하기 위한 임의의 적합한 모듈들을 포함할 수 있다. 도 2에 도시된 바와 같이, 예를 들어, NFC 컴포넌트(120)는 NFC 디바이스 모듈(130), NFC 컨트롤러 모듈(140), 및 NFC 메모리 모듈(150)을 포함할 수 있다.

[0129] NFC 디바이스 모듈(130)은 NFC 데이터 모듈(132), NFC 안테나(134), 및 NFC 부스터(136)를 포함할 수 있다. NFC 데이터 모듈(132)은, NFC 컴포넌트(120)에 의해 판매자 서브시스템(200)으로 비접촉식 근접-기반 또는 NFC 통신(5)의 일부로서 송신될 수 있는 임의의 적합한 데이터를 포함하거나, 라우팅하거나, 또는 그렇지 않으면 제공하도록 구성될 수 있다. 부가적으로 또는 대안적으로, NFC 데이터 모듈(132)은, 비접촉식 근접-기반 통신(예컨대, NFC 컴포넌트(120') 및 판매자 단말기(220) 사이의 통신(5))의 일부로서 판매자 서브시스템(200)으로부터 NFC 컴포넌트(120)에 의해 수신될 수 있는 임의의 적합한 데이터를 포함하거나, 라우팅하거나, 또는 그렇지 않

으면 수신하도록 구성될 수 있다.

- [0130] NFC 송수신기 또는 NFC 안테나(134)는, 일반적으로 NFC 데이터 모듈(132)로부터 판매자 서브시스템(200)으로 그리고/또는 서브시스템(200)으로부터 NFC 데이터 모듈(132)로의 통신의 전달을 가능하게 할 수 있는, 임의의 적합한 안테나 또는 다른 적합한 송수신기 회로일 수 있다. 따라서, NFC 안테나(134)(예컨대, 루프 안테나)는 특히 NFC 컴포넌트(120)의 비접촉식 근접-기반 통신 기능들을 가능하게 하기 위해 제공될 수 있다.
- [0131] 대안적으로 또는 부가적으로, NFC 컴포넌트(120)는, 전자 디바이스(100)의 다른 통신 컴포넌트(예컨대, 통신 컴포넌트(106))가 활용할 수 있는 동일한 송수신기 회로 또는 안테나(예컨대, 안테나(116))를 활용할 수 있다. 예를 들어, 통신 컴포넌트(106)가 안테나(116)를 레버리지하여 전자 디바이스(100)와 다른 원격 엔티티 사이의 Wi-Fi, 블루투스™, 셀룰러, 또는 GPS 통신을 가능하게 할 수 있는 한편, NFC 컴포넌트(120)는 안테나(116)를 레버리지하여 NFC 디바이스 모듈(130)의 NFC 데이터 모듈(132)과 다른 엔티티(예컨대, 판매자 서브시스템(200)) 사이의 비접촉식 근접-기반 또는 NFC 통신을 가능하게 할 수 있다. 그러한 실시예들에서, NFC 디바이스 모듈(130)은, NFC 컴포넌트(120)의 데이터(예컨대, NFC 데이터 모듈(132) 내의 데이터)에 적절한 신호 증폭을 제공하여 그러한 데이터가 서브시스템(200)으로 통신으로서 공유 안테나(116)에 의해 적절히 송신되도록 구성될 수 있는, NFC 부스터(136)를 포함할 수 있다. 예를 들어, 공유 안테나(116)는, 안테나(116)(예컨대, 비-루프 안테나)가 전자 디바이스(100)와 판매자 서브시스템(200) 사이의 비접촉식 근접-기반 또는 NFC 통신을 전달하기 위해 적절히 인에이블될 수 있기 전에, 부스터(136)로부터의 증폭을 요구할 수 있다(예컨대, 안테나(116)를 이용하여 다른 유형들의 데이터를 송신하기 위해 필요할 수 있는 것보다, 안테나(116)를 이용하여 NFC 데이터를 송신하기 위해 필요할 수 있는 전력이 더 클 수 있다).
- [0132] NFC 컨트롤러 모듈(140)은 적어도 하나의 NFC 프로세서 모듈(142)을 포함할 수 있다. NFC 프로세서 모듈(142)은 NFC 디바이스 모듈(130)과 공조하여 동작하여, 전자 디바이스(100)와 판매자 서브시스템(200) 사이에서 NFC 통신을 전달하기 위한 NFC 컴포넌트(120)를 인에이블하고, 활성화하고, 허용하고, 그리고/또는 그렇지 않으면 제어할 수 있다. NFC 프로세서 모듈(142)은 별개의 컴포넌트로서 존재할 수 있거나, 다른 칩셋 내에 통합될 수 있거나, 또는 예를 들어, 시스템 온 칩("SoC")의 일부로서 프로세서(102)와 통합될 수 있다. 도 2에 도시된 바와 같이, NFC 컨트롤러 모듈(140)의 NFC 프로세서 모듈(142)은, NFC 컴포넌트(120)의 기능을 지시하는 데 도움을 줄 수 있는, NFC 저전력 모드 또는 월렛 애플리케이션(143)과 같은, 하나 이상의 애플리케이션을 실행하는 데 사용될 수 있다. 애플리케이션(143)은 하나 이상의 운영 체제 애플리케이션, 펌웨어 애플리케이션, NFC 저전력 애플리케이션, 또는 NFC 컴포넌트(120)에 액세스가능할 수 있는 임의의 다른 적합한 애플리케이션들(예컨대, 애플리케이션(103/113))을 포함할 수 있지만 이들로 제한되지 않는다. NFC 컨트롤러 모듈(140)은 다른 NFC 디바이스(예컨대, 판매자 서브시스템(200))와 통신하기 위한, 근거리 통신 인터페이스 및 프로토콜("NFCIP-1")들과 같은, 하나 이상의 프로토콜을 포함할 수 있다. 프로토콜들은 통신 속도를 조정하고, 접속된 디바이스들 중 하나를 근거리 통신을 제어하는 개시 디바이스로서 지정하는 데 사용될 수 있다.
- [0133] NFC 컨트롤러 모듈(140)은 NFC 컴포넌트(120)의 근거리 통신 모드를 제어할 수 있다. 예를 들어, NFC 프로세서 모듈(142)은, NFC 태그들로부터(예컨대, 판매자 서브시스템(200)으로부터) NFC 데이터 모듈(132)로의 정보(예컨대, 통신(5))를 판독하기 위한 판독기/기록기 모드, 다른 NFC 인에이블된 디바이스(예컨대, 판매자 서브시스템(200))와 데이터(예컨대, 통신(5))를 교환하기 위한 피어-투-피어 모드, 및 다른 NFC 인에이블 디바이스(예컨대, 판매자 서브시스템(200))가 NFC 데이터 모듈(132)로부터 정보(예컨대, 통신(5))를 판독할 수 있게 하기 위한 카드 에뮬레이션 모드 사이에서, NFC 디바이스 모듈(130)을 전환시키도록 구성될 수 있다. NFC 컨트롤러 모듈(140)은 또한 능동 및 수동 모드들 사이에서 NFC 컴포넌트(120)를 전환시키도록 구성될 수 있다. 예를 들어, NFC 프로세서 모듈(142)은, NFC 디바이스 모듈(130)이 자신의 RF 필드를 생성할 수 있는 능동 모드와, NFC 디바이스 모듈(130)이 RF 필드를 생성하는 다른 디바이스(예컨대, 판매자 서브시스템(200))로 데이터를 전송하기 위해 부하 변조를 이용할 수 있는 수동 모드 사이에서, (예컨대, NFC 안테나(134) 또는 공유 안테나(116)와 공조하여) NFC 디바이스 모듈(130)을 전환시키도록 구성될 수 있다. 그러한 수동 모드에서의 동작은, 그러한 능동 모드에서의 동작과 비교하여 전자 디바이스(100)의 배터리 수명을 연장시킬 수 있다. NFC 디바이스 모듈(130)의 모드들은 사용자의 선호도에 기초하여 그리고/또는 디바이스(100)의 제조업자의 선호도에 기초하여 제어될 수 있으며, 이는 디바이스(100) 상에 실행중인 애플리케이션(예컨대, 애플리케이션(103) 및/또는 애플리케이션(143))에 의해 정의되거나 그렇지 않으면 지시될 수 있다.
- [0134] NFC 메모리 모듈(150)은 NFC 디바이스 모듈(130) 및/또는 NFC 컨트롤러 모듈(140)과 공조하여 동작하여, 전자 디바이스(100)와 판매자 서브시스템(200) 사이의 NFC 통신을 허용할 수 있다. NFC 메모리 모듈(150)은 NFC 디바이스 하드웨어 내에 또는 NFC 집적회로("IC") 내에 임베드될 수 있다. NFC 메모리 모듈(150)은 변조 방지일

