



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2021년03월26일

(11) 등록번호 10-2232649

(24) 등록일자 2021년03월22일

(51) 국제특허분류(Int. Cl.)

G06Q 20/38 (2012.01) G06Q 20/12 (2012.01)

G06Q 20/32 (2012.01) H04L 29/06 (2006.01)

(52) CPC특허분류

G06Q 20/3821 (2013.01)

G06Q 20/12 (2013.01)

(21) 출원번호 10-2018-7021765

(22) 출원일자(국제) 2017년01월03일

심사청구일자 2018년07월27일

(85) 번역문제출일자 2018년07월27일

(65) 공개번호 10-2018-0100158

(43) 공개일자 2018년09월07일

(86) 국제출원번호 PCT/US2017/012036

(87) 국제공개번호 WO 2017/136092

국제공개일자 2017년08월10일

(30) 우선권주장

62/289,656 2016년02월01일 미국(US)

(뒷면에 계속)

(56) 선행기술조사문헌

JP2013539567 A*

US20150088756 A1*

US20150095219 A1*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

애플 인크.

미국 캘리포니아 (우편번호 95014) 쿠파티노 원

애플 파크 웨이

(72) 발명자

칼슨, 칼, 앤더스

미국 95014 캘리포니아주 쿠파티노 인피니트 루프 1

디드리히, 안톤, 케이.

미국 95014 캘리포니아주 쿠파티노 인피니트 루프 1

(뒷면에 계속)

(74) 대리인

장덕순, 백만기

전체 청구항 수 : 총 21 항

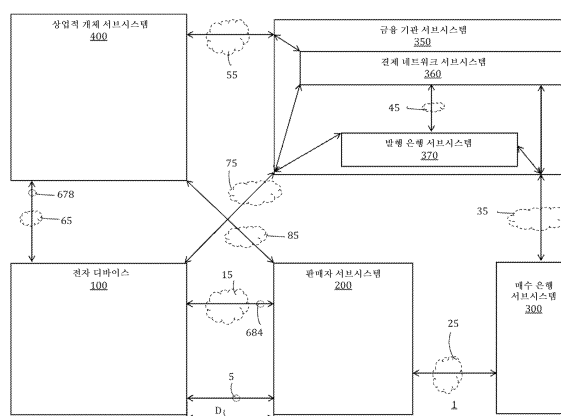
심사관 : 송미라

(54) 발명의 명칭 보안 디바이스 기능에 대한 온라인 액세스 확인

(57) 요약

보안 디바이스 기능에 대한 온라인 액세스를 확인하기 위하여 상이한 서브시스템들 간의 공유 비밀 및 제한된 사용 확인 데이터를 이용할 수 있는 시스템, 방법, 및 컴퓨터 판독가능 매체가 제공된다.

대표도 - 도1



(52) CPC특허분류

G06Q 20/3227 (2020.05)

G06Q 20/3278 (2013.01)

H04L 63/10 (2013.01)

G06Q 2220/00 (2013.01)

(72) 발명자

샤프, 크리스토퍼

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

파솔리, 지안파올로

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

스타코비악, 마치에이

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

바잉턴, 매튜, 씨.

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

시어러, 니콜라스, 제이.

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

웨이닉, 새뮤얼, 엠.

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

(30) 우선권주장

62/297,923 2016년02월21일 미국(US)

62/348,960 2016년06월12일 미국(US)

62/348,979 2016년06월12일 미국(US)

15/275,122 2016년09월23일 미국(US)

명세서

청구범위

청구항 1

프로세싱 서브시스템과 상기 프로세싱 서브시스템에 통신가능하게 결합된 전자 디바이스 간의, 상기 전자 디바이스 상에서 실행되는 온라인 리소스를 통한 보안 트랜잭션을 수행하는 관리 개체 서브시스템을 사용하기 위한 방법으로서,

상기 관리 개체 서브시스템에서, 상기 프로세싱 서브시스템으로부터 상기 온라인 리소스에 대한 확인 요청을 수신하는 단계 - 상기 확인 요청은 확인 요청 데이터를 포함함 -;

상기 관리 개체 서브시스템에서, 상기 확인 요청 데이터 및 등록 데이터를 이용하여 상기 온라인 리소스를 확인하는 단계 - 상기 등록 데이터는 상기 확인 요청을 수신하기 전에 초기에 상기 관리 개체 서브시스템에 이용가능하게 됨 -;

상기 관리 개체 서브시스템에서, 무작위 데이터를 포함하는 확인 응답 데이터를 생성하는 단계;

상기 관리 개체 서브시스템에서, 상기 관리 개체 서브시스템의 메모리 컴포넌트에서 상기 확인 응답 데이터를 상기 확인 요청 데이터의 적어도 일부분과 연관시키는 단계 - 상기 확인 요청 데이터의 상기 적어도 일부분은 상기 전자 디바이스와 상기 프로세싱 서브시스템 간의 상기 온라인 리소스를 통한 잠재적 트랜잭션을 나타내는 잠재적 트랜잭션 식별 정보를 포함함 -;

상기 관리 개체 서브시스템에서, 상기 온라인 리소스가 확인된 후, 상기 확인 응답 데이터를 상기 전자 디바이스에 전달하는 단계;

상기 관리 개체 서브시스템에서, 상기 확인 응답 데이터를 상기 전자 디바이스에 전달한 후, 상기 전자 디바이스로부터 디바이스 트랜잭션 데이터를 수신하는 단계;

상기 관리 개체 서브시스템에서, 상기 메모리 컴포넌트에서 연관된 상기 확인 응답 데이터의 상기 무작위 데이터 및 상기 잠재적 트랜잭션 식별 정보를 이용하여 상기 디바이스 트랜잭션 데이터를 확인하는 단계; 및

상기 관리 개체 서브시스템에서, 상기 디바이스 트랜잭션 데이터가 확인된 후, 상기 프로세싱 서브시스템에 의해 사용하기 위하여 상기 디바이스 트랜잭션 데이터에 기초하여 보안 트랜잭션 데이터를 생성하는 단계를 포함하는, 방법.

청구항 2

제1항에 있어서,

상기 확인 요청 데이터는 확인 세션 식별자를 포함하고;

상기 확인 응답 데이터 또는 상기 확인 요청 데이터의 상기 적어도 일부분 중 적어도 하나는 상기 확인 세션 식별자를 포함하는, 방법.

청구항 3

제2항에 있어서, 상기 확인 세션 식별자는 상기 전자 디바이스에 의해 생성된 데이터를 포함하는, 방법.

청구항 4

제3항에 있어서, 상기 확인 요청은 상기 관리 개체 서브시스템에서 상기 프로세싱 서브시스템의 결제 서비스 제공자 서브시스템으로부터 수신되는, 방법.

청구항 5

제2항에 있어서, 상기 확인 세션 식별자는 상기 프로세싱 서브시스템에 의해 생성된 데이터를 포함하는, 방법.

청구항 6

제1항에 있어서,

상기 확인 요청 데이터는 상기 온라인 리소스를 나타내는 프로세싱 식별자를 포함하고;

상기 등록 데이터는 상기 프로세싱 식별자 및 상기 관리 개체 서브시스템과 상기 프로세싱 서브시스템 간의 프로세싱 공유 비밀을 포함하고;

상기 온라인 리소스를 확인하는 단계는 상기 프로세싱 공유 비밀을 이용하여 상기 확인 요청 데이터로부터의 상기 프로세싱 식별자에 액세스하는 단계를 포함하는, 방법.

청구항 7

제1항에 있어서,

상기 확인 요청 데이터는 상기 온라인 리소스를 나타내는 프로세싱 식별자를 포함하고;

상기 연관시키는 단계는 상기 관리 개체 서브시스템의 상기 메모리 컴포넌트에서 상기 프로세싱 식별자에 대하여 상기 무작위 데이터를 저장하는 단계를 포함하는, 방법.

청구항 8

제7항에 있어서,

상기 등록 데이터는 상기 프로세싱 식별자 및 상기 관리 개체 서브시스템과 상기 프로세싱 서브시스템 간의 프로세싱 공유 비밀을 포함하고;

상기 보안 트랜잭션 데이터를 생성하는 단계는 상기 프로세싱 공유 비밀을 이용하여 상기 디바이스 트랜잭션 데이터의 일부분을 암호화하는 단계를 포함하는, 방법.

청구항 9

제7항에 있어서, 상기 프로세싱 식별자는 상기 전자 디바이스와 상기 프로세싱 서브시스템 간의 상기 온라인 리소스를 통한 상기 잠재적 트랜잭션에 고유한 확인 세션 식별자를 포함하는, 방법.

청구항 10

제7항에 있어서, 상기 확인 응답 데이터를 상기 전자 디바이스에 전달하는 단계는:

상기 관리 개체 서브시스템에서, 상기 관리 개체 서브시스템과 상기 전자 디바이스 간의 공유 비밀을 이용하여 상기 무작위 데이터에 서명하는 단계; 및

상기 서명된 무작위 데이터를 상기 전자 디바이스와 공유하는 단계를 포함하는, 방법.

청구항 11

제10항에 있어서, 상기 디바이스 트랜잭션 데이터를 확인하는 단계는 상기 디바이스 트랜잭션 데이터가 상기 무작위 데이터를 포함함을 결정하는 단계를 포함하는, 방법.

청구항 12

제7항에 있어서,

상기 확인 응답 데이터를 상기 전자 디바이스에 전달하는 단계는 상기 무작위 데이터 및 상기 프로세싱 식별자를 상기 전자 디바이스와 공유하는 단계를 포함하고;

상기 디바이스 트랜잭션 데이터를 확인하는 단계는 상기 디바이스 트랜잭션 데이터의 적어도 일부분이 상기 관리 개체 서브시스템의 상기 메모리 컴포넌트에서 상기 프로세싱 식별자에 대하여 저장되어 있음을 결정하는 단계를 포함하는, 방법.

청구항 13

제12항에 있어서, 상기 프로세싱 식별자에 대해 상기 무작위 데이터를 저장하는 단계는 상기 무작위 데이터가 상기 관리 개체 서브시스템의 상기 메모리 컴포넌트에서 상기 프로세싱 식별자에 대하여 특정 길이의 시간 이차 동안 저장되게 하는 단계를 포함하는, 방법.

청구항 14

제1항에 있어서,

상기 연관시키는 단계는 상기 관리 개체 서브시스템의 상기 메모리 컴포넌트에서 상기 잠재적 트랜잭션 식별 정보에 대하여 상기 무작위 데이터를 저장하는 단계를 포함하고;

상기 확인 응답 데이터를 상기 전자 디바이스에 전달하는 단계는 상기 무작위 데이터를 상기 전자 디바이스와 공유하는 단계를 포함하고;

상기 디바이스 트랜잭션 데이터는 디바이스 트랜잭션 식별 정보를 포함하고;

상기 디바이스 트랜잭션 데이터를 확인하는 단계는:

상기 디바이스 트랜잭션 데이터가 상기 무작위 데이터를 포함함을 결정하는 단계; 및

상기 디바이스 트랜잭션 데이터의 상기 디바이스 트랜잭션 식별 정보가 상기 잠재적 트랜잭션 식별 정보의 임계치 내에 있음을 결정하는 단계를 포함하는, 방법.

청구항 15

프로세싱 서브시스템과 상기 프로세싱 서브시스템에 통신가능하게 결합된 전자 디바이스 간의, 상기 전자 디바이스 상에서 실행되는 온라인 리소스를 통한 보안 트랜잭션을 인에이블하는 관리 개체 서브시스템을 사용하기 위한 방법으로서,

상기 관리 개체 서브시스템에서, 상기 온라인 리소스를 등록하는 단계 - 상기 등록하는 단계는 상기 관리 개체 서브시스템과 상기 프로세싱 서브시스템 간의 프로세싱 공유 비밀을 설정하는 단계를 포함함 -;

상기 관리 개체 서브시스템에서, 상기 등록하는 단계 후에, 상기 프로세싱 서브시스템으로부터 상기 온라인 리소스에 대한 확인 요청을 수신하는 단계 - 상기 확인 요청은 상기 온라인 리소스를 나타내는 프로세싱 식별자를 포함하고, 상기 확인 요청은 상기 전자 디바이스와 상기 프로세싱 서브시스템 간의 상기 온라인 리소스를 통한 잠재적 트랜잭션에 고유한 상기 전자 디바이스에 의해 생성된 확인 세션 식별자를 추가로 포함함 -; 및

상기 관리 개체 서브시스템에서, 상기 확인 세션 식별자 및 상기 프로세싱 공유 비밀을 이용하여 상기 프로세싱 식별자에 의해 표시되는 상기 온라인 리소스를 확인하는 단계를 포함하는, 방법.

청구항 16

제15항에 있어서, 상기 확인하는 단계는:

무작위 데이터를 생성하는 단계;

상기 무작위 데이터를 상기 확인 세션 식별자에 대하여 저장하는 단계;

상기 프로세싱 공유 비밀을 이용하여 상기 무작위 데이터를 암호화하는 단계;

상기 암호화된 무작위 데이터를 상기 프로세싱 서브시스템에 전달하는 단계;

상기 암호화된 무작위 데이터를 상기 프로세싱 서브시스템에 전달한 후, 상기 프로세싱 서브시스템으로부터 챌린지 응답 데이터를 수신하는 단계; 및

상기 수신된 챌린지 응답 데이터의 적어도 일부분이 상기 확인 세션 식별자에 대하여 저장되어 있음을 결정하는 단계를 포함하는, 방법.

청구항 17

제15항에 있어서, 상기 확인하는 단계는:

무작위 데이터를 생성하는 단계;

상기 프로세싱 공유 비밀을 이용하여 상기 무작위 데이터를 암호화하는 단계;

상기 암호화된 무작위 데이터를 상기 프로세싱 서브시스템에 전달하는 단계;

상기 암호화된 무작위 데이터를 상기 프로세싱 서브시스템에 전달한 후, 상기 프로세싱 서브시스템으로부터 쉼
린지 응답 데이터를 수신하는 단계; 및

상기 수신된 쉼린지 응답 데이터가 상기 무작위 데이터를 포함하는지 검출하는 단계를 포함하는, 방법.

청구항 18

제17항에 있어서, 상기 확인하는 단계는 상기 온라인 리소스의 상기 등록이 상기 암호화된 무작위 데이터를 전
달하기 전에 유효함을 결정하는 단계를 추가로 포함하는, 방법.

청구항 19

프로세싱 서브시스템과 상기 프로세싱 서브시스템에 통신가능하게 결합된 전자 디바이스 간의, 상기 전자 디바
이스 상에서 실행되는 온라인 리소스를 통한 보안 트랜잭션을 수행하는 관리 개체 서브시스템을 사용하기 위한
방법으로서,

상기 관리 개체 서브시스템에서, 상기 프로세싱 서브시스템으로부터 상기 온라인 리소스에 대한 확인 요청을 수
신하는 단계 - 상기 확인 요청은 확인 요청 데이터를 포함하고, 상기 확인 요청 데이터는 상기 전자 디바이스와
상기 프로세싱 서브시스템 간의 상기 온라인 리소스를 통한 잠재적 트랜잭션을 나타내는 잠재적 트랜잭션 식별
정보를 포함함 -;

상기 관리 개체 서브시스템에서, 상기 확인 요청 데이터의 적어도 일부분을 이용하여 상기 온라인 리소스를 확
인하는 단계;

상기 관리 개체 서브시스템에서, 확인 응답 데이터를 적어도 상기 잠재적 트랜잭션 식별 정보와 연관시키는 단
계;

상기 관리 개체 서브시스템에서, 상기 온라인 리소스가 확인된 후, 상기 확인 응답 데이터를 상기 전자 디바이
스에 전달하는 단계;

상기 관리 개체 서브시스템에서, 상기 확인 응답 데이터를 상기 전자 디바이스에 전달한 후, 상기 전자 디바이
스로부터 디바이스 트랜잭션 데이터를 수신하는 단계;

상기 관리 개체 서브시스템에서, 상기 확인 응답 데이터 및 상기 잠재적 트랜잭션 식별 정보를 이용하여 상기
디바이스 트랜잭션 데이터를 확인하는 단계; 및

상기 관리 개체 서브시스템에서, 상기 디바이스 트랜잭션 데이터가 확인된 후, 상기 프로세싱 서브시스템에 의
해 사용하기 위하여 상기 디바이스 트랜잭션 데이터에 기초하여 보안 트랜잭션 데이터를 생성하는 단계를 포함
하고,

상기 잠재적 트랜잭션 식별 정보는,

상기 잠재적 트랜잭션의 제품을 나타내는 정보;

상기 잠재적 트랜잭션의 가격을 나타내는 정보;

상기 잠재적 트랜잭션의 배송 주소를 나타내는 정보; 또는

상기 잠재적 트랜잭션의 결제 크리덴셜을 나타내는 정보

중 적어도 하나를 포함하는, 방법.

청구항 20

제19항에 있어서,

상기 확인 응답 데이터는 무작위 데이터를 포함하고;

상기 연관시키는 단계는 상기 관리 개체 서브시스템에서 상기 잠재적 트랜잭션 식별 정보에 대하여 상기 무작위

데이터를 저장하는 단계를 포함하고;

상기 확인 응답 데이터를 상기 전자 디바이스에 전달하는 단계는 상기 무작위 데이터를 상기 전자 디바이스와 공유하는 단계를 포함하고;

상기 디바이스 트랜잭션 데이터는 디바이스 트랜잭션 식별 정보를 포함하고;

상기 디바이스 트랜잭션 데이터를 확인하는 단계는:

상기 디바이스 트랜잭션 데이터가 상기 무작위 데이터를 포함함을 결정하는 단계; 및

상기 디바이스 트랜잭션 데이터의 상기 디바이스 트랜잭션 식별 정보가 상기 잠재적 트랜잭션 식별 정보의 임계치 내에 있음을 결정하는 단계를 포함하는, 방법.

청구항 21

제19항에 있어서,

상기 온라인 리소스를 확인하는 단계는 상기 확인 요청 데이터의 상기 적어도 일부분 및 등록 데이터를 이용하는 단계를 포함하고;

상기 등록 데이터는 상기 확인 요청을 수신하기 전에 초기에 상기 관리 개체 서브시스템에 이용가능하게 되고;

상기 등록 데이터는 상기 관리 개체 서브시스템과 상기 프로세싱 서브시스템 간의 프로세싱 공유 비밀을 포함하고;

상기 보안 트랜잭션 데이터를 생성하는 단계는 상기 프로세싱 공유 비밀을 이용하여 상기 디바이스 트랜잭션 데이터의 일부분을 암호화하는 단계를 포함하는, 방법.

발명의 설명

기술 분야

[0001] 관련 출원에 대한 상호 참조

[0002] 본 출원은 2016년 2월 1일자로 출원된 선행 출원 미국 가특허 출원 제62/289,656호, 2016년 2월 21일자로 출원된 선행 출원 미국 가특허 출원 제62/297,923호, 2016년 6월 12일자로 출원된 선행 출원 미국 가특허 출원 제62/348,960호, 및 2016년 6월 12일자로 출원된 선행 출원 미국 가특허 출원 제62/348,979호의 이익을 주장하며, 이것들의 각각은 본 명세서에서 전체적으로 참조로서 포함된다.

[0003] 기술분야

[0004] 본 개시내용은 보안 디바이스 기능에 대한 온라인 액세스를 확인하는 것에 관한 것으로, 더 구체적으로, 제3자 서브시스템에 의한 전자 디바이스의 보안 기능에 대한 온라인 액세스를 인에이블하기 위하여 제3자 서브시스템을 확인하는 것에 관한 것이다.

배경 기술

[0005] 휴대용 전자 디바이스들(예컨대, 셀룰러 전화기)은 전자 디바이스가 신용 카드 크리덴셜과 같은 원시 결제 크리덴셜을 생성, 액세스, 및/또는 다른 개체와 공유하도록 요구하는 데이터 트랜잭션들과 같은 다른 개체(예컨대, 판매자)와 민감한 데이터의 비접촉식 근접성 기반 통신을 인에이블하기 위한 근거리 통신("NFC") 컴포넌트들을 구비할 수 있다. 그러나, 이러한 원시 결제 크리덴셜을 전자 디바이스가 다른 유형들의 통신에서 안전하게 사용하는 것(예컨대, 온라인 트랜잭션)은 종종 비효율적이었다.

발명의 내용

[0006] 본 문서는 보안 디바이스 기능에 대한 온라인 액세스를 확인하기 위한 시스템, 방법, 및 컴퓨터 판독가능 매체를 설명한다.

[0007] 예를 들어, 상업적 개체 서브시스템을 이용하여 판매자 서브시스템과 판매자 온라인 리소스를 통해 판매자 서브시스템에 통신가능하게 결합된 전자 디바이스 간의 보안 트랜잭션을 수행하는 방법이 제공될 수 있다. 방법은, 상업적 개체 서브시스템에서, 판매자 서브시스템으로부터, 판매자 온라인 리소스에 대한 확인 요청을 수신하는

단계, 확인 요청 및 수신하는 단계 전에 초기에 상업적 개체 서브시스템에 이용가능하게 된 등록 데이터를 이용하여 판매자 온라인 리소스를 확인하는 단계, 확인 후, 확인 요청의 적어도 일부분과 연관성있는 확인 데이터를 생성하는 단계, 전자 디바이스에, 확인 데이터를 전달하는 단계, 전자 디바이스로부터, 디바이스 트랜잭션 데이터를 수신하는 단계, 디바이스 트랜잭션 데이터가 확인 데이터를 포함함을 결정하는 단계, 및, 결정 후, 판매자 서브시스템에 의한 사용을 위해 디바이스 트랜잭션 데이터에 기초하여 보안 트랜잭션 데이터를 생성하는 단계를 포함할 수 있다.