수 있고 보안 요소의 적어도 일부분을 제공할 수 있다. 예를 들어, NFC 메모리 모듈(150)은 NFC 컨트롤러 모듈(140)에 의해 액세스될 수 있는 NFC 통신들과 관련된 하나 이상의 애플리케이션(예컨대, 애플리케이션(143))을 저장할 수 있다. 예를 들어, 그러한 애플리케이션들은 금융 결제 애플리케이션, 보안 액세스 시스템 애플리케이션, 로열티 카드(loyalty card) 애플리케이션, 및 다른 애플리케이션들을 포함할 수 있으며, 이들은 암호화될 수 있다. 일부 실시예들에서, NFC 컨트롤러 모듈(140) 및 NFC 메모리 모듈(150)은 독립적으로 또는 조합하여, 운영 체제, 메모리, 애플리케이션 환경, 및 민감한 애플리케이션들을 전자 디바이스(100) 상에서 저장 및 실행시키는 데 사용되도록 의도되는 보안 프로토콜들을 포함할 수 있는 전용 마이크로프로세서 시스템을 제공할 수 있다. NFC 컨트롤러 모듈(140) 및 NFC 메모리 모듈(150)은 독립적으로 또는 조합하여, 변조 방지일 수 있는 보안 요소(145)의 적어도 일부분을 제공할 수 있다. 예를 들어, 그러한 보안 요소(145)는, 잘-식별된 신뢰 기관들의 세트에 의해 제시될 수 있는 규칙들 및 보안 요건들(예컨대, 금융 기관 서브시스템의 권한 및/또는 글로벌 플랫폼과 같은 산업 표준)에 따라 애플리케이션들 및 그것들의 기밀의 암호화 데이터(예컨대, 애플릿(153) 및 키(155))를 안전하게 호스팅할 수 있는 변조-방지 플랫폼을(예컨대, 단일의 또는 다중 칩 보안 마이크로컨트롤러로서) 제공하도록 구성될 수 있다. NFC 메모리 모듈(150)은 메모리(104)의 일부분, 또는 NFC 컴포넌트(120)에 대해 특정한 적어도 하나의 전용 칩일 수 있다. NFC 메모리 모듈(150)은 전자 디바이스(100)의 마더보드 상의 전용 칩인 SIM 상에, 또는 메모리 카드 내의 외부 플러그로서 상주할 수 있다. NFC 메모리 모듈(150)은 NFC 컨트롤러 모듈(140)에 완전히 독립적일 수 있으며, 디바이스(100)의 상이한 컴포넌트들에 의해 제공될 수 있고/있거나 상이한 탈착가능한 서브시스템들에 의해 전자 디바이스(100)에 제공될 수 있다. 보안 요소(145)는 전자 디바이스(100) 상에 민감한 데이터 또는 애플리케이션을 저장하는 데 사용될 수 있는 칩 내의 고도로 안전한 변조 방지 하드웨어 컴포넌트일 수 있다. 보안 요소(145)의 적어도 일부분은 착탈식 회로 카드, 예컨대, 이동 통신("GSM") 네트워크, 범용 이동 통신 시스템("UMTS") 및/또는 롱 텀 에볼루션("LTE") 표준 네트워크를 지원하는 글로벌 시스템 내에 호환가능한 전자 디바이스(100)에 사용될 수 있는 범용 집적 회로 카드(UICC) 또는 가입자 아이덴티티 모듈("SIM") 카드 내에 제공될 수 있다. 대안적으로 또는 부가적으로, 보안 요소(145)의 적어도 일부분은 디바이스(100)의 제조 중에 전자 디바이스(100)에 임베드될 수 있는 집적 회로에 제공될 수 있다. 대안적으로 또는 부가적으로, 보안 요소(145)의 적어도 일부분은 마이크로 보안 디지털("SD") 메모리 카드와 같은 전자 디바이스(100)에 플러그(plugged), 삽입 또는 그렇지 않으면 연결될 수 있는 주변 디바이스에 제공될 수 있다.

[0135] 도 2에 도시된 바와 같이, NFC 메모리 모듈(150)은 발행자 보안 도메인("ISD")(152) 및 보충적 보안 도메인("SSD")(154)(예컨대, 서비스 제공자 보안 도메인("SPSD"), 신뢰 서비스 관리자 보안 도메인("TSMSPD") 등) 중 하나 이상을 포함할 수 있으며, 이는 NFC 규격 표준(예컨대, 글로벌플랫폼)에 의해 정의 및 관리될 수 있다. 예를 들어, ISD(152)는, 신뢰 서비스 관리자("TSM") 또는 발행 금융 기관(예컨대, 상업적 엔티티 서브시스템(400) 및/또는 금융 기관 서브시스템(350))이, 크리덴셜 콘텐츠 관리, 및/또는 보안 도메인 관리를 위해, (예컨대, 통신 컴포넌트(106)를 통해) 하나 이상의 크리덴셜(예컨대, 다양한 신용 카드, 은행 카드, 선물 카드, 액세스 카드, 교통 패스, 디지털 화폐(예컨대, 비트코인 및 연관된 결제 네트워크) 등과 연관된 상거래 크리덴셜들)을 생성하거나 그렇지 않으면 전자 디바이스(100) 상에 프로비저닝하기 위한 키들 및/또는 다른 적합한 정보를 저장할 수 있는, NFC 메모리 모듈(150)의 일부분일 수 있다. 특정 보충적 보안 도메인("SSD")(154)(예컨대, SSD(154a))은 전자 디바이스(100)에 특정 특권 또는 결제 권한을 제공할 수 있는 특정 TSM 및 적어도 하나의 특정 상거래 크리덴셜(예컨대, 특정 신용 카드 크리덴셜 또는 특정 대중 교통 카드 크리덴셜)과 연관될 수 있다. 예를 들어, 제1 결제 네트워크 서브시스템(360)(예컨대, 비자)은 제1 SSD(154a)에 대한 TSM일 수 있고 제1 SSD(154a)의 애플릿(153a)은 제1 결제 네트워크 서브시스템(360)에 의해 관리되는 상거래 크리덴셜과 연관될 수 있는 한편, 제2 결제 네트워크 서브시스템(360)(예컨대, 마스터 카드)은 다른 SSD(154)에 대한 TSM일 수 있다.

[0136] 보안 특징들은 NFC 컴포넌트(120)의 사용을 인에이블하기 위해(예컨대, 디바이스(100) 상에 프로비저닝된 상거래 크리덴셜들의 활성화를 인에이블하기 위해) 제공될 수 있으며, 이는 크리덴셜의 신용 카드 정보 또는 은행 계좌 정보와 같은 기밀 결제 정보를 전자 디바이스(100)로부터 판매자 서브시스템(200)에 송신할 때 특히 유용할 수 있다. 그러한 보안 특징들은 또한 제한된 액세스를 가질 수 있는 보안 저장 영역을 포함할 수 있다. 예를 들어, (예컨대, 사용자가 보안 요소의 보안 도메인 요소의 수명 주기 상태를 변경하기 위해) 보안 저장 영역에 액세스하도록 개인 식별 번호("PIN") 입력을 통한 사용자 인증, 또는 생체인식 센서와의 사용자 상호작용을 통한 사용자 인증이 제공될 필요가 있을 수 있다. 소정 실시예들에서, 보안 특징들의 일부 또는 모두가 NFC 메모리 모듈(150) 내에 저장될 수 있다. 또한, 서브시스템(200)과의 통신을 위한 인증 키와 같은 보안 정보가, NFC 메모리 모듈(150) 내에 저장될 수 있다. 소정 실시예들에서, NFC 메모리 모듈(150)은 전자 디바이스(100) 내에 임베드된 마이크로컨트롤러를 포함할 수 있다.

[0137] 도 1b의 판매자 서브시스템(200)의 판매자 단말기(220)는 전자 디바이스(100) 또는 전자 디바이스(100')로부터의 NFC 통신(예컨대, 클라이언트 디바이스(100')가 판매자 단말기(220)의 일정 거리 또는 근접 내에 있을 때의 통신(5))을 검출, 판독 또는 그렇지 않으면 수신하기 위한 판독기를 포함할 수 있다. 따라서, 그러한 판매자 단말기와 전자 디바이스(100/100') 사이의 NFC 통신이 무선으로 발생할 수 있으며, 그와 같이, 각각의 디바이스들 사이에 명확한 "가시선(line of sight)"이 요구되지 않을 수도 있음을 유의한다. 언급한 바와 같이, NFC 디바이스 모듈(130)은 수동적이거나 능동적일 수 있다. 수동인 경우, NFC 디바이스 모듈(130)은 그러한 판매자 단말기의 적합한 판독기의 응답 범위 내에서만 활성화될 수 있다. 예를 들어, 그러한 판매자 단말기의 판독기는 비교적 저전력의 전파장(radio wave field)을 방출할 수 있으며, 이는 NFC 디바이스 모듈(130)에 의해 활용되는 안테나(예컨대, 공유 안테나(shared antenna)(116) 또는 NFC-특정 안테나(134))에 전력을 공급하는 데 사용될 수 있으며, 이에 의해, 안테나가 적합한 NFC 통신 정보(예컨대, 신용 카드 크리덴셜 정보)를 NFC 데이터 모듈(132)로부터, 안테나(116) 또는 안테나(134)를 통해, 그러한 판매자 단말기로 NFC 통신으로서 송신하게 할 수 있다. 능동인 경우, NFC 디바이스 모듈(130)은 전자 디바이스(100)에 로컬인 전원(예컨대, 전원 공급 디바이스(108))을 포함하거나 그렇지 않으면 그에 대한 액세스를 가질 수 있으며, 이는 공유 안테나(116) 또는 NFC-특정 안테나(134)가, 수동 NFC 디바이스 모듈(130)의 경우에서와 같이 무선 주파수 신호들을 반사하기보다는, NFC 통신 정보(예컨대, 신용 카드 크리덴셜 정보)를 NFC 데이터 모듈(132)로부터, 안테나(116) 또는 안테나(134)를 통해, 판매자 단말기(220)로 NFC 통신으로서 능동적으로 송신하게 할 수 있다. 판매자 단말기(220)는 (예컨대, 상점에 있는 디바이스(100')의 사용자에게 제품들 또는 서비스들을 직접 판매하기 위한 판매자의 상점에서) 판매자 서브시스템(200)의 판매자에 의해 제공될 수 있다. NFC 컴포넌트(120)가 근거리 통신에 관하여 기술되었지만, 컴포넌트(120)는 전자 디바이스(100)와 그러한 판매자 단말기 사이의 임의의 적합한 비접촉식 근접-기반 모바일 결제 또는 임의의 다른 적합한 유형의 비접촉식 근접-기반 통신을 제공하도록 구성될 수 있다는 것이 이해되어야 한다. 예를 들어, NFC 컴포넌트(120)는 전자기/정전기 커플링 기술들을 수반하는 것들과 같은 임의의 적합한 단거리 통신을 제공하도록 구성될 수 있다.

[0138] NFC 컴포넌트(120)가 근거리 통신에 관하여 기술되었지만, 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200) 사이의 임의의 적합한 비접촉식 근접-기반 모바일 결제 또는 임의의 다른 적합한 유형의 비접촉식 근접-기반 통신을 제공하도록 구성될 수 있다는 것이 이해되어야 한다. 예를 들어, NFC 컴포넌트(120)는 전자기/정전기 커플링 기술들을 수반하는 것들과 같은 임의의 적합한 단거리 통신을 제공하도록 구성될 수 있다. 또한, 일부 실시예들에서, 클라이언트 디바이스(100')의 NFC 컴포넌트(120')는 호스트 디바이스(100)의 NFC 컴포넌트(120)와 동일하거나 실질적으로 동일할 수 있다. 대안적으로, 일부 실시예들에서, 클라이언트 디바이스(100')의 NFC 컴포넌트(120')는 클라이언트 디바이스(100')의 NFC 컴포넌트(120')와 판매자 서브시스템(200)의 판매자 단말기(220) 사이에서 프로세서(102') 또는 디바이스(100')의 임의의 다른 부분에 이용가능한 데이터가 임의의 적합한 비접촉식 근접-기반 통신으로 통신되도록 인에이블하기 위한 임의의 적합한 컴포넌트들을 포함하도록 구성될 수 있으나, NFC 컴포넌트(120')는 호스트 디바이스(100)에 네이티브한 크리덴셜 데이터와 같은 금융 거래를 안전하게 지불하기 위해 클라이언트 디바이스(100') 상에 보안 크리덴셜 데이터를 생성하기 위한 크리덴셜 애플릿을 안전하게 저장하는 보안 요소를 포함하거나 포함하지 않을 수 있다.

[0139] 전자 디바이스(100)에는 또한, 디바이스(100) 외부의 잔해물 및 다른 분해하는 힘들로부터의 보호를 위해 디바이스(100)의 컴포넌트들 중 하나 이상을 적어도 부분적으로 둘러쌀 수 있는 하우징(101)이 제공될 수 있다. 일부 실시예들에서, 컴포넌트들 중 하나 이상이 자신의 하우징 내에 제공될 수 있다(예컨대, 입력 컴포넌트(110)는, 자신의 하우징 내에 제공될 수 있는 프로세서(102)와 무선으로 또는 와이어를 통해 통신할 수 있는 자신의 하우징 내의 독립적 키보드 또는 마우스일 수 있다). 임의의 클라이언트 디바이스(100')는 전자 디바이스(100)와 관련하여 설명된 특징들 중 하나, 일부 또는 전부를 포함할 수 있고/있거나 전자 디바이스(100)와 관련하여 설명되지 않은 추가 특징들을 포함할 수 있음을 이해해야 한다. 또한, 임의의 호스트 디바이스(100) 또는 임의의 클라이언트 디바이스(100')는 서로 공조하여 동작하는 2개 이상의 디바이스(예컨대, 임의의 적합한 근접 통신 프로토콜(예컨대, 블루투스™)을 통해 통신가능하게 연결된 셀룰러 전화와 스마트 시계)의 조합으로서 제공될 수 있다.

[0140] 언급한 바와 같이, 그리고 도 3에 도시된 바와 같이, 전자 디바이스(100)의 하나의 특정 예는 아이폰™과 같은 핸드헬드 전자 디바이스일 수 있으며, 여기서 하우징(101)은 다양한 입력 컴포넌트(110a 내지 110i), 다양한 출력 컴포넌트(112a 내지 112c), 및 디바이스(100)와 사용자 및/또는 주변 환경이 그것을 통해 서로 인터페이스할 수 있는 다양한 I/O 컴포넌트(114a 내지 114d)에 대한 액세스를 허용할 수 있다. 입력 컴포넌트(110a)는, 눌러질 때, "홈" 스크린 또는 현재 실행중인 애플리케이션의 메뉴가 디바이스(100)에 의해 디스플레이되게 할 수 있

는 버튼을 포함할 수 있다. 입력 컴포넌트(110b)는 슬립 모드와 웨이크 모드 사이에서 또는 임의의 다른 적합한 모드들 사이에서 전자 디바이스(100)를 토글하기 위한 버튼일 수 있다. 입력 컴포넌트(110c)는 전자 디바이스(100)의 소정 모드들에서 하나 이상의 출력 컴포넌트(112)를 디스에이블할 수 있는 2-위치 슬라이더를 포함할 수 있다. 입력 컴포넌트들(110d, 110e)은 음량 출력 또는 전자 디바이스(100)의 출력 컴포넌트(112)의 임의의 다른 특성 출력을 증가 및 감소시키기 위한 버튼들을 포함할 수 있다. 입력 컴포넌트들(110a 내지 110e) 각각은 기계적 입력 컴포넌트, 예컨대 돔 스위치에 의해 지지되는 버튼, 슬라이딩 스위치, 제어 패드, 키, 노브(knob), 스크롤 휠, 또는 임의의 다른 적합한 형태일 수 있다.

[0141] 출력 컴포넌트(112a)는 시각적 또는 그래픽 사용자 인터페이스("GUI")(180)를 디스플레이하는 데 사용될 수 있는 디스플레이일 수 있으며, 이는 사용자가 전자 디바이스(100)와 상호작용하게 할 수 있다. GUI(180)는, 디스플레이 출력 컴포넌트(112a)의 영역들 전체 또는 일부에 디스플레이될 수 있는, 다양한 계층, 윈도우, 스크린, 템플릿, 요소, 메뉴, 및/또는 현재 실행중인 애플리케이션(예컨대, 애플리케이션(103) 및/또는 애플리케이션(113) 및/또는 애플리케이션(143))의 다른 컴포넌트들을 포함할 수 있다. 예를 들어, 도 3에 도시된 바와 같이, GUI(180)는 제1 스크린(190)을 디스플레이하도록 구성될 수 있다. 사용자 입력 컴포넌트들(110a 내지 110i) 중 하나 이상이 GUI(180)를 통해 내비게이션하는 데 사용될 수 있다. 예를 들어, 하나의 사용자 입력 컴포넌트(110)는 사용자가 GUI(180)의 하나 이상의 그래픽 요소 또는 아이콘(182)을 선택하게 할 수 있는 스크롤 휠을 포함할 수 있다. 아이콘들(182)은 또한 디스플레이 출력 컴포넌트(112a) 및 연관된 터치 입력 컴포넌트(110f)를 포함할 수 있는 터치 스크린 I/O 컴포넌트(114a)를 통해 선택될 수 있다. 그러한 터치 스크린 I/O 컴포넌트(114a)는 저항성, 용량성, 적외선, 표면 탄성과, 전자기적, 또는 근거리 이미징과 같은, 그러나 이들로 제한되지 않는 임의의 적합한 유형의 터치 스크린 입력 기술을 채용할 수 있다. 또한, 터치 스크린 I/O 컴포넌트(114a)는 단일 지점 또는 다중-지점(예컨대, 다중-터치) 입력 감지를 채용할 수 있다.

[0142] 아이콘들(182)은 사용자의 선택 시 디스플레이 컴포넌트(112a)의 영역들의 일부 또는 전체에 디스플레이될 수 있는 다양한 계층, 윈도우, 스크린, 템플릿, 요소, 및/또는 다른 컴포넌트들을 표현할 수 있다. 또한, 특정 아이콘(182)의 선택은 계층적 내비게이션 프로세스로 이어질 수 있다. 예를 들어, 특정 아이콘(182)의 선택은, 동일한 애플리케이션의 또는 그 아이콘(182)과 연관된 새로운 애플리케이션의 하나 이상의 추가적인 아이콘 또는 다른 GUI 요소를 포함할 수 있는, GUI(180)의 새로운 스크린으로 이어질 수 있다. 텍스트 표시자들(181)은 각각의 그래픽 요소 아이콘(182)의 사용자 해석을 용이하게 하기 위해 각각의 아이콘(182) 상에 또는 그 근처에 디스플레이될 수 있다. GUI(180)가 계층적 및/또는 비-계층적 구조들로 배열된 다양한 컴포넌트를 포함할 수 있다는 것이 이해될 것이다. 특정 아이콘(182)이 선택되면, 디바이스(100)는 그 아이콘(182)과 연관된 새로운 애플리케이션을 열고 그 애플리케이션과 연관된 GUI(180)의 대응하는 스크린을 디스플레이하도록 구성될 수 있다. 예를 들어, "판매자 앱" 텍스트 표시자(181)로 라벨링된 특정 아이콘(182)(즉, 특정 아이콘(183))이 선택되면, 디바이스(100)는 특정 판매자 애플리케이션을 시작하거나 그렇지 않으면 그것에 액세스할 수 있고, 특정 방식으로 디바이스(100)와 상호작용하기 위한 하나 이상의 툴 또는 특징부를 포함할 수 있는 특정 사용자 인터페이스의 스크린들을 디스플레이할 수 있다. 각각의 애플리케이션에 대해, 스크린은 디스플레이 출력 컴포넌트(112a) 상에 디스플레이될 수 있고 다양한 사용자 인터페이스 요소(예컨대, 도 3a 내지 도 3h의 스크린(190a 내지 190h))를 포함할 수 있다. 부가적으로 또는 대안적으로, 각각의 애플리케이션에 대해, 다양한 다른 유형들의 비-시각적 정보가 디바이스(100)의 다양한 다른 출력 컴포넌트(112)를 통해 사용자에게 제공될 수 있다. 다양한 GUI(180)에 관하여 기술된 동작들은 매우 다양한 그래픽 요소 및 시각적 기법으로 달성될 수 있다. 따라서, 기술된 실시예들은 본 명세서에서 채택된 정확한 사용자 인터페이스 규약으로 제한되도록 의도되지 않는다. 오히려, 실시예들은 매우 다양한 사용자 인터페이스 양식을 포함할 수 있다.

[0143] 전자 디바이스(100)는 또한 디바이스(100)와 다른 디바이스들 사이의 통신을 허용할 수 있는 다양한 다른 I/O 컴포넌트(114)를 포함할 수 있다. I/O 컴포넌트(114b)는, 원격 데이터 소스로부터 미디어 파일들 또는 고객 주문 파일들과 같은 데이터 파일들을, 그리고/또는 외부 전원으로부터 전력을 송신하고 수신하도록 구성될 수 있는 접속 포트일 수 있다. 예를 들어, I/O 컴포넌트(114b)는 미국 캘리포니아주 쿠퍼티노 소재의 애플 인크.의 라이트닝(Lightning)TM 커넥터 또는 30-핀 도크 커넥터와 같은 전매 포트일 수 있다. I/O 컴포넌트(114c)는 SIM 카드 또는 임의의 다른 유형의 탈착가능한 컴포넌트를 수용하기 위한 접속 슬롯일 수 있다. I/O 컴포넌트(114d)는 마이크로폰 컴포넌트를 포함하거나 포함하지 않을 수 있는 오디오 헤드폰들을 접속하기 위한 헤드폰 잭일 수 있다. 전자 디바이스(100)는 또한 마이크로폰과 같은 적어도 하나의 오디오 입력 컴포넌트(110g), 및 오디오 스피커와 같은 적어도 하나의 오디오 출력 컴포넌트(112b)를 포함할 수 있다.