[0008] 다른 예로서, 관리 개체 서브시스템을 이용하여 프로세싱 서브시스템과 전자 디바이스 상에서 실행되는 온라인 리소스를 통해 프로세싱 서브시스템에 통신가능하게 결합된 전자 디바이스 간의 보안 트랜잭션을 수행하는 방법이 제공될 수 있다. 방법은, 관리 개체 서브시스템에서, 온라인 리소스에 대한 확인 요청을 수신하는 단계 - 확인 요청은 확인 요청 데이터를 포함함 -, 확인 요청 데이터 및 등록 데이터를 이용하여 온라인 리소스를 확인하는 단계 - 등록 데이터는 확인 요청을 수신하기 이전에 초기에 관리 개체 서브시스템에 이용가능하게 됨 -, 확인 응답 데이터를 확인 요청 데이터의 적어도 일부분과 연관시키는 단계, 온라인 리소스가 확인된 후에, 확인 응답 데이터를 전자 디바이스에 전달하는 단계, 확인 응답 데이터를 전자 디바이스에 전달한 후, 디바이스 트랜잭션 데이터를 전자 디바이스로부터 수신하는 단계, 확인 응답 데이터를 이용하여 디바이스 트랜잭션 데이터를 확인하는 단계, 디바이스 트랜잭션 데이터가 확인된 후, 프로세싱 서브시스템에 의한 사용을 위해 디바이스 트랜잭션 데이터에 기초하여 보안 트랜잭션 데이터를 생성하는 단계를 포함할 수 있다.

[0009] 또 다른 예로서, 관리 개체 서브시스템을 이용하여 프로세싱 서브시스템과 전자 디바이스 상에서 실행되는 온라인 리소스를 통해 프로세싱 서브시스템에 통신가능하게 결합된 전자 디바이스 간의 보안 트랜잭션을 인에이블하는 방법이 제공될 수 있다. 방법은, 관리 개체 서브시스템에서, 온라인 리소스를 등록하는 단계 - 등록하는 것은 관리 개체 서브시스템과 프로세싱 서브시스템 간의 프로세싱 공유 비밀을 설정하는 것을 포함함 -, 온라인 리소스에 대한 확인 요청을 수신하는 단계 - 확인 요청은 온라인 리소스를 나타내는 프로세싱 식별자를 포함하고, 확인 요청은 전자 디바이스와 프로세싱 서브시스템 간의 온라인 리소스를 통한 잠재적 트랜잭션에 고유한 확인 세션 식별자를 추가로 포함함 -, 및 확인 세션 식별자 및 프로세싱 공유 비밀을 이용하여 프로세싱 식별자에 의해 표시되는 온라인 리소스를 확인하는 단계를 포함할 수 있다.

[0010] 또 다른 예로서, 관리 개체 서브시스템을 이용하여 프로세싱 서브시스템과 전자 디바이스 상에서 실행되는 온라인 리소스를 통해 프로세싱 서브시스템에 통신가능하게 결합된 전자 디바이스 간의 보안 트랜잭션을 수행하는 방법이 제공될 수 있다. 방법은, 관리 개체 서브시스템에서, 온라인 리소스에 대한 확인 요청을 수신하는 단계 - 확인 요청은 확인 요청 데이터를 포함하고, 확인 요청 데이터는 전자 디바이스와 프로세싱 서브시스템 간의 온라인 리소스를 통한 잠재적 트랜잭션을 나타내는 잠재적 트랜잭션 식별 정보를 포함함 -, 확인 요청 데이터의 적어도 일부분을 이용하여 온라인 리소스를 확인하는 단계, 확인 응답 데이터를 적어도 잠재적 트랜잭션 식별 정보와 연관시키는 단계, 온라인 리소스가 확인된 후, 확인 응답 데이터를 전자 디바이스에 전달하는 단계, 확인 응답 데이터를 전자 디바이스에 전달한 후, 디바이스 트랜잭션 데이터를 전자 디바이스로부터 수신하는 단계, 확인 응답 데이터 및 잠재적 트랜잭션 식별 정보를 이용하여 디바이스 트랜잭션 데이터를 확인하는 단계, 및, 디바이스 트랜잭션 데이터가 확인된 후, 프로세싱 서브시스템에 의한 사용을 위해 디바이스 트랜잭션 데이터에 기초하여 보안 트랜잭션 데이터를 생성하는 단계를 포함할 수 있다.

[0011] 본 발명의 내용은 단지 본 문헌에 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. 다른 방식으로 진술되지 않는 한, 일 예의 콘텍스트에 기재된 특징부들은 하나 이상의 다른 예의 콘텍스트에 기재된 특징부들과 조합 또는 함께 사용될 수 있다. 본 명세서에 기술되는 주제의 다른 특징들, 양태들 및 이점들은 다음의 상세한 설명, 도면 및 청구범위로부터 명백해질 것이다.

도면의 간단한 설명

[0012] 이하의 논의는 하기 도면들을 참조하며, 도면들에서 유사한 참조 부호들은 전체에 걸쳐 유사한 부분들을 지칭한다.

도 1은 보안 디바이스 기능에 대한 온라인 액세스를 확인하기 위한 도시적인 시스템의 개략도이다.

도 1a는 도 1의 시스템의 다른 더 상세한 개략도이다.

도 2는 도 1 및 도 1a의 시스템의 예시 전자 디바이스의 더 상세한 개략도이다.

도 2a는 도 1 내지 도 2의 예시 전자 디바이스의 다른 더 상세한 개략도이다.

도 3은 도 1 내지 도 2a의 예시 전자 디바이스의 정면도이다.

도 3a 내지 도 3d는 보안 디바이스 기능에 대한 온라인 액세스를 확인하기 위한 프로세스들을 도시하는 도 1 내지 도 3 중 하나 이상의 예시 전자 디바이스의 그래픽 사용자 인터페이스의 스크린들의 정면도이다.

도 4는 도 1 및 도 1a의 시스템의 예시 상업적 개체 서브시스템의 더 상세한 개략도이다.

도 5 내지 도 9는 보안 디바이스 기능에 대한 온라인 액세스를 확인하기 위한 도시화된 프로세스들의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0013] 프로세싱(또는 판매자) 서브시스템은, 프로세싱 서브시스템의 온라인 리소스(예컨대, 원시 애플리케이션 또는 웹사이트)가, 파트너 결제 서비스 제공자("PSP") 내장형 결제 형태의 여부에 상관없이, 사용자 전자 디바이스로부터 민감한 데이터(예컨대, 보안 요소 결제 크리덴셜 데이터)를 안전하게 수신하는 데 사용되기 전에 PSP의 여부에 상관없이 신뢰하는 관리(또는 상업적) 개체 서브시스템에 의해 확인될 수 있다. 또한, 온라인 리소스가 사용자 디바이스에 프로세싱 서브시스템과의 트랜잭션에서 민감한 데이터를 공유하는 옵션을 제시하도록 동작할 수 있기 전에 온라인 리소스의 확인에 추가적으로, 특정 트랜잭션을 인에이블하는 데 사용하기 위한 온라인 리소스를 재인가하기 위하여 이러한 옵션의 선택에 응답하여 추가적인 세션 확인 프로세스가 수행될 수 있다.
- [0014] 도 1 및 도 1a는 시스템(1)을 도시하며, 시스템(1)에서 하나 이상의 크리덴셜이 상업적(또는 관리) 개체 서브시스템(400) 및 금융 기관(또는 트랜잭션 또는 발행자) 서브시스템(350)으로부터 전자 디바이스(100) 상으로 발급될 수 있고, 이러한 크리덴셜들이 전자 디바이스(100)에 의해 판매자(또는 프로세싱) 서브시스템(200) 및 연관된 매수 은행(또는 매수자) 서브시스템(300)과 트랜잭션(예컨대, 금융 거래 또는 임의의 다른 적합한 보안 데이터 트랜잭션)을 수행하는 데 사용될 수 있고(예컨대, 전자 디바이스(100)의 보안 디바이스 기능), 도 2 내지 도 3은 시스템(1)의 전자 디바이스(100)의 특정 실시예들에 대한 더 상세사항들을 도시하며, 도 3a 내지 도 3d는 이러한 트랜잭션 동안 시스템(1)의 전자 디바이스(100)의 그래픽 사용자 인터페이스를 나타낼 수 있는 예시 스크린들(190a 내지 190d)을 도시하며, 도 4는 시스템(1)의 상업적 개체 서브시스템(400)의 특정 실시예들에 대하여 상세사항들을 추가적으로 도시하고, 도 5 내지 도 9는 보안 디바이스 기능에 대한 온라인 액세스를 확인하기 위한(예컨대, 이러한 금융 거래를 수행함) 도시화된 프로세스들의 흐름도이다.
- [0015] 도 1의 설명
- [0016] 도 1은 제3자 서브시스템에 의한 전자 디바이스의 보안 기능에 대한 온라인 액세스를 인에이블하기 위한 제3자 서브시스템의 확인을 허용할 수 있는 도시하는 시스템(1)의 개략도이고, 여기서 확인은, 예컨대, 판매자 서브시스템과의 트랜잭션(예컨대, 온라인 결제 또는 비접촉식 근접성 기반 결제)에서 전자 디바이스 상의 크리덴셜의 안전한 사용을 인에이블하기 위한 판매자(또는 프로세싱) 서브시스템의 확인이다. 예를 들어, 도 1에 도시된 바와 같이, 시스템(1)은 전자 디바이스(100)뿐만 아니라, 하나 이상의 크리덴셜을 전자 디바이스(100) 상에 안전하게 발급하기 위한 상업적(또는 관리) 개체 서브시스템(400) 및 금융 기관(또는 트랜잭션 또는 발행자) 서브시스템(350)을 포함할 수 있다. 또한, 도 1에 도시된 바와 같이, 시스템(1)은 또한 판매자(또는 프로세싱) 서브시스템(200)을 포함할 수 있고, 이로써 이러한 발급된 크리덴셜은 전자 디바이스(100)에 의해 판매자 서브시스템(200)과의 트랜잭션(예컨대, 금융 거래 또는 임의의 다른 적합한 보안 데이터 트랜잭션)을 수행하는 데 사용될 수 있다. 예를 들어, 판매자 서브시스템(200)으로부터 잠재적 트랜잭션 데이터를 수신하는 것에 응답하여, 전자 디바이스(100)는 비접촉식 근접성 기반 통신(5)(예컨대, 근거리 통신 또는 블루투스™ 통신) 및/또는 판매자 서브시스템(200)과의 특정 금융 거래에 자금을 제공하기 위한 온라인 기반 통신(684)(예컨대, 네트워크 전기통신 또는 기타 다른 방식)과 같이 발급된 크리덴셜의 보안 디바이스 데이터를 판매자 서브시스템(200)과 공유할 수 있다. 시스템(1)은 또한 이러한 비접촉식 근접성 기반 통신(5) 및/또는 금융 기관 서브시스템(350)과의 트랜잭션을 완료하기 위한 이러한 온라인 기반 통신(684)을 활용할 수 있는 매수 은행(또는 매수자) 서브시스템(300)을 포함할 수 있다.
- [0017] 시스템(1)은 전자 디바이스(100)와 판매자 서브시스템(200) 간 통신을 인에이블하기 위한 통신 경로(15), 판매자 서브시스템(200)과 매수 은행 서브시스템(300) 간 통신을 인에이블하기 위한 통신 경로(25), 통신 매수 은행 서브시스템(300)과 금융 기관 서브시스템(350) 간 통신을 인에이블하기 위한 통신 경로(35), 금융 기관 서브시