[0144] 전자 디바이스(100)는 또한, 적어도 하나의 햅틱 또는 촉각적 출력 컴포넌트(112c)(예컨대, 럼블러), 카메라 및

/또는 스캐너 입력 컴포넌트(110h)(예컨대, 비디오 또는 스틸 카메라, 및/또는 바코드 스캐너 또는 바코드, QR 코드 등과 같은 코드로부터 제품 식별 정보를 획득할 수 있는 임의의 다른 적합한 스캐너), 및 생체인식 입력 컴포넌트(110i)(예컨대, 사용자를 인증하기 위해 전자 디바이스(100)에 액세스가능할 수 있는 특징-프로세싱 애플리케이션과 공조하여 동작할 수 있는, 지문 판독기 또는 다른 특징 인식 센서)를 포함할 수 있다. 도 3에 도시된 바와 같이, 생체인식 입력 컴포넌트(110i)의 적어도 일부는 입력 컴포넌트(110a) 또는 디바이스(100)의 임의의 다른 적합한 입력 컴포넌트(110) 내에 통합되거나 그렇지 않으면 그와 조합될 수 있다. 예를 들어, 생체인식 입력 컴포넌트(110i)는, 사용자가 사용자의 손가락으로 입력 컴포넌트(110a)를 누름으로써 기계적 입력 컴포넌트(110a)와 상호작용할 때 그 손가락의 지문을 스캔하도록 구성될 수 있는 지문 판독기일 수 있다. 다른 예로서, 생체인식 입력 컴포넌트(110i)는 터치 스크린 I/O 컴포넌트(114a)의 터치 입력 컴포넌트(110f)와 조합될 수 있는 지문 판독기일 수 있어서, 사용자가 사용자의 손가락으로 터치 스크린 입력 컴포넌트(110f)를 누르거나 그것을 따라 슬라이딩함으로써 터치 스크린 입력 컴포넌트(110f)와 상호작용할 때 그 생체인식 입력 컴포넌트(110i)가 그 손가락의 지문을 스캔하도록 구성될 수 있다. 또한, 언급된 바와 같이, 전자 디바이스(100)는, 안테나(116) 및/또는 안테나(134)(도 3에 도시되지 않음)를 통해 서브시스템(200)에 통신가능하게 액세스할 수 있는 NFC 컴포넌트(120)를 추가로 포함할 수 있다. NFC 컴포넌트(120)는 적어도 부분적으로 하우스징(101) 내에 위치될 수 있고, 마크 또는 심볼(121)이 하우스징(101)의 외부 상에 제공될 수 있어서, NFC 컴포넌트(120)와 연관된 안테나들 중 하나 이상의 안테나의 일반적 위치(예컨대, 안테나(116) 및/또는 안테나(134)의 일반적 위치)를 식별할 수 있다.

[0145] 도 1 내지 도 10에 관하여 기술된 프로세스들 중 하나, 일부, 또는 모두는 각각 소프트웨어에 의해 구현될 수 있지만, 또한 하드웨어, 펌웨어, 또는 소프트웨어, 하드웨어, 및 펌웨어의 임의의 조합으로 구현될 수 있다. 이들 프로세스를 수행하기 위한 명령어들은 또한 기계 또는 컴퓨터 판독가능 매체 상에 기록되는 기계 또는 컴퓨터 판독가능 코드로서 구현될 수 있다. 일부 실시예들에서, 컴퓨터 판독가능 매체는 비일시적 컴퓨터 판독가능 매체일 수 있다. 그러한 비일시적 컴퓨터 판독가능 매체의 예들은, 판독 전용 메모리, 랜덤 액세스 메모리, 플래시 메모리, CD-ROM, DVD, 자기 테이프, 탈착가능한 메모리 카드, 및 데이터 저장 디바이스(예컨대, 도 2의 메모리(104) 및/또는 메모리 모듈(150))를 포함하지만 이들로 제한되지 않는다. 다른 실시예들에서, 컴퓨터 판독가능 매체는 일시적 컴퓨터 판독가능 매체일 수 있다. 그러한 실시예들에서, 일시적 컴퓨터 판독가능 매체는 컴퓨터 판독가능 코드가 분산 방식으로 저장되고 실행되도록 네트워크로 연결된 컴퓨터 시스템들에 걸쳐 분산되어 있을 수 있다. 예를 들어, 그러한 일시적 컴퓨터 판독가능 매체는 임의의 적합한 통신 프로토콜을 사용하여 한 전자 디바이스로부터 다른 전자 디바이스로 전달될 수 있다(예컨대, 컴퓨터 판독가능 매체는 통신 컴포넌트(106)를 통해 전자 디바이스(100)로(예컨대, 애플리케이션(103)의 적어도 일부분으로서 그리고/또는 애플리케이션(113)의 적어도 일부분으로서 그리고/또는 애플리케이션(143)의 적어도 일부분으로서) 전달될 수 있다). 그러한 일시적 컴퓨터 판독가능 매체는 컴퓨터 판독가능 코드, 명령어들, 데이터 구조들, 프로그램 모듈들, 또는 다른 데이터를 반송파 또는 다른 전송 매커니즘과 같은 변조된 데이터 신호에서 구현할 수 있으며, 임의의 정보 전달 매체를 포함할 수 있다. 변조된 데이터 신호는, 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호일 수 있다.

[0146] 시스템(1)의 임의의, 각각의, 또는 적어도 하나의 모듈 또는 컴포넌트 또는 서브시스템은 소프트웨어 구조, 펌웨어 구조, 하나 이상의 하드웨어 컴포넌트, 또는 이들의 조합으로 제공될 수 있다는 것이 이해되어야 한다. 예를 들어, 시스템(1)의 임의의, 각각의, 또는 적어도 하나의 모듈 또는 컴포넌트 또는 서브시스템은, 하나 이상의 컴퓨터 또는 다른 디바이스들에 의해 실행될 수 있는 프로그램 모듈들과 같은 컴퓨터 실행가능 명령어들의 일반적 맥락으로 기술될 수 있다. 일반적으로, 프로그램 모듈은 하나 이상의 특정한 태스크를 수행할 수 있거나 하나 이상의 특정한 추상 데이터 형을 구현할 수 있는 하나 이상의 루틴, 프로그램, 객체, 컴포넌트, 및/또는 데이터 구조를 포함할 수 있다. 시스템(1)의 모듈들 및 컴포넌트들 및 서브시스템들의 수, 구성, 기능, 및 상호접속은 단지 예시적인 것이며, 기존 모듈들, 컴포넌트들 및/또는 서브시스템들의 수, 구성, 기능, 및 상호접속이 수정되거나 생략될 수 있고, 추가적인 모듈들, 컴포넌트들 및/또는 서브시스템들이 추가될 수 있으며, 소정 모듈들, 컴포넌트들 및/또는 서브시스템들의 상호접속이 변경될 수 있다는 것이 또한 이해될 것이다.

[0147] 시스템(1)의 모듈들 또는 컴포넌트들 또는 서브시스템들 중 하나 이상의 적어도 일부는, 임의의 적합한 방식으로(예컨대, 디바이스(100)의 메모리(104) 내에(예컨대, 애플리케이션(103)의 적어도 일부분으로서 그리고/또는 애플리케이션(113)의 적어도 일부분으로서 그리고/또는 애플리케이션(143)의 적어도 일부분으로서)) 시스템(1)의 엔티티에 저장되거나 그렇지 않으면 그에 액세스가능할 수 있다. 예를 들어, NFC 컴포넌트(120)의 임의의 또는 각각의 모듈은 임의의 적합한 기술들을 사용하여(예컨대, 하나 이상의 집적회로 디바이스로서) 구현될 수 있으며, 상이한 모듈들이 구조, 기능들, 및 동작에 있어서 동일하거나 동일하지 않을 수 있다. 시스템(1)의

모듈들 또는 다른 컴포넌트들 중 임의의 것 또는 모두는, 확장 카드 상에 장착되거나, 시스템 마더보드 상에 직접 장착되거나, 또는 시스템 칩셋 컴포넌트 내에(예컨대, "노스 브리지(north bridge)" 칩 내에) 통합될 수 있다.

[0148] 시스템(1)의 임의의 또는 각각의 모듈 또는 컴포넌트(예컨대, NFC 컴포넌트(120)의 임의의 또는 각각의 모듈)는 다양한 버스 표준에 맞춰진 하나 이상의 확장 카드를 사용하여 구현되는 전용 시스템일 수 있다. 예를 들어, 모듈들 모두는 상이한 상호접속된 확장 카드들 상에 장착될 수 있거나, 모듈들 모두가 하나의 확장 카드 상에 장착될 수 있다. NFC 컴포넌트(120)에 관하여, 단지 예로서, NFC 컴포넌트(120)의 모듈들은, 확장 슬롯(예컨대, 주변장치 상호접속(peripheral component interconnect, "PCI") 슬롯 또는 PCI 익스프레스 슬롯)을 통해 디바이스(100)의 프로세서(102) 또는 마더보드와 인터페이싱할 수 있다. 대안적으로, NFC 컴포넌트(120)는 탈착가능할 필요는 없으며, 모듈의 활용에 전용되는 메모리(예컨대, RAM)를 포함할 수 있는 하나 이상의 전용 모듈을 포함할 수 있다. 다른 실시예들에서, NFC 컴포넌트(120)는 디바이스(100) 내에 통합될 수 있다. 예를 들어, NFC 컴포넌트(120)의 모듈은 디바이스(100)의 디바이스 메모리(104)의 일부분을 활용할 수 있다. 시스템(1)의 임의의 또는 각각의 모듈 또는 컴포넌트(예컨대, NFC 컴포넌트(120)의 임의의 또는 각각의 모듈)는 자신의 프로세싱 회로 및/또는 메모리를 포함할 수 있다. 대안적으로, 시스템(1)의 임의의 또는 각각의 모듈 또는 컴포넌트(예컨대, NFC 컴포넌트(120)의 임의의 또는 각각의 모듈)는, NFC 컴포넌트(120)의 임의의 다른 모듈 및/또는 디바이스(100)의 프로세서(102) 및/또는 메모리(104)와, 프로세싱 회로 및/또는 메모리를 공유할 수 있다.

[0149] 언급한 바와 같이, 디바이스(100)의 입력 컴포넌트(110)(예컨대, 입력 컴포넌트(110f))는, 유선 또는 무선 버스(118)를 통해 디바이스(100)의 다른 컴포넌트들과 상호작용하기 위해 터치 입력을 수신할 수 있는 터치 입력 컴포넌트를 포함할 수 있다. 그러한 터치 입력 컴포넌트(110)는, 키보드, 마우스 등과 같은 다른 입력 컴포넌트들을 대신하여 또는 그것들과 조합하여 사용자 입력을 디바이스(100)에 제공하는 데 사용될 수 있다.

[0150] 터치 입력 컴포넌트(110)는 전체적으로 또는 부분적으로 투명한, 반투명한, 불투명한, 또는 이들의 임의의 조합일 수 있는 터치 감응형 패널을 포함할 수 있다. 터치 입력 컴포넌트(110)는 터치 스크린, 터치 패드, 터치 패드로서 기능하는 터치 스크린(예컨대, 랩톱의 터치 패드를 대체하는 터치 스크린), 임의의 다른 입력 디바이스와 조합되거나 통합된 터치 스크린 또는 터치 패드(예컨대, 키보드 상에 배치된 터치 스크린 또는 터치 패드), 또는 터치 입력을 수신하기 위한 터치 감응형 표면을 갖는 임의의 다차원 물체로 구현될 수 있다. 일부 실시예들에서, 터치 스크린 및 터치 패드라는 용어들은 상호교환가능하게 사용될 수 있다.