시스템(350)의 결제 네트워크 서브시스템(360)과 금융 기관 서브시스템(350)의 발행 은행 서브시스템(370) 간의 통신을 인에이블하기 위한 통신 경로(45), 금융 기관 서브시스템(350)과 상업적 개체 서브시스템(400) 간 통신을 인에이블하기 위한 통신 경로(55), 상업적 개체 서브시스템(400)과 전자 디바이스(100) 간 통신을 인에이블하기 위한 통신 경로(65), 금융 기관 서브시스템(350)과 전자 디바이스(100) 간 통신을 인에이블하기 위한 통신 경로(75), 및 상업적 개체 서브시스템(400)과 판매자 서브시스템(200) 간의 통신을 인에이블하기 위한 통신 경로(85)를 포함할 수 있다. 경로들(15, 25, 35, 45, 55, 65, 75, 85) 중 하나 이상은 하나 이상의 신뢰 서비스 관리자("TSM")에 의해 적어도 부분적으로 관리될 수 있다. 통신 네트워크를 생성하는 데 동작가능할 수 있는 임의의 적합한 회로부, 디바이스, 시스템, 또는 이들의 조합(예컨대, 하나 이상의 통신탑, 전기통신 서버 등을 포함할 수 있는 유선 및/또는 무선 통신 기반시설)을 이용하여 경로들(15, 25, 35, 45, 55, 65, 75, 85) 중 하나 이상을 제공할 수 있고, 이들은 임의의 적합한 유선 또는 무선 통신 프로토콜을 이용하여 통신을 제공할 수 있다. 예를 들어, 경로들(15, 25, 35, 45, 55, 65, 75, 85) 중 하나 이상은 Wi-Fi(예컨대, 802.11 프로토콜), ZigBee(예컨대, 802.15.4 프로토콜), WiDi™, 이더넷, 블루투스™, BLE, 고주파수 시스템(예컨대, 900 MHz, 2.4 GHz, 및 5.6 GHz 통신 시스템), 적외선, TCP/IP, SCTP, DHCP, HTTP, 비트토렌트(BitTorrent™), FTP, RTP, RTSP, RTCP, RAOP, RDTP, UDP, SSH, WDS-브리징, 무선 및 셀룰러 전화기 및 개인용 이메일 디바이스들에 의해 사용될 수 있는 임의의 통신 프로토콜(예컨대, GSM, GSM 플러스 EDGE, CDMA, OFDMA, HSPA, 다중대역 등), 저전력 무선 개인 영역 네트워크("6LoWPAN") 모듈에 의해 사용될 수 있는 임의의 통신 프로토콜, 임의의 기타 통신 프로토콜, 또는 이들의 임의의 조합을 지원할 수 있다.

[0018] 도 1a의 설명

[0019] 도 1a를 이제 참조하면, 도 1a는 도 1에 대하여 위에서 기재한 시스템(1)의 더 상세한 도면을 도시한다. 도 1a에 도시된 바와 같이, 예를 들어, 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 기관들(예컨대, 글로벌 플랫폼(GlobalPlatform))과 같은 금융 기관 서브시스템 및/또는 산업 표준의 기관)의 세트에 의해 제시될 수 있는 규칙 및 보안 요구조건에 따라 애플리케이션들 및 그것들의 비밀 및 암호 데이터(예컨대, 크리덴셜 애플릿들 및 연관된 크리덴셜 키들, 예를 들어, 크리덴셜 키(155a'), 및 액세스 키(155a), 및/또는 발행자 보안 도메인("ISD") 키(156k), 이는 도 1a에 도시된 바와 같음)를 안전하게 호스팅할 수 있는 (예컨대, 싱글칩 또는 다중칩 보안 마이크로제어기와 같은) 부정조작 방지(tamper-resistant) 플랫폼을 제공하도록 구성될 수 있는 보안 요소(145)를 포함하거나 또는 다른 방식으로 제공할 수 있다. 아래 더 상세하게 기재된 바와 같이, 디바이스(100)의 보안 요소(145)(예컨대, NFC 컴포넌트(120)) 상의 크리덴셜 애플릿 또는 결제 애플리케이션은 결제 크리덴셜 데이터를 자금 계좌 또는 기타 금융 상품 또는 신용 소스(예컨대, 금융 기관 서브시스템(350)에 있음)를 식별하는 데 충분히 상세한 트랜잭션 데이터로서 제공하도록 구성될 수 있고, 이러한 결제 크리덴셜 데이터는 디바이스(100)에 의해 금융 거래를 용이하게 하기 위하여 판매자 서브시스템(200) 및/또는 상업적 개체 서브시스템(400)과의 하나 이상의 통신에 사용될 수 있다. NFC 컴포넌트(120)는 판매자 서브시스템(200)(예컨대, 판매자 서브시스템(200)의 판매자 단말기(220)로서, 소매 상점 또는 디바이스(100)의 사용자가 디바이스(100) 상에 저장된 크리덴셜을 이용하여 비접촉식 근접성 기반 통신을 통해 근접하게 위치한 판매자 단말기(220)와 금융 거래를 수행할 수 있는 임의의 물리적 위치에 위치할 수 있음)과의 비접촉식 근접성 기반 통신(5)(예컨대, 근거리 통신)으로서 이러한 호스트 결제 크리덴셜 데이터를 전달하도록 구성될 수 있다. 대안적으로 또는 추가적으로, 통신 컴포넌트(106)가 제공되어 디바이스(100)로 하여금 임의의 적합한 결제 크리덴셜 데이터를 (예컨대, 온라인 기반 통신(684)으로서) 임의의 적합한 유선 또는 무선 프로토콜을 이용하여(예컨대, 통신 경로들(15, 65, 및/또는 75) 중 하나 이상을 통해) 하나 이상의 다른 전자 디바이스 또는 서버 또는 서브시스템과(예컨대, 시스템(1)의 하나 이상의 서브시스템 또는 기타 컴포넌트들, 예를 들어, 임의의 적합한 온라인 통신을 통한 판매자 서브시스템(200)의 판매자 서버(210)와) 교환하도록 할 수 있다. 디바이스(100)의 프로세서(102)는 디바이스(100)의 하나 이상의 컴포넌트의 동작들 및 성능을 제어하도록 동작할 수 있는 임의의 프로세싱 회로부를 포함할 수 있다. 예를 들어, 프로세서(102)는 데이터(예컨대, 트랜잭션 데이터의 결제 크리덴셜 데이터)가 판매자 서브시스템(200)과의 금융 거래에 자금을 공급하기 위하여 디바이스(100)에 의해 교환될 수 있는 방법을 적어도 부분적으로 구술할 수 있는 하나 이상의 애플리케이션(예컨대, 애플리케이션(103) 및/또는 온라인 리소스 또는 판매자 애플리케이션(113))을 디바이스(100) 상에서 실행하도록 구성될 수 있다. 또한, 도 1a에 도시된 바와 같이, 디바이스(100)는 임의의 적합한 디바이스 식별 정보 또는 디바이스 식별자(119)를 포함할 수 있고, 이는 프로세서(102) 또는 디바이스(100)의 임의의 다른 적합한 부분에 액세스가능할 수 있다. 디바이스 식별 정보(119)는 상업적 개체 서브시스템(400) 및/또는 판매자 서브시스템(200) 및/또는 금융 기관 서브시스템(350)에 의해 디바이스(100)를 고유하게 식별하여 판매자 서브시스템(200)과의 트랜잭션을 용이하게 하고/하거나 디바이

스(100)와의 임의의 적합한 보안 통신을 인에이블하기 위하여 활용될 수 있다. 단지 하나의 예로서, 디바이스 식별 정보(119)는 전화 번호 또는 이메일 주소 또는 디바이스(100)와 연관될 수 있는 임의의 고유 식별자일 수 있다.

[0020]