[0151] 일부 실시예들에서, 터치 스크린으로서 구현되는 터치 입력 컴포넌트(110)는 디스플레이의 적어도 일부분 위에, 아래에, 그리고/또는 그 내에 부분적으로 또는 전체적으로 위치하는 투명한 그리고/또는 반투명한 터치 감응형 패널을 포함할 수 있다(예컨대, 디스플레이 출력 컴포넌트(112a)). 다른 실시예들에서, 터치 입력 컴포넌트(110)는, 터치 감응형 컴포넌트들/디바이스들이 디스플레이 컴포넌트들/디바이스들과 통합되는, 통합형 터치 스크린으로서 구현될 수 있다. 또 다른 실시예들에서, 터치 입력 컴포넌트(110)는, 보충적인 그래픽 데이터 또는 주 디스플레이와 동일한 그래픽 데이터를 디스플레이하기 위한 보충적인 또는 추가적인 디스플레이 스크린으로서 그리고 터치 입력을 수신하는 데 사용될 수 있다.

[0152] 터치 입력 컴포넌트(110)는, 용량성, 저항성, 광학적, 음향적, 유도성, 기계적, 화학적 측정, 또는 입력 컴포넌트(110)에 근접한 하나 이상의 터치 혹은 준터치(near touch)의 발생들에 대하여 측정될 수 있는 임의의 현상에 기초하여, 하나 이상의 터치 또는 준터치의 위치를 검출하도록 구성될 수 있다. 소프트웨어, 하드웨어, 펌웨어 또는 이들의 임의의 조합이, 검출된 터치들의 측정들을 프로세싱하여 하나 이상의 제스처를 식별하고 추적하는 데 사용될 수 있다. 제스처는 터치 입력 컴포넌트(110) 상의 정지된 또는 정지되지 않은, 단일 또는 다중의, 터치들 또는 준터치들에 대응할 수 있다. 본질적으로 동시에, 인접하게, 또는 연속하여, 두드리거나, 누르거나, 흔들거나, 문지르거나, 회전시키거나, 비틀거나, 배향을 바꾸거나, 변화하는 압력으로 누르는 것 등에 의한 것과 같이, 터치 입력 컴포넌트(110) 상에서 특정 방식으로 하나 이상의 손가락 또는 다른 물체를 움직임으로써, 제스처가 수행될 수 있다. 제스처는, 임의의 다른 손가락 또는 손가락들을 이용하거나 그 사이의 집기(pinching), 끌어당기기(pulling), 미끄러지기(sliding), 긁기(swiping), 회전시키기(rotating), 구부리기(flexing), 끌기(dragging), 또는 두드리기 모션으로 특징될 수 있지만, 이들로 제한되지 않는다. 한 명 이상의 사용자에게 의해, 하나 이상의 손으로, 또는 임의의 이들의 조합으로, 단일 제스처가 수행될 수 있다.

[0153] 언급한 바와 같이, 전자 디바이스(100)는 디스플레이(예컨대, 디스플레이 출력 컴포넌트(112a))를 그래픽 데이터로 구동하여 그래픽 사용자 인터페이스("GUI")(180)를 디스플레이할 수 있다. GUI(180)는 터치 입력 컴포넌

트(110f)를 통해 터치 입력을 수신하도록 구성될 수 있다. (예컨대, 디스플레이 출력 컴포넌트(112a)를 I/O 컴포넌트(114a)로서 갖는) 터치 스크린으로서 구현된, 터치 I/O 컴포넌트(110f)는 GUI(180)를 디스플레이할 수 있다. 대안적으로, GUI(180)는 터치 입력 컴포넌트(110f)로부터 분리된 디스플레이(예컨대, 디스플레이 출력 컴포넌트(112a)) 상에 디스플레이될 수 있다. GUI(180)는 인터페이스 내의 특정 위치들에 디스플레이되는 그래픽 요소들을 포함할 수 있다. 그래픽 요소들은, 가상 스크롤 휠, 가상 키보드, 가상 노브, 가상 버튼, 임의의 가상 사용자 인터페이스("UI") 등을 포함하는, 다양한 디스플레이된 가상 입력 디바이스들을 포함할 수 있지만, 이들로 제한되지 않는다. 사용자는, GUI(180)의 그래픽 요소들과 연관될 수 있는, 터치 입력 컴포넌트(110f) 상의 하나 이상의 특정 위치에서 제스처들을 수행할 수 있다. 다른 실시예들에서, 사용자는 GUI(180)의 그래픽 요소들의 위치들에 독립적인 하나 이상의 위치에서 제스처들을 수행할 수 있다. 터치 입력 컴포넌트(110) 상에서 수행되는 제스처들은, 직접적으로 또는 간접적으로, GUI 내의 커서, 아이콘, 미디어 파일, 리스트, 텍스트, 이미지들의 전체 또는 부분들 등과 같은 그래픽 요소들을 조작, 제어, 수정, 이동, 작동, 개시하거나, 일반적으로 영향을 줄 수 있다. 예를 들어, 터치 스크린의 경우, 사용자는 터치 스크린 상의 그래픽 요소 위에서 제스처를 수행함으로써 그래픽 요소와 직접 상호작용할 수 있다. 대안적으로, 터치 패드는 일반적으로 간접 상호작용을 제공할 수 있다. 제스처들은 또한 디스플레이되지 않는 GUI 요소들에 영향을 줄 수 있거나(예컨대, 사용자 인터페이스들이 나타나게 함) 또는 디바이스(100)의 다른 작동들에 영향을 줄 수 있다(예컨대, GUI, 애플리케이션, 또는 운영 체제의 상태 또는 모드에 영향을 줌). 제스처들은 터치 입력 컴포넌트(110) 상에서, 디스플레이되는 커서와 공조하여 수행되거나 수행되지 않을 수 있다. 예를 들어, 제스처들이 터치패드 상에서 수행되는 경우에, 커서 또는 포인터가 디스플레이 스크린 또는 터치 스크린 상에 디스플레이될 수 있고, 커서 또는 포인터는 터치패드 상의 터치 입력을 통해 제어되어 디스플레이 스크린 상의 그래픽 객체들과 상호작용할 수 있다. 대안적으로, 제스처들이 터치 스크린 상에서 직접 수행될 때, 사용자는 터치 스크린 상에 디스플레이되는 커서 또는 포인터를 이용하여 또는 이용하지 않고 터치 스크린 상의 객체들과 직접 상호작용할 수 있다. 터치 입력 컴포넌트(110) 상의 터치 또는 준터치들에 응답하여 또는 기초하여 버스(118)를 통해 사용자에게 피드백이 제공될 수 있다. 피드백은 광학적으로, 기계적으로, 전기적으로, 후각적으로, 청각적으로 등이나, 이들의 임의의 조합으로 그리고 가변적 또는 비가변적 방식으로 송신될 수 있다.

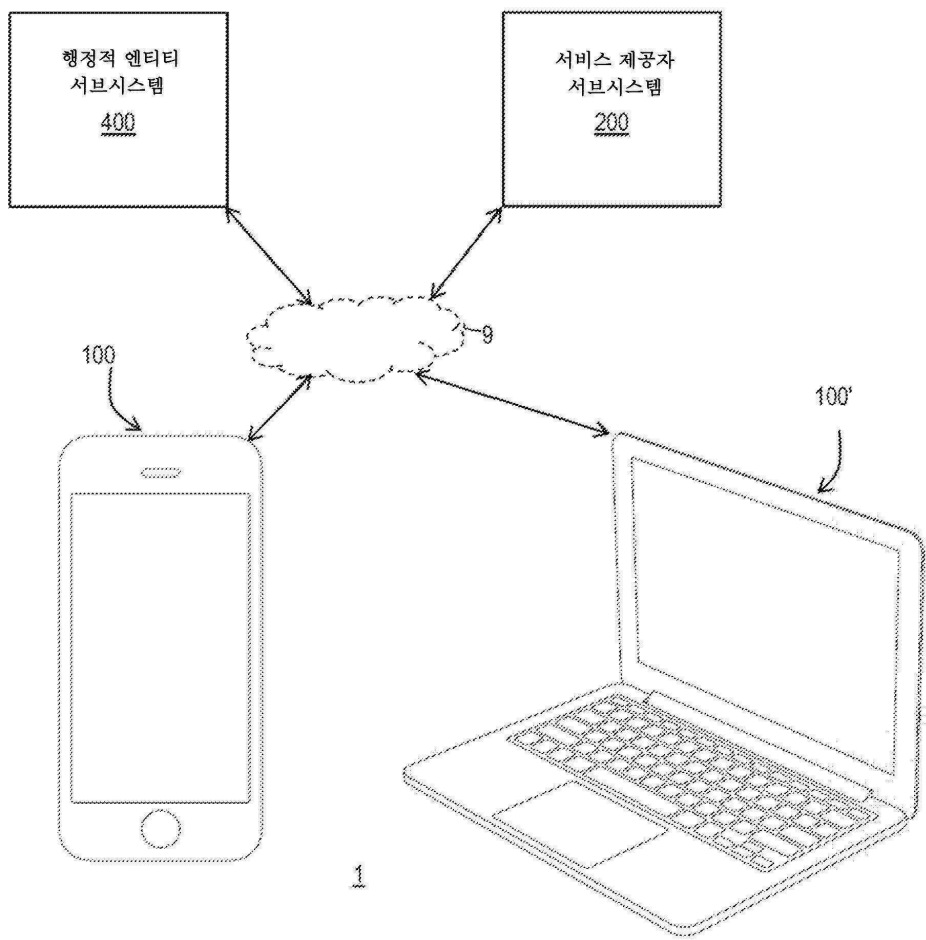
[0154] 설명된 개념들의 추가 애플리케이션들

[0155] 비-네이티브 크리덴셜과 함께 전자 디바이스를 사용하여 거래를 수행하기 위한 시스템, 방법 및 컴퓨터-판독가능 매체가 설명되었지만, 어떤 식으로든 본 명세서에 기술된 주제의 기술적 사상 및 범주로부터 벗어나지 않으면서 본 명세서에서 많은 변경들이 행해질 수 있다는 것이 이해되어야 한다. 현재 알려져 있거나 추후에 고안되는, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자의 관점에서 보아 청구된 주제로부터의 비실질적인 변경들은, 청구범위의 범주 내에 동등하게 있는 것으로 명백히 고려된다. 따라서, 현재 또는 추후에 통상의 기술자에게 알려지는 명확한 대안물들이, 정의된 요소들의 범주 내에 있는 것으로 규정된다.