판매자 서브시스템(200)은 도 1a에 도시된 바와 같이 임의의 적합한 판매자 서버(210)를 포함할 수 있는데, 이는 임의의 적합한 데이터를 임의의 적합한 통신 프로토콜(예컨대, Wi-Fi, 블루투스™, 셀룰러, 유선 네트워크 프로토콜 등)을 통해 상업적 개체 서브시스템(400)의 통신 컴포넌트(예컨대, 통신 경로(85)를 통함) 및/또는 매수 은행(300)의 통신 컴포넌트(예컨대, 통신 경로(25)를 통함) 및/또는 디바이스(100)의 통신 컴포넌트(예컨대, 통신 경로(15)를 통함)와 교환하도록 구성될 수 있는 임의의 적합한 컴포넌트 또는 서브시스템을 포함할 수 있다. 예를 들어, 판매자 서버(210)는 임의의 적합한 온라인-컨텍스트 내에서, 예컨대, 디바이스(100)의 사용자가 판매자 서버(210)와 통신하여 디바이스(100) 상에서 실행될 수 있는 임의의 적합한 판매자 온라인 리소스(113), 예를 들어, 판매자 서버(210)에 의해 관리될 수 있는 디바이스(100) 상에서 실행되는 제3자 판매자 애플리케이션(113)(예컨대, 원시 애플리케이션) 또는 타겟 또는 웹 리소스가 판매자 서버(210)에 의해 관리될 수 있는 "URL"(uniform resource locator)로 지향될 수 있는 디바이스(100) 상에서 실행되는 인터넷 애플리케이션(113)(예컨대, 애플 인크에 의한 사파리(Safari™))(예컨대, 판매자 웹사이트, 판매자 웹사이트로 인도되는 웹 화면을 이용하는 판매자 애플리케이션(예컨대, 판매자 애플리케이션 내부에 번들로 포함되어, 하이브리드 앱으로 지칭될 수 있는 것을 생성하는 인터넷 브라우저, 이는 이러한 앱이 웹 기술(예컨대, HTML, 자바스크립트(JavaScript), CSS 등)을 이용하여 설치되도록 할 수 있을뿐만 아니라 또한 이러한 앱이 원시 앱으로서 패키징화되도록 할 수 있음), 및/또는 판매자 웹사이트로 인도되는 웹 화면을 이용하는 비-판매자 애플리케이션)를 통해 트랜잭션을 수행할 때, 잠재적 트랜잭션 데이터(660)를 디바이스(100)의 통신 컴포넌트(106)와 교환하도록 동작할 수 있다. 따라서, 주의할 점은, 판매자 서버(210)와 디바이스(100) 간의 통신은 무선으로 및/또는 유선 경로(예컨대, 인터넷)를 통해 일어날 수 있다는 것이다. 판매자 서버(210)는 판매자 서브시스템(200)의 판매자에 의해 (예컨대, 웹사이트 데이터를 호스트하고/하거나 제3자 애플리케이션 데이터를 관리하는 웹서버로서) 구비될 수 있다. 추가적으로 또는 대안적으로, 도 1a에 도시된 바와 같이, 판매자 서브시스템(200)은 임의의 적합한 판매자 단말기(220)(예컨대, 판매자 결제 단말기)를 포함할 수 있고, 이는 임의의 적합한 데이터를 디바이스(100)의 비접촉식 근접성 기반 통신 컴포넌트와 교환하도록 구성될 수 있는 임의의 적합한 컴포넌트 또는 서브시스템을 포함할 수 있다(예컨대, 디바이스(100)의 NFC 컴포넌트(120)를 이용한 비접촉식 근접성 기반 통신(5)). 또한, 도 1a에 도시된 바와 같이, 판매자 서브시스템(200)은 판매자 키(157) 및/또는 판매자 식별자("ID")(167)를 포함할 수 있다. 도시되지 않았지만, 판매자 서브시스템(200)은 또한 도 1a 및 도 2의 전자 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 판매자 프로세서 컴포넌트, 도 1a 및 도 2의 전자 디바이스(100)의 통신 컴포넌트(106)와(예컨대, 서버(210)의 일부분으로서) 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 컴포넌트(108)와 동일하거나 유사할 수 있는 판매자 전원 공급 컴포넌트를 포함할 수 있다.

[0021]

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 크리덴셜로 발생할 수 있는 대금을 지불할 소비자의 능력에 대한 1차 책임(primary liability)을 맡을 수 있는 금융 기관일 수 있다. 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, 지불 카드(charge card), 선불 카드, 플릿 카드(fleet card), 선물 카드 등을 포함한, 다양한 유형들의 결제 카드가 적합할 수 있다. 특정 결제 카드의 상거래 크리덴셜은 (예컨대, 직접 또는 상업적 개체 서브시스템(400)을 통해) 판매자 서브시스템(200)과의 상거래 크리덴셜 데이터 통신(예컨대, 비접촉식 근접성 기반 통신 및/또는 온라인 기반 통신)에 사용하기 위해, 발행 은행 서브시스템(370)에 의해 디바이스(100) 상에 (예컨대, 아래에 기재된 바와 같이, NFC 컴포넌트(120)의 크리덴셜 보충적 보안 도메인의 크리덴셜과 같이) 발급될 수 있다. 각각의 크리덴셜은 결제 네트워크 서브시스템(360)에 의해 상표화될 수 있는 결제 카드의 특정 상표일 수 있다. 결제 네트워크 서브시스템(360)은 특정 상표의 결제 카드들(예컨대, 상거래 크리덴셜들)의 사용을 처리할 수 있는 다양한 발행 은행들(370) 및/또는 다양한 매수 은행들(300)의 네트워크일 수 있다.

[0022]

금융 거래가 시스템(1) 내에서 일어나도록 하기 위하여, 적어도 하나의 상거래 크리덴셜이 전자 디바이스(100)의 보안 요소 상에 안전하게 발급되어야 한다. 예를 들어, 이러한 상거래 크리덴셜은 적어도 부분적으로 디바

이스(100)의 보안 요소(145) 상에 금융 기관 서브시스템(350)으로부터 직접 발급될 수 있다(예컨대, 금융 기관 서브시스템(350)과 디바이스(100) 간 통신 경로(75)를 통한 크리덴셜 데이터(654)로서, 이는 통신 컴포넌트(106)를 통해 보안 요소(145)에 전달될 수 있음). 추가적으로 또는 대안적으로, 이러한 상거래 크리덴셜은 적어도 부분적으로 금융 기관 서브시스템(350)으로부터 상업적 개체 서브시스템(400)을 통해 디바이스(100)의 보안 요소(145) 상에 발급될 수 있다(예컨대, 금융 기관 서브시스템(350)과 상업적 개체 서브시스템(400) 간의 통신 경로(55)를 통한 크리덴셜 데이터(654)로서, 이는 상업적 개체 서브시스템(400)의 서버(410)와 디바이스(100)의 통신 컴포넌트(106) 간의 통신 경로(65)를 통한 크리덴셜 데이터(654)로서 디바이스(100)에 전달될 수 있고, 이어서 통신 컴포넌트(106)로부터 보안 요소(145)로 전달될 수 있음). 경로(75) 및/또는 경로들(55/65)을 통한 크리덴셜 데이터(654)는 디바이스(100)의 보안 요소(145) 상에 보안 요소의 적어도 일부분 또는 모든 크리덴셜 보충적 보안 도메인으로서 발급될 수 있고, 크리덴셜 정보 및/또는 크리덴셜 키를 구비한 크리덴셜 애플릿, 예컨대 크리덴셜 정보(161a) 및 크리덴셜 키(155a')를 구비한 결제 애플리케이션 또는 크리덴셜 애플릿(153a)을 포함할 수 있다. 도 1a에 도시된 바와 같이, 예를 들어, 금융 기관 서브시스템(350)은 또한 크리덴셜 키(155a')에 액세스할 수 있다(예컨대, 디바이스(100)에 의해 암호화된 데이터를 크리덴셜 키(155a')를 이용하여 복호화하기 위함). 금융 기관 서브시스템(350)은 크리덴셜 키(155a')의 관리를 책임질 수 있는데, 이는 이러한 키의 생성, 교환, 저장, 사용, 및 교체를 포함할 수 있다. 금융 기관 서브시스템(350)은 그것의 크리덴셜 키(155a')의 버전을 금융 기관 서브시스템(350)의 보안 요소에 저장할 수 있다. 디바이스(100)와 금융 기관 서브시스템(350)의 크리덴셜 키(155a')는 임의의 적합한 공유 비밀(예컨대, 패스워드, 패스프레이즈, 무작위로 선택된 바이트들의 어레이, 하나 이상의 대칭키, 공개키-개인키(예컨대, 비대칭키) 등)일 수 있으며, 이는 전자 디바이스(100)의 보안 요소와 금융 기관 서브시스템(350) 둘 모두에 이용되어, 예컨대, 기능적 출력이 적어도 부분적으로 공유 비밀에 의해 결정될 수 있는 임의의 적합한 암호화 알고리즘 또는 암호(cipher)를 이용함으로써, 임의의 적합한 암호 데이터(예컨대, 암호) 또는 전자 디바이스(100) 및 금융 기관 서브시스템(350)에 의해 독립적으로 생성되는 임의의 다른 적합한 데이터(예컨대, 금융 거래에 대한 결제 데이터를 확인하기 위함)를 인에이블하도록 동작할 수 있으며, 이러한 공유 비밀은 금융 기관 서브시스템(350)에 의해 디바이스(100) 상에 발급될 수 있음이 이해될 것이다. 공유 비밀은 사전에 금융 기관 서브시스템(350)과 디바이스(100) 간에(예컨대, 금융 기관 서브시스템(350)에 의해 디바이스(100) 상에 크리덴셜을 발급하는 동안) 공유될 수 있으며, 이러한 경우 이러한 공유 비밀은 사전공유된 키라고 지칭될 수 있고, 또는 공유 비밀이 특정 금융 거래에 사용하기 전에 키-동의 프로토콜을 이용(예컨대, 디피-헬만법(Diffie-Hellman)과 같은 공개키 암호화, 또는 커버로스(Kerberos)와 같은 대칭키 암호화를 이용)함으로써 생성될 수 있다. 공유 비밀 및 기능적 출력이 적어도 부분적으로 공유 비밀에 의해 결정될 수 있는 임의의 적합한 암호화 알고리즘 또는 암호는 디바이스(100)의 보안 요소에 액세스가능할 수 있다.

[0023]

상업적 개체 서브시스템(400)은 금융 기관 서브시스템(350)과 디바이스(100) 간의 중개장치로서 제공될 수 있는데, 상업적 개체 서브시스템(400)은 새로운 보안 계층을 제공하고/하거나 크리덴셜이 디바이스(100)의 보안 요소 상에 발급중일 때 및/또는 이러한 발급된 크리덴셜이 디바이스(100)와 판매자 서브시스템(200) 간의 상거래 크리덴셜 데이터 통신의 일부로서 사용중일 때 더 매끄러운 사용자 경험을 제공하도록 구성될 수 있다. 상업적 개체 서브시스템(400)은 그 상업적 개체와의 사용자별 계좌에 대한 사용자별 로그인 정보를 통해(예컨대, 사용자별 식별 및 패스워드 조합을 통해) 다양한 서비스들을 디바이스(100)의 사용자에게 제공할 수 있는 특정 상업적 개체에 의해 제공될 수 있다. 단지 하나의 예로서, 상업적 개체 서브시스템(400)은 미국 캘리포니아주 쿠파티노 소재의 애플 사(Apple Inc.)에 의해 제공될 수 있으며, 애플 사는 또한 디바이스(100)의 사용자들에 대한 다양한 서비스의 제공자일 수 있고(예를 들어, 디바이스(100)에 의해 재생되는 미디어를 판매/대여하기 위한 아이튠즈(iTunes)TM 스토어, 디바이스(100) 상에서 사용할 애플리케이션들을 판매/대여하기 위한 애플 앱 스토어(Apple App Store)TM, 디바이스(100)로부터의 데이터를 저장 및/또는 다수의 사용자 디바이스들 및/또는 다수의 사용자 프로필들을 서로 연관시키기 위한 애플 아이클라우드(Apple iCloud)TM 서비스, 다양한 애플 제품을 온라인에서 구입하기 위한 애플 온라인 스토어(Apple Online Store), 디바이스들 간의 미디어 메시지들을 교환하기 위한 애플 아이메시지 서비스(Apple iMessageTM Service) 등), 애플 사는 또한 디바이스(100) 자체(예컨대, 디바이스(100)가 아이팟(iPod)TM, 아이패드(iPad)TM, 아이폰(iPhone)TM 등인 경우) 및/또는 디바이스(100)의 운영체제(예컨대, 디바이스 애플리케이션(103))의 제공자, 제조자, 및/또는 개발자일 수 있다. 상업적 개체 서브시스템(400)을 제공할 수 있는 상업적 개체(예컨대, 애플 사)는 금융 기관 서브시스템(350)의 임의의 금융 개체와 별개이고 그에 독립적일 수 있다. 예를 들어, 상업적 개체 서브시스템(400)을 제공할 수 있는 상업적 개체는 임의의 신용 카드 또는 최종 사용자 디바이스(100) 상에 발급된 임의의 기타 상거래 크리덴셜을 제공 및/또는 관리할 수 있는 임의의 결제 네트워크 서브시스템(360) 또는 발행 은행 서브시스템(370)과 별개이고/이거나 그

에 독립적일 수 있다. 추가적으로 또는 대안적으로, 상업적 개체 서브시스템(400)을 제공할 수 있는 상업적 개체(예컨대, 애플 인크)는 판매자 서브시스템(200)의 임의의 판매자와 별개이고 그에 독립적일 수 있다. 예를 들어, 상업적 개체 서브시스템(400)을 제공할 수 있는 상업적 개체는 비접촉식 근접성 기반 통신을 위한 판매자 단말기, 온라인 통신을 위한 제3자 애플리케이션 또는 온라인 리소스(113), 및/또는 임의의 기타 양태의 판매자 서브시스템(200)을 제공할 수 있는 판매자 서브시스템(200)의 임의의 판매자와 별개이고/이거나 그에 독립적일 수 있다. 이러한 상업적 개체는, 사용자가 금융 기관 서브시스템(350)에 의해 제공되는 크리덴셜을 디바이스(100) 상에 발급하기를 원할 때 및/또는 이러한 발급된 크리덴셜이 판매자 서브시스템(200)과의 상거래 크리덴셜 데이터 통신의 일부로서 금융 거래에 자금을 제공하는 데 사용중일 때 디바이스(100)의 사용자에게 더 매끄러운 사용자 경험을 제공하기 위하여, 디바이스(100)의 다양한 컴포넌트들(예컨대, 그 상업적 개체가 적어도 부분적으로 디바이스(100)를 생성 또는 관리할 수 있을 때의, 디바이스(100)의 소프트웨어 및/또는 하드웨어 컴포넌트들)을 구성 또는 제어하는 자신의 잠재 능력을 이용할 수 있다. 예를 들어, 일부 실시예들에서, 디바이스(100)는 (예컨대, 디바이스(100)와 판매자 서브시스템(200) 간의 온라인 기반 보안 데이터 통신 동안) 더 높은 수준의 보안을 인에이블 할 수 있는 소정 데이터를 공유 및/또는 수신하기 위하여 (예컨대, 통신 경로(65)를 통해) 디바이스(100)의 사용자에게 끊임없이 투명하게 상업적 개체 서브시스템(400)과 통신하도록 구성될 수 있다. 도시되지 않았지만, 상업적 개체 서브시스템(400)은 또한 도 1a 및 도 2의 전자 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 프로세서 컴포넌트, 도 1a 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 컴포넌트(108)와 동일하거나 유사할 수 있는 전원 공급 컴포넌트를 포함할 수 있고, 이들 중 하나, 일부 또는 전부는 적어도 부분적으로 서버(410)에 의해 제공될 수 있다.

[0024] 적어도 하나의 상거래 크리덴셜이 디바이스(100)의 보안 요소 상에 발급되는 것뿐만 아니라(예컨대, 크리덴셜 키(155a') 및 크리덴셜 정보(161a)를 갖는 크리덴셜 SSD의 일부분으로서), 더 안전하게 디바이스(100)가 판매자 서브시스템(200)과 금융 거래를 수행하도록 하기 위하여 액세스 키(155b)를 갖는 적어도 하나의 액세스 SSD가 또한 디바이스(100)의 보안 요소 상에 발급될 수 있다. 예를 들어, 액세스 SSD는 적어도 부분적으로 상업적 개체 서브시스템(400)으로부터 직접 디바이스(100)의 보안 요소 상에 발급될 수 있다(예컨대, 상업적 개체 서브시스템(400)의 서버(410)와 디바이스(100)의 통신 컴포넌트(106) 간의 통신 경로(65)를 통한 액세스 데이터(652)로서, 이는 이어서 통신 컴포넌트(106)로부터 보안 요소(145)로 전달될 수 있음). 경로(65)를 통한 액세스 데이터(652)는 디바이스(100)의 보안 요소 상에 적어도 일부분 또는 모든 액세스 SSD로서 발급될 수 있고, 액세스 키(155b)를 갖는 액세스 애플릿(153b)을 포함할 수 있다. 도 1a에 도시된 바와 같이, 상업적 개체 서브시스템(400)은 또한 액세스 키(155b)에 액세스 할 수 있다(예컨대, 디바이스(100)에 의해 암호화된 데이터를 액세스 키(155b)를 이용하여 복호화하기 위함). 상업적 개체 서브시스템(400)은 액세스 키(155b)의 관리를 책임질 수 있는데, 이는 이러한 키의 생성, 교환, 저장, 사용, 및 교체를 포함할 수 있다. 상업적 개체 서브시스템(400)은 그것의 액세스 키(155b)의 버전을 상업적 개체 서브시스템(400)의 보안 요소에 저장할 수 있다. 액세스 키(155b)를 구비한 디바이스(100)의 액세스 SSD는 (예컨대, 생체인식 입력 컴포넌트와 같은 디바이스(100)의 하나 이상의 입력 컴포넌트(110)를 통해) 디바이스(100)의 사용자의 의도 및 로컬 인증을 결정하도록 구성될 수 있고, 이러한 결정에 응답하여, 결제 트랜잭션을 수행하도록 (예컨대, 디바이스(100)의 크리덴셜 SSD의 크리덴셜을 이용하여) 다른 특정 SSD를 인에이블하도록 구성될 수 있다. 이러한 액세스 SSD를 디바이스(100)의 보안 요소 내에 저장함으로써, 금융 거래에 대한 사용자 의도 및 금융 거래의 인증을 신뢰성있게 결정하는 그것의 능력은 증가될 수 있다. 또한, 디바이스(100)의 이러한 액세스 SSD의 액세스 키(155b)는 디바이스(100)의 보안 요소의 외부에서 교환될 수 있는 트랜잭션 데이터에 증가된 암호화를 제공하는 이점이 있을 수 있다. 추가적으로 또는 대안적으로, 아래에 기재된 바와 같이, 액세스 데이터(652)는 전자 디바이스(100)의 보안 요소의 발행자 보안 도메인("ISD")에 대한 ISD 키(156k)를 포함할 수 있는데, 이는 또한 상업적 개체 서브시스템(400)에 의해 유지될 수 있고, 액세스 키(155b)에 추가적으로 또는 대안적으로 사용될 수 있으며, 이는 아래에 기재된 바와 같다.

[0025] 디바이스(100)와 판매자 서브시스템(200) 간에 용이하게 될 온라인 금융 거래를 인에이블하거나 또는 판매자 서브시스템(200)에 의한 디바이스(100)의 임의의 다른 적합한 보안 디바이스 기능에 대한 온라인 액세스를 인에이블하기 위하여, 판매자 애플리케이션 또는 온라인 리소스(113)는 디바이스(100)에 의해 액세스될 수 있다. 우선, 애플리케이션(113)이 효과적으로 디바이스(100)에 의해 활용될 수 있기 전에, 이러한 애플리케이션(113)은