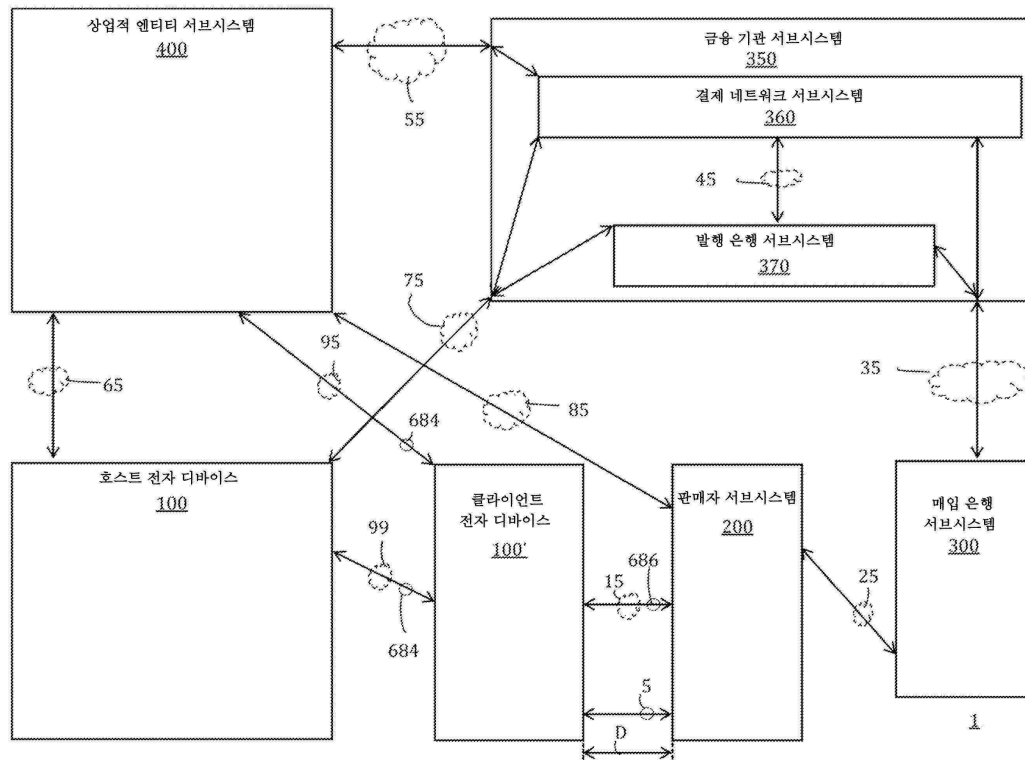
[0156] 따라서, 이들 통상의 기술자는, 본 발명이, 제한이라기보다는 예시의 목적으로 제시되는, 기술된 실시예들 이외의 것에 의해 실시될 수 있다는 것을 이해할 것이다.