상업적 개체 서브시스템(400)에 의해 승인 또는 등록되거나 또는 다른 방식으로 인에이블될 수 있다. 예를 들어, 상업적 개체 서브시스템(400)의 애플리케이션 스토어(420)(예컨대, 애플 앱 스토어(Apple App Store™))는 애플리케이션(113)을 나타내는 적어도 일부 데이터를 판매자 서브시스템(200)으로부터 통신 경로(85)를 통해 수신할 수 있다. 또한, 일부 실시예들에서, 상업적 개체 서브시스템(400)은 애플리케이션(113)에 대한 판매자 키(157)를 생성하거나 또는 다른 방식으로 배정할 수 있고, 이러한 판매자 키(157)를 판매자 서브시스템(200)에(예컨대, 경로(85)를 통해) 제공할 수 있다. 대안적으로, 판매자 서브시스템(200)은 애플리케이션(113)에 대한 판매자 키(157)를 생성하거나 또는 다른 방식으로 배정할 수 있고, 이러한 판매자 키(157)를 상업적 개체 서브시스템(400)에(예컨대, 경로(85)를 통해) 제공할 수 있다. 판매자 서브시스템(200) 또는 상업적 개체 서브시스템(400) 중 어느 하나는 판매자 키(157)의 관리를 책임질 수 있는데, 이는 이러한 키의 생성, 교환, 저장, 사용, 및 교체를 포함할 수 있다. 이러한 판매자 키(157)가 어떻게 또는 어디서 생성 및/또는 관리될 수 있는지 상관없이, 판매자 서브시스템(200) 및 상업적 개체 서브시스템(400) 둘 모두는 판매자 키(157)의 버전을 저장할 수 있다(예컨대, 판매자 서브시스템(200) 및 상업적 개체 서브시스템(400)의 각각의 보안 요소에 저장함, 일부 실시예들에서, 판매자 서브시스템(200)에 의해 저장된 판매자 키(157)는 개인키일 수 있고, 상업적 개체 서브시스템(400)에 의해 저장된 판매자 키(157)는 대응하는 공개키(예컨대, 비대칭키 암호화/복호화 프로세스에 사용하기 위함)일 수 있음). 일부 실시예들에서, 이러한 판매자 키(157)는 구체적으로 판매자 애플리케이션(113)과 연관될 수 있고, 반면에, 다른 실시예들에서, 판매자 키(157)는 구체적으로 판매자 서브시스템(200)의 판매자와 연관되어, 판매자 키(157)가 동일한 판매자 서브시스템(200)의 판매자에 의해 동작되는 다수의 제3자 애플리케이션들 또는 웹 리소스들과 연관될 수 있도록 할 수 있다. 고유 판매자 식별자(167)는 상업적 개체 서브시스템(400) 및/또는 판매자 서브시스템(200)에 의해 생성 및/또는 다른 방식으로 배정되거나 애플리케이션(113)과 연관될 수 있다. 예를 들어, 판매자 식별자(167)는 영숫자 스트링, 도메인(예컨대, 웹 리소스형 온라인 리소스 애플리케이션(113)을 위한 URL 또는 다른 방식), 또는 판매자 및/또는 특정 판매자 온라인 리소스를 고유하게 식별할 수 있는 임의의 다른 적합한 식별자일 수 있다(예컨대, 상업적 개체 서브시스템(400)에 대한 것들을 고유하게 식별함). 표(430) 또는 임의의 다른 적합한 데이터 구조 또는 상업적 개체 서브시스템(400)에 액세스가 가능할 수 있는 정보의 소스가 특정 판매자 키(157)를 판매자 애플리케이션(113) 또는 판매자 개체의 특정 판매자 식별자(167)와 연관시키기 위하여 제공될 수 있다. 판매자 온라인 리소스가 특정 판매자 식별자(167) 및 특정 판매자 키(157)와 연관될 수 있고, 이들의 각각은 판매자 서브시스템(200)과 상업적 개체 서브시스템(400) 간에 안전하게 공유될 수 있다. 표(430)는 디바이스(100)가 키(157) 및 판매자 식별자(167)와 연관된 판매자 애플리케이션(113)을 통해 판매자 서브시스템(200)과 교류하는 것을 수반할 수 있는 트랜잭션을 위하여, 판매자 서브시스템(200)에 전달되는 임의의 보안 디바이스 데이터(예컨대, 디바이스(100)에 원래 있던 결제 크리덴셜 데이터를 포함할 수 있는 상거래 크리덴셜 데이터)에 보안 계층을 제공하기 위한 적절한 판매자 키(157)를 결정 및 활용하도록 상업적 개체 서브시스템(400)을 인에이블할 수 있다. 디바이스(100)는(예컨대, 애플리케이션 스토어(420)로부터 통신 경로(65)를 통해) 애플리케이션(113)에 액세스하고, (예컨대, 프로세서(102)를 이용하여) 애플리케이션(113)을 실행하도록 구성될 수 있다. 대안적으로 또는 추가적으로, 판매자 키(157) 및 판매자 식별자(167)는 일반적으로, 판매자의 제3자 원시 앱 이외에, 또는 이에 추가적으로, 판매자의 웹사이트(예컨대, 하나 이상의 URL 또는 도메인, 이들은 일부 실시예들에서 판매자 온라인 리소스 또는 판매자 애플리케이션으로 본 명세서에서 지칭될 수 있음) 또는 그 판매자와 연관될 수 있다. 예를 들어, 판매자 서브시스템(200)의 판매자는 상업적 개체 서브시스템(400)과 함께 특정 판매자 웹사이트 또는 판매자를 일반적으로 표(430) 내의 특정 판매자 키(157) 및 판매자 식별자(167)와 연관시키도록 작업하는데, 이는 상업적 개체 서브시스템(400)이 트랜잭션을 위하여 판매자 서브시스템(200)에 전달되는 임의의 보안 디바이스 데이터(예컨대, 디바이스(100)에 원래 있던 결제 크리덴셜 데이터를 포함할 수 있는 상거래 크리덴셜 데이터)에 보안 계층을 제공하기 위한 적절한 판매자 키(157)를 결정 및 활용하도록 인에이블할 수 있으며, 이는 디바이스(100)가 판매자 서버(210)와 교류하여 타겟 또는 웹 리소스가 그 판매자 키(157) 및 판매자 식별자(167)와 연관될 수 있는 URL 또는 도메인(예컨대, 그 웹 리소스의 고유 도메인(예컨대, store.merchant.com))으로 지향될 수 있는 디바이스(100) 상에서 실행 중인 인터넷 애플리케이션 또는 웹 브라우저를 통해 트랜잭션을 수행하는 것을 수반할 수 있다. 디바이스(100)는, 예를 들어, 판매자 서버(210)로부터 통신 경로(15)를 통해 이러한 URL에 액세스하도록 구성될 수 있다(예컨대, 이러한 판매자 웹 리소스를 타겟팅할 때 판매자 온라인 리소스로서 고려될 수 있는 디바이스(100) 상의 인터넷 애플리케이션(113)을 이용함). 다른 실시예들에서, 애플리케이션(113)은 특정 판매자, 판매자 서브시스템(200), 판매자 키(157) 및/또는 판매자 식별자(167)와 연관되지 않을 수 있지만, 대신 이러한 판매자 웹 리소스를 타겟으로 하는 웹화면을 갖는 디바이스(100)에 이용가능한 독립적인 애플리케이션이어서, 판매자 온라인 리소스의 역할을 할 수 있다. 상업적 개체 서브시스템(400)에 의한 판매자 온라인 리소스의 이러한 등록(예컨대, 판매자 서브시스템(200)과 상업적 개체 서브시스템(400) 간의 판매자 키(157) 및 판매자 식별자(167)의 안전한

고 확인된 공유(예컨대, 표(430)에 저장하기 위함))이 임의의 적합한 방식으로 수행되어 판매자 서브시스템(200)이 온라인 리소스의 유효한 소유자임을 상업적 개체 서브시스템(400)에게 보장할 수 있다. 언급된 바와 같이, 판매자 온라인 리소스(예컨대, 원시 앱, 도메인/URL, 또는 임의의 다른 적합한 웹 리소스, 또는 간혹 판매자 단말기)는 특정 판매자 식별자(167) 및 특정 판매자 키(157)와 연관될 수 있고(예컨대, 도 5의 단계(501) 및/또는 도 6의 단계(606)에서 등록 시), 이들의 각각은 판매자 서브시스템(200)과 상업적 개체 서브시스템(400) 간에 임의의 적합한 방식으로 안전하게 공유될 수 있고, 이러한 연관성은 상업적 개체 서브시스템(400)에 액세스가능하게 할 수 있다(예컨대, 표(430)).

[0026] 도 2의 설명

[0027] 도 2를 이제 참조하면, 도 2는 도 1 및 도 1a에 대하여 위에서 기재한 시스템(1)의 전자 디바이스(100)의 더 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. 게다가, 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. 사용자가 디바이스(100)와 상호작용 또는 교류하도록 하는 하나 이상의 입력 컴포넌트(110)가 제공될 수 있고/있거나 정보(예컨대, 그래픽, 청각, 및/또는 촉각 정보)를 디바이스(100)의 사용자에게 나타내는 하나 이상의 출력 컴포넌트(112)가 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 처리 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. 일 예로서, 애플리케이션(103)은 운영 체제 애플리케이션일 수 있는 반면, 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 디바이스 식별 정보(119)에 액세스할 수 있는데, 이는 디바이스(100)의 사용자 및/또는 상업적 개체 서브시스템(400)에 의해 디바이스(100)의 식별을 제공하는 데 활용될 수 있다.

[0028] NFC 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200)의 판매자 단말기(예컨대, 판매자 결제 단말기(220)) 간의 비접촉식 근접성 기반 트랜잭션 또는 통신을 인에이블할 수 있는 임의의 적합한 근접성 기반 통신 메커니즘일 수 있다. NFC 컴포넌트(120)는 전자 디바이스(100)와 이러한 판매자 단말기 간의 비접촉식 근접성 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 제어기 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 근접성 기반 또는 NFC 통신의 일부로서 전송될 수 있는 임의의 적합한 데이터를 포함하거나, 라우팅하거나, 또는 다른 방식으로 제공하도록 구성될 수 있다. 추가적으로 또는 대안적으로, NFC 데이터 모듈(132)은 NFC 컴포넌트(120)에 의해 판매자 단말기로부터 비접촉식 근접성 기반 통신의 일부로서 수신될 수 있는 임의의 적합한 데이터를 포함하거나, 라우팅하거나, 또는 다른 방식으로 수신하도록 구성될 수 있다. NFC 제어기 모듈(140)은 적어도 하나의 NFC 프로세서 모듈(142)을 포함할 수 있다. NFC 프로세서 모듈(142)은 NFC 디바이스 모듈(130)과 연계하여 동작하여, 전자 디바이스(100)와 판매자 단말기 간의 NFC 통신을 교환하기 위하여 NFC 컴포넌트(120)를 인에이블, 활성화, 허용, 및/또는 다른 방식으로 제어할 수 있다. NFC 제어기 모듈(140)은, NFC 컴포넌트(120)의 기능을

지시하는 데 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 제어기 모듈(140)과 연계하여 동작하여, 전자 디바이스(100)와 판매자 서브시스템(200) 간의 NFC 통신을 허용할 수 있다. NFC 메모리 모듈(150)은 부정조작 방지될 수 있고, 보안 요소(145)의 적어도 일부분을 제공할 수 있다(예컨대, 도 2a 참조). 예를 들어, 이러한 보안 요소는 잘 식별된 신뢰 기관들(예컨대, 글로벌플랫폼과 같은 금융 기관 서브시스템 및/또는 산업 표준의 기관)의 세트에 의해 제시될 수 있는 규칙 및 보안 요구조건에 따라 애플리케이션들 및 그것들의 비밀 및 암호 데이터(예컨대, 애플릿들(153) 및 키들(155))를 안전하게 호스팅할 수 있는 (예컨대, 싱글칩 또는 멀티칩 보안 마이크로제어기와 같은) 부정조작 방지 플랫폼을 제공하도록 구성될 수 있다.

[0029] 도 2에 도시된 바와 같이, 예를 들어, 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("TSM") 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 다른 식으로 전자 디바이스(100) 상에 발급하기 위한 키들 및/또는 다른 적합한 정보를 저장할 수 있는 NFC 메모리 모듈(150)의 일부분일 수 있다. 크리덴셜은 사용자/소비자에 배정될 수 있고, 전자 디바이스(100) 상에 안전하게 저장될 수 있는 크리덴셜 데이터(예컨대, 크리덴셜 정보(161a)), 예컨대, 신용 카드 결제 번호(예컨대, 디바이스 기본 계좌 번호("DPAN"), DPAN 만료일, CVV 등 (예컨대, 토큰 또는 다른 방식의 것))를 포함할 수 있다. 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 특정 특권 또는 결제 권한을 전자 디바이스(100)에 제공할 수 있는 특정 크리덴셜(예컨대, 금융 기관 서브시스템(350)에 의해 발급되는 특정 신용 카드 크리덴셜 또는 특정 대중 교통 카드 크리덴셜)과 연관될 수 있는 반면, 제2 SSD(154b)(예컨대, 액세스 SSD(154b))는 다른 SSD(예컨대, 제1 SSD(154a))의 특정 크리덴셜에 대한 디바이스(100)의 액세스를 제어하여, 예를 들어, 특정 특권 또는 결제 권한을 전자 디바이스(100)에 제공할 수 있는 상업적 개체(예컨대, 상업적 개체 서브시스템(400)의 상업적 개체로서, 이는 디바이스(100)에 대한 제어 개체일 수 있음)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 발급되는 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)는 애플릿(153a)과 연관되고, SSD(154b)는 애플릿(153b)과 연관됨). 예를 들어, SSD(154)의 애플릿(153)은 NFC 컴포넌트(120)의 보안 요소 상에서(예컨대, 글로벌플랫폼 환경에서) 실행될 수 있는 애플리케이션일 수 있다. 크리덴셜 애플릿(153)은 크리덴셜 정보(161)(예컨대, 애플릿(153a)의 정보(161a) 및/또는 애플릿(153b)의 정보(161b))를 포함하거나 또는 그와 연관될 수 있다. 각각의 SSD(154) 및/또는 애플릿(153)은 또한 자체 키들(155) 중 적어도 하나를 포함하고/하거나 그와 연관될 수 있다(예컨대, 애플릿(153a)은 적어도 하나의 키(155a)와 연관되고, 애플릿(153b)은 적어도 하나의 키(155b)와 연관됨).