도면

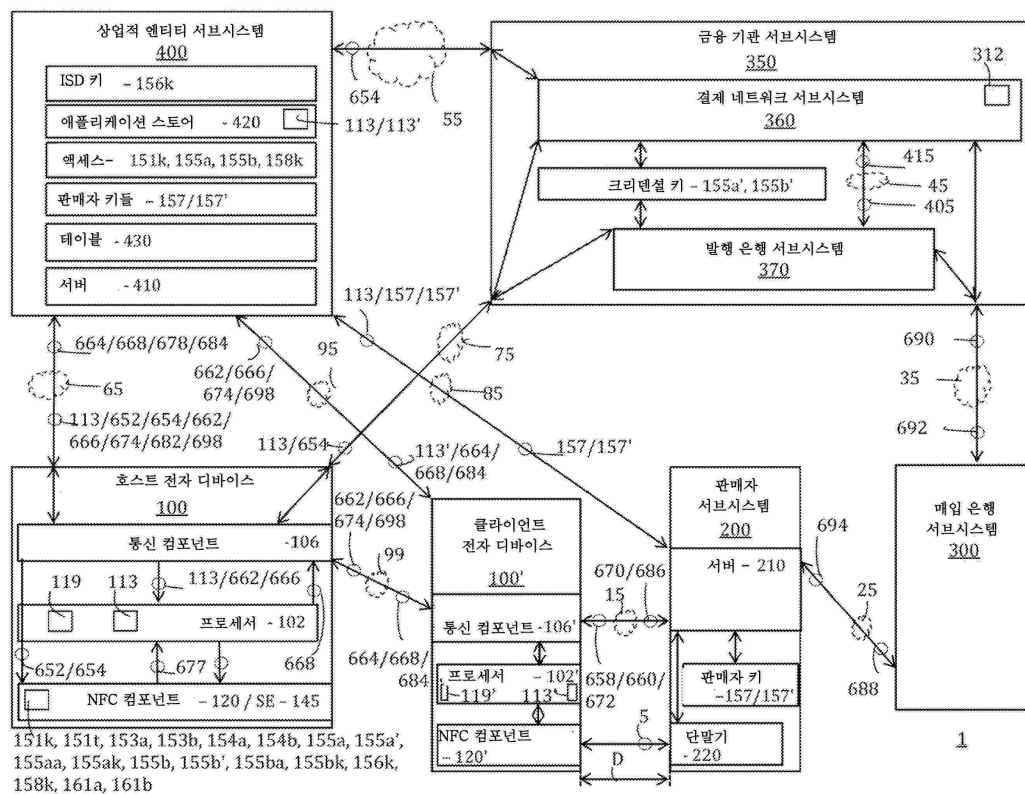
도면1



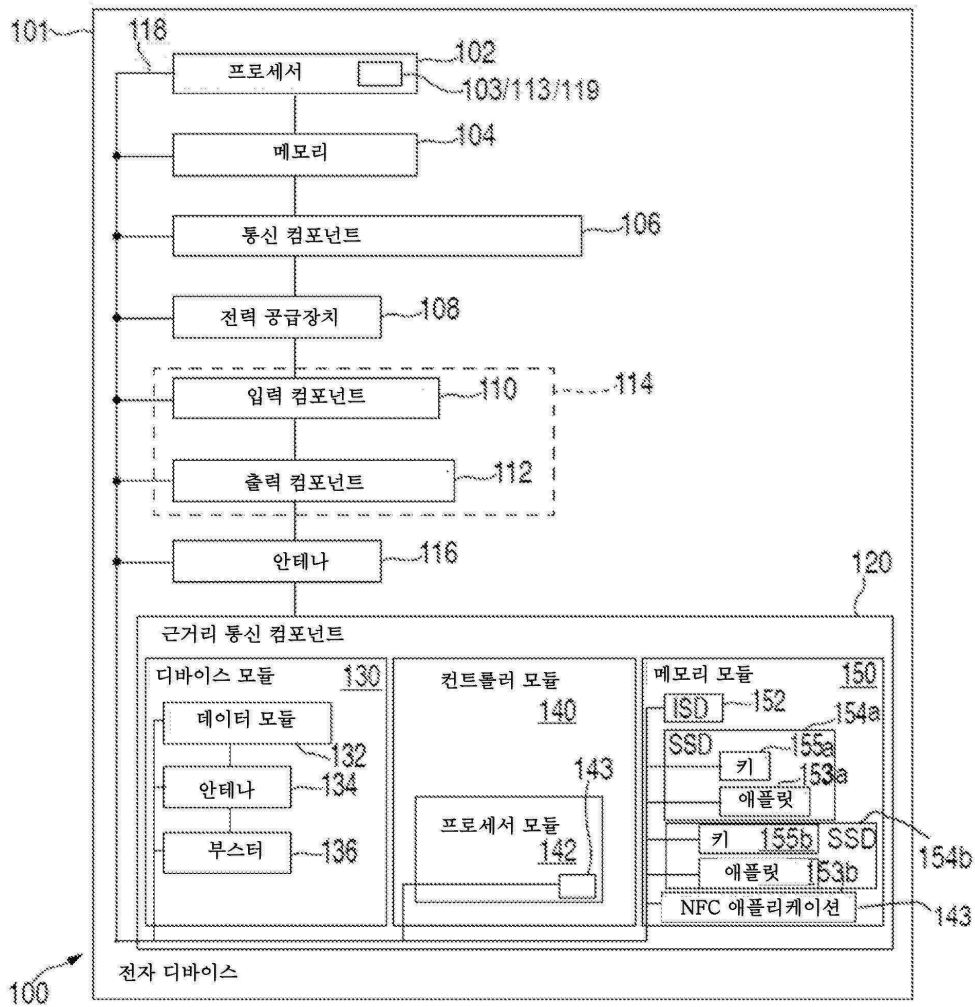
도면1a



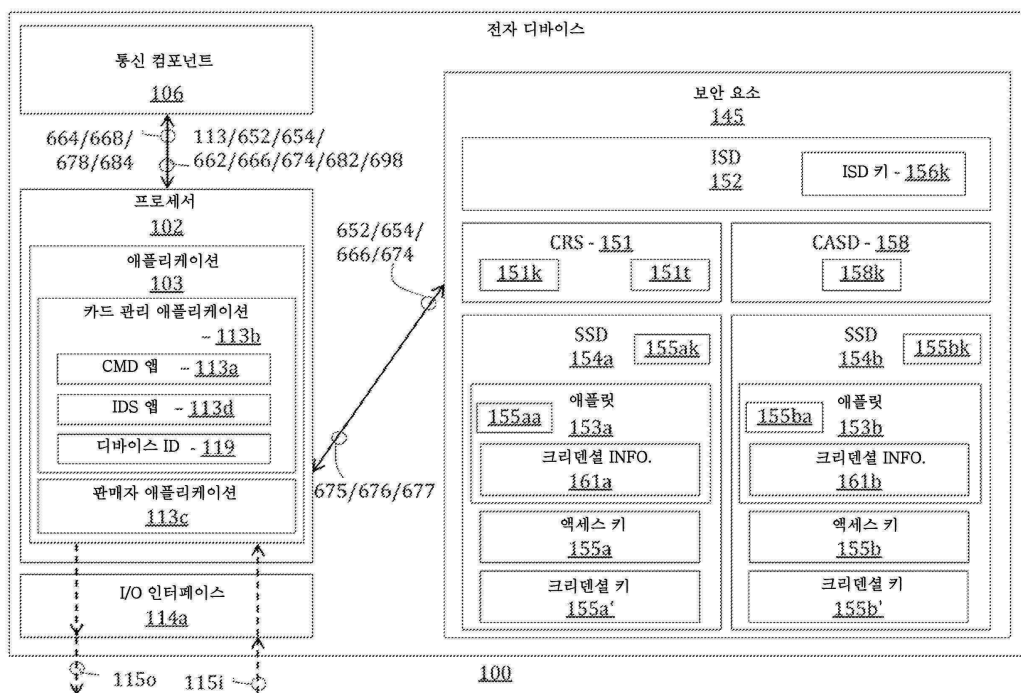
도면1b



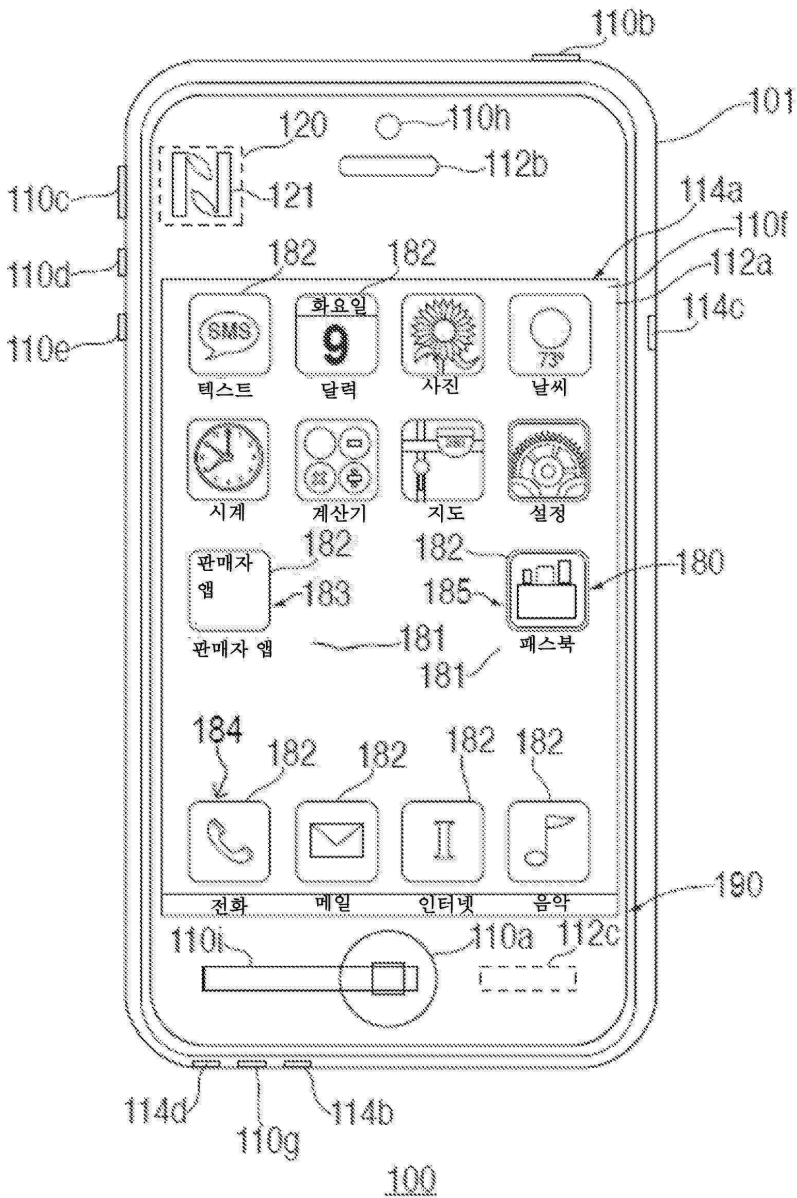
도면2



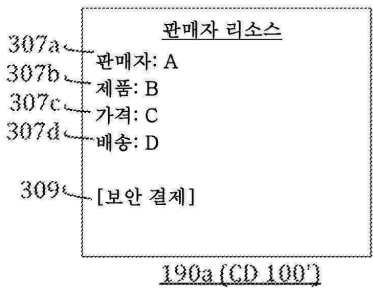
도면2a



도면3



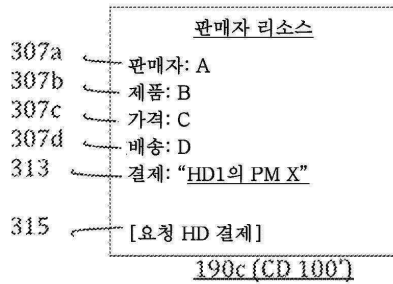
도면3a



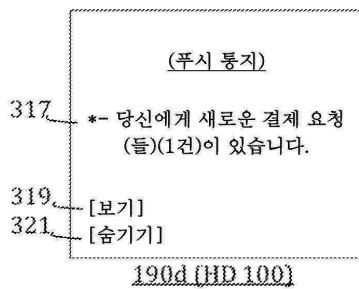
도면3b



도면3c



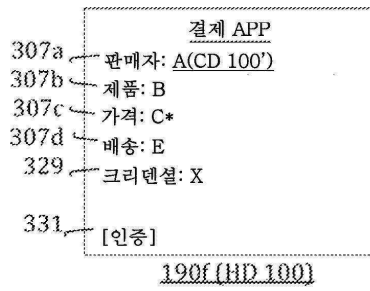
도면3d



도면3e



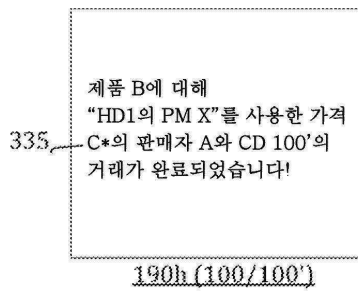
도면3f



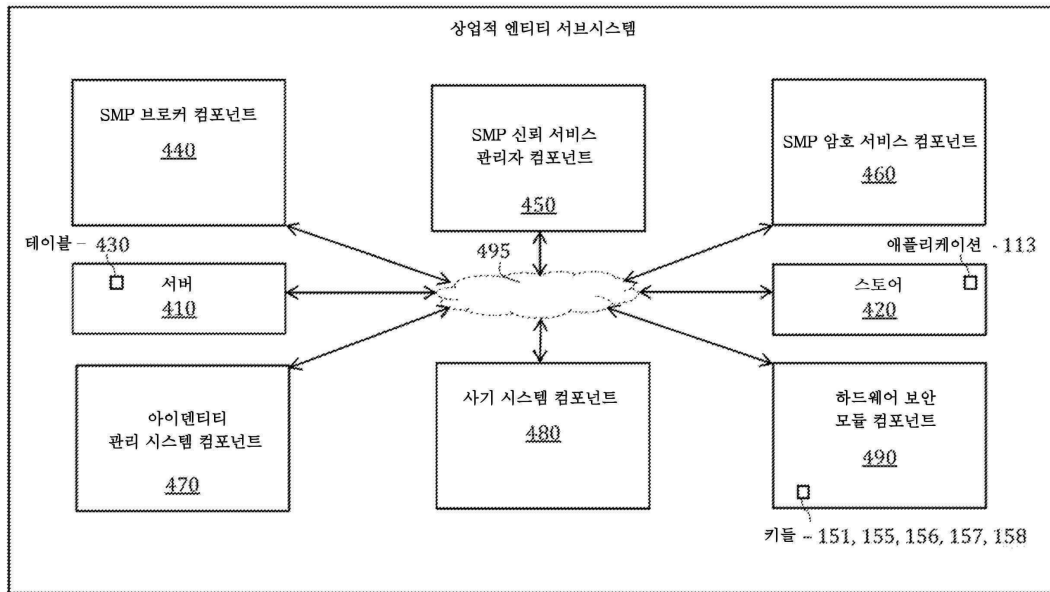
도면3g



도면3h

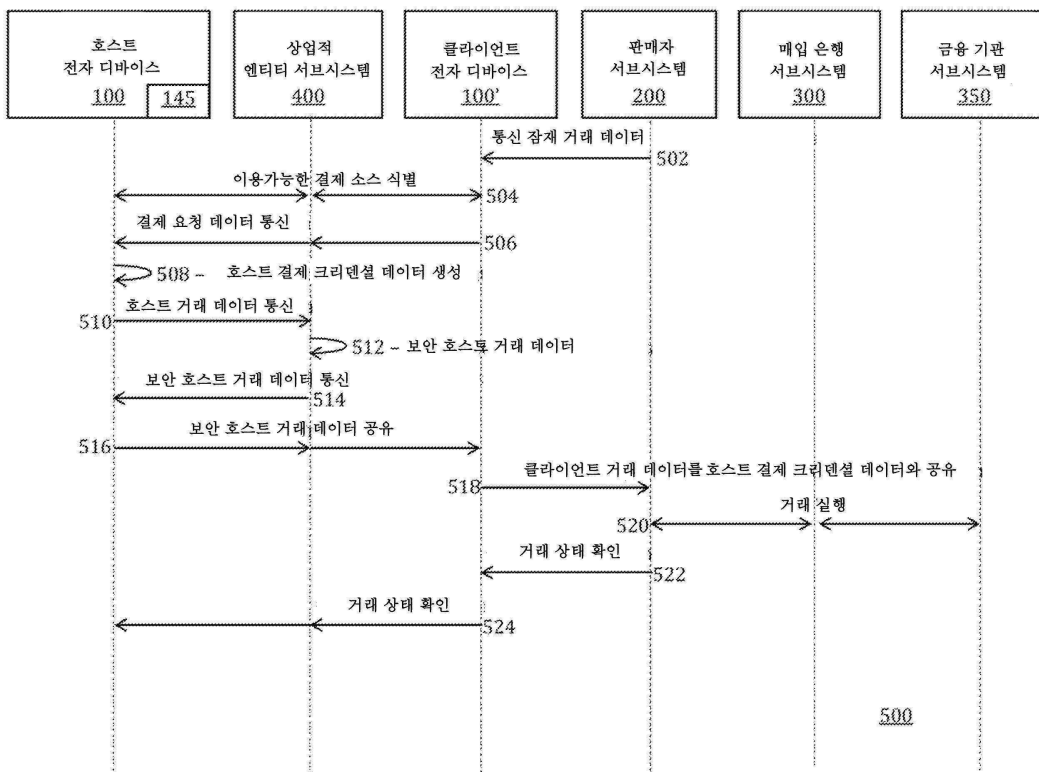


도면4

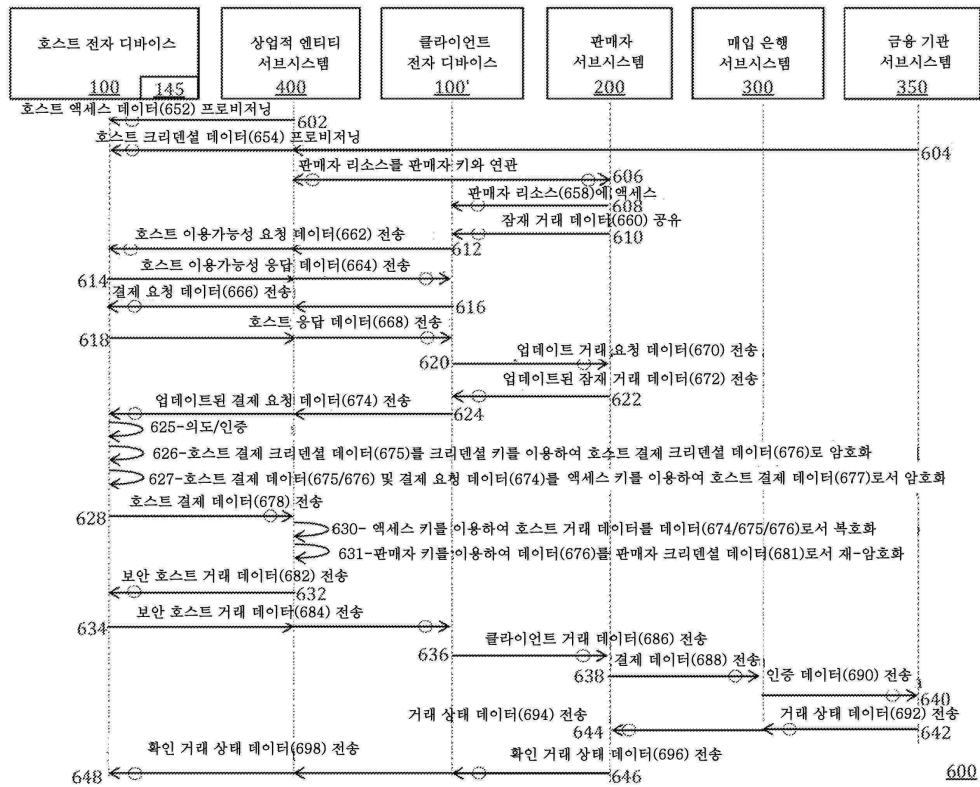


400

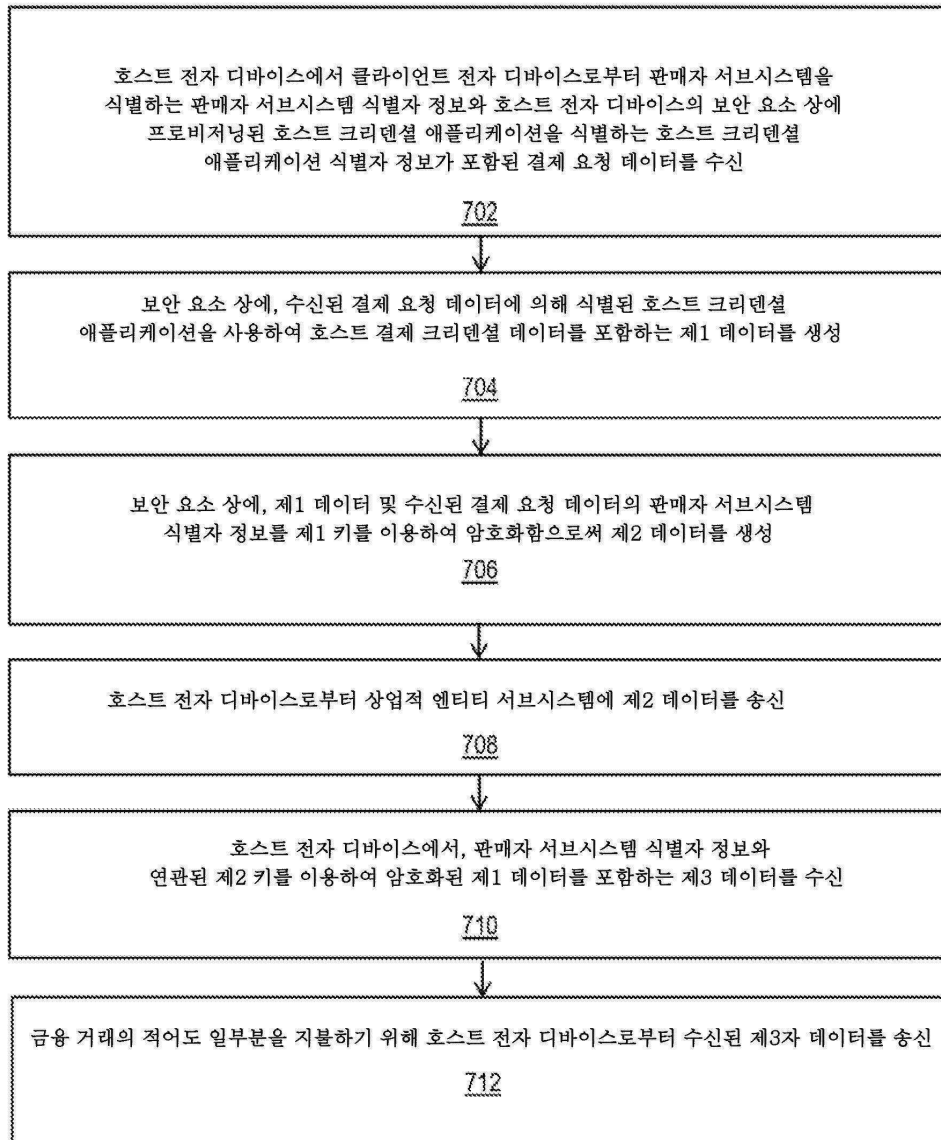
도면5



도면6

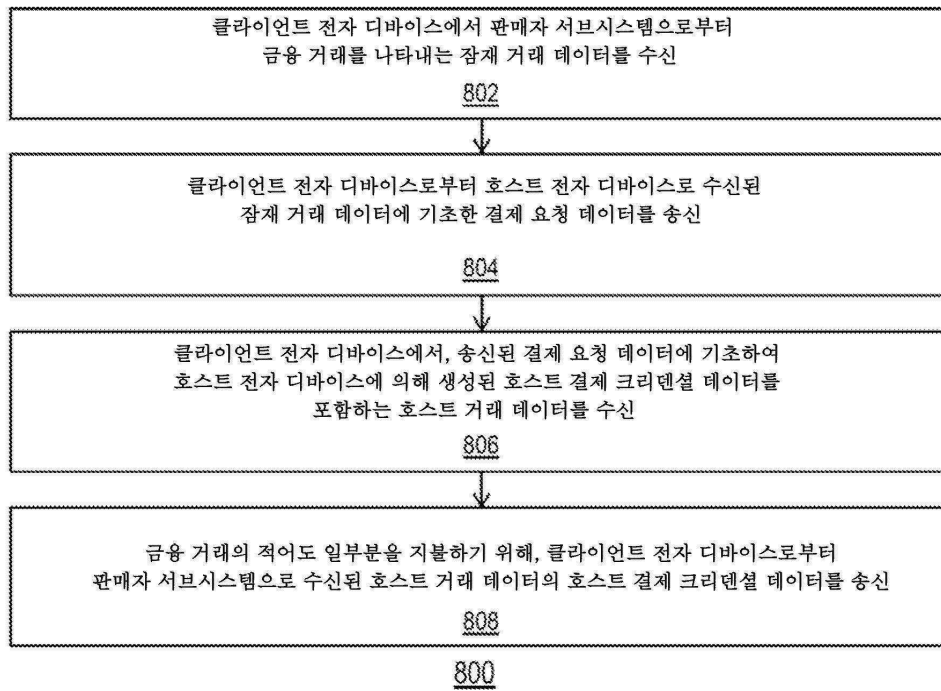


도면7

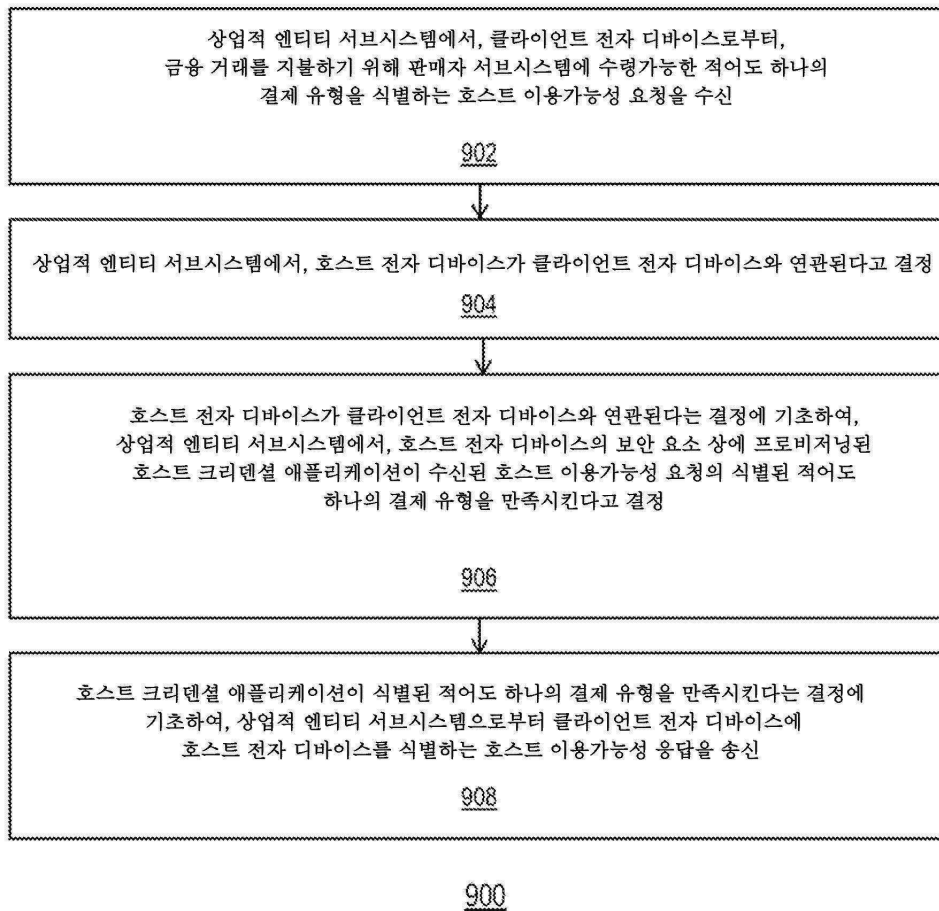


700

도면8



도면9



도면10