[0030] SSD(154)의 키(155)는 암호화 알고리즘 또는 암호의 기능적 출력을 결정할 수 있는 한 편의 정보일 수 있다. 예를 들어, 암호화 시, 키는 평문의 암호문으로의 특정 변환을 명시할 수 있거나, 또는 복호화 시 그 반대로의 변환을 명시할 수 있다. 키는 또한 디지털 서명 기법 및 메시지 인증 코드와 같은 다른 암호화 알고리즘에 사용될 수 있다. SSD의 키는 다른 개체와의 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 사전로딩될 수 있다. 일 예로서, 크리덴셜 SSD(154a)가 특정 신용 카드 크리덴셜과 연관될 수 있는 반면, 그 특정 크리덴셜은 단지 그 크리덴셜 SSD(154a)의 애플릿(153a)이 이러한 사용을 위해 인에이블되었거나 또는 다른 방식으로 활성화 또는 잠금해제되었을 때 금융 거래를 위해 디바이스(100)의 보안 요소로부터(예컨대, NFC 컴포넌트(120)로부터) 판매자 서브시스템(200)으로 상거래 크리덴셜 데이터 통신으로서 전달될 수 있다.

[0031] NFC 컴포넌트(120)의 사용을 인에이블하기 위한 보안 특징들이 제공될 수 있으며, 이는 크리덴셜의 신용 카드 정보 또는 은행 계좌 정보와 같은 기밀 결제 정보를 전자 디바이스(100)로부터 판매자 서브시스템(200)으로 전송할 때 특히 유용할 수 있다. 그러한 보안 특징들은 또한 제한된 액세스를 가질 수 있는 보안 저장 영역을 포함할 수 있다. 예를 들어, 개인 식별 번호("PIN") 입력을 통한, 또는 생체인식 센서와의 사용자 상호작용을 통

한 사용자 인증이, 보안 저장 영역에 액세스하기 위해 제공될 필요가 있을 수 있다. 예를 들어, 액세스 SSD(154b)는 애플릿(153b)을 이용하여 이러한 인증이 다른 SSD들(154)(예컨대, 크리덴셜 SSD(154a))이 그것의 크리덴셜 정보(161a)를 전달하는 데 사용되도록 하기 전에 일어났는지 결정할 수 있다. 소정 실시예들에서, 보안 특징들의 일부 또는 모두가 NFC 메모리 모듈(150) 내에 저장될 수 있다. 또한, 상거래 크리덴셜 데이터를 판매자 서브시스템(200)과 교환하기 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 마이크로제어기를 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 있고, 이러한 결정에 응답하여, (예컨대, 크리덴셜 SSD(154a)의 크리덴셜을 이용하여) 결제 트랜잭션을 수행하기 위하여 다른 특정 SSD를 인에이블하도록 구성될 수 있다.

[0032] 도 2a의 설명

[0033] 도 2a를 이제 참조하면, 도 2a는 도 1 내지 도 2에 대하여 위에서 기재된 시스템(1)의 전자 디바이스(100)의 일 부분의 다른 상세한 도면을 도시한다. 도 2a에 도시된 바와 같이, 예를 들어, 디바이스(100)의 보안 요소(145)는, 애플릿(153a), 크리덴셜 정보(161a), 액세스 키(155a), 및/또는 크리덴셜 키(155a')를 포함하거나 또는 그와 연관될 수 있는 SSD(154a), 및 애플릿(153b), 크리덴셜 정보(161b), 액세스 키(155b), 및/또는 크리덴셜 키(155b')를 포함하거나 또는 그와 연관될 수 있는 SSD(154b)를 포함할 수 있다. 일부 실시예들에서, 특정 보충적 보안 도메인("SSD")(154)(예컨대, SSD들(154a, 154b) 중 하나)은 특정 특권 또는 결제 권한을 전자 디바이스(100)에 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 인에이블하기 위해 활성화될 필요가 있을 수 있는 자체 관리자 키(155)(예컨대, 키들(155ak, 155bk)의 각각)를 가질 수 있다. 추가적으로 또는 대안적으로, 각각의 SSD(154)는 특정 상거래 크리덴셜과 연관된 자체 크리덴셜 애플리케이션 또는 크리덴셜 애플릿 중 적어도 하나(예컨대, Java 카드 애플릿 인스턴스)를 포함하고/하거나 그와 연관될 수 있는데(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 애플릿은 자체 액세스 키(예컨대, 크리덴셜 애플릿(153a)에 대한 액세스 키(155a) 및/또는 크리덴셜 애플릿(153b)에 대한 액세스 키(155b)) 및/또는 자체 크리덴셜 키(예컨대, 크리덴셜 애플릿(153a)에 대한 크리덴셜 키(155a') 및/또는 크리덴셜 애플릿(153b)에 대한 크리덴셜 키(155b'))를 가질 수 있고, 크리덴셜 애플릿은 (예컨대, 판매자 단말기(220)와) NFC 통신 및/또는 (예컨대, 상업적 개체 서브시스템(400)을 통한) 전자 디바이스(100)와 판매자 서브시스템(200) 간의 온라인 기반 통신으로서 NFC 디바이스 모듈(130)에 의한 사용을 위해 그것의 연관된 상거래 크리덴셜을 인에이블하도록 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 이러한 크리덴셜을 책임질 수 있는 금융 기관 서브시스템(350)에 의해 생성될 수 있고, 보안 요소(145)와 금융 기관 서브시스템(350) 간의 (예컨대, 판매자 서브시스템(200)을 통한) 그 애플릿의 그 크리덴셜 정보의 보안 전송을 인에이블하기 위하여 금융 기관 서브시스템(350)에 의해 (예컨대, 도 1a에 도시된 바와 같이) 액세스가능할 수 있다. 추가적으로 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 상업적 개체 서브시스템(400)에 의해 생성될 수 있고, 보안 요소(145)와 상업적 개체 서브시스템(400) 간의 그 애플릿의 그 크리덴셜 정보의 보안 전송을 인에이블하기 위하여 상업적 개체 서브시스템(400)에 의해 (예컨대, 도 1a에 도시된 바와 같이) 액세스가능할 수 있다. 추가적으로 또는 대안적으로, 도시된 바와 같이, 각각의 애플릿은 자체 고유 애플리케이션 식별자("AID"), 예컨대, 애플릿(153a)의 AID(155aa) 및/또는 애플릿(153b)의 AID(155ba)를 포함할 수 있다. 예를 들어, AID는 특정 카드 기법 및 제품, 프로그램, 또는 네트워크(예컨대, 마스터카드 시리즈(MasterCard Cirrus), 비자 플러스(Visa PLUS), 인터랙(Interac) 등)을 식별할 수 있고, AID는 AID와 연관된 크리덴셜의 결제 시스템(예컨대, 카드 기법) 또는 네트워크(예컨대, 마스터카드, 비자, 인터랙 등)를 식별하는 데 사용될 수 있는 등록된 애플리케이션 제공자 식별자("RID")뿐만 아니라, 또한 AID와 연관된 크리덴셜의 제공자 또는 결제 시스템에 의해 제공되는 제품, 프로그램, 또는 애플리케이션들을 구분하는 데 사용될 수 있는 독점적 애플리케이션 식별자 확장("PIX")을 포함할 수 있다. 보안 요소(145)의 펌웨어를 관장하도록 동작할 수 있는 임의의 적합한 설명서(예컨대, Java 카드 설명서)는 보안 요소(145) 상의 각각의 AID의 고유함을 보장하거나 또는 다른 방식으로 강요하도록 동작할 수 있다(예컨대, 보안 요소(145) 상의 각각의 크리덴셜 인스턴스는 자체 고유 AID와 연관될 수 있음).

[0034] 추가적으로 또는 대안적으로, 도 2a에 도시된 바와 같이, 보안 요소(145)는 ISD(152)를 포함할 수 있고, 이는

그 보안 도메인과 연관된 신뢰 서비스 관리자(예컨대, 상업적 개체 서브시스템(400), 도 1a에 도시된 바와 같음)에 또한 알려질 수 있는 ISD 키(156k)를 포함할 수 있다. ISD 키(156k)는 상업적 개체 서브시스템(400)과 전자 디바이스(100)의 보안 요소(145) 간의 보안 전송을 인에이블하기 위하여 액세스 키(155a) 및/또는 액세스 키(155b)와 유사하게 및/또는 그를 대신하여 상업적 개체 서브시스템(400) 및 전자 디바이스(100)에 의해 이용될 수 있다. 또한, 도 2a에 도시된 바와 같이, 프로세서(102)와 보안 요소(145) 간에 다양한 데이터가 교환될 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)를 수신 및/또는 I/O 출력 데이터(115o)를 송신하기 위함), 및/또는 통신 컴포넌트(106)와 정보를 교환할 수 있는 디바이스 애플리케이션(103)을 실행하도록 구성될 수 있다. 또한, 도시된 바와 같이, 프로세서(102)는 디바이스 식별 정보(119)에 액세스할 수 있는데, 이는 디바이스(100)와 원격 개체들 간의 보안 통신을 인에이블하기 위하여 활용될 수 있다.

[0035]

추가적으로 또는 대안적으로, 도 2a에 도시된 바와 같이, 보안 요소(145)는 감독 기관 보안 도메인("CASD")(158)을 포함할 수 있는데, 이는 제3자 탑재형 신뢰 루트(third-party on-element root of trust)의 역할을 하도록 구성될 수 있는 특수 목적 보안 도메인일 수 있다. CASD(158)의 연관된 애플리케이션은 다른 애플리케이션들 및/또는 특정 관리 계층(예컨대, 글로벌 플랫폼 관리 계층)에 대한 글로벌 서비스로서 탑재형 기밀 키 생성(on-element confidential key generation)을 제공하도록 구성될 수 있다. CASD(158) 내에 사용될 수 있는 기밀 키 재료는 보안 요소(145)의 발행자를 포함하여, 어떠한 개체에 의해서도 검사 또는 변경될 수 없도록 구성될 수 있다. CASD(158)는 CASD 액세스 키트(158k)(예컨대, CASD 개인키("CASD-SK"), CASD 공개키("CASD-PK"), CASD 증명서("CASD-Cert."), 및/또는 CASD-서명 모듈)를 포함하도록 구성될 수 있고/있거나 이를 생성 및/또는 다른 방식으로 포함하도록 구성될 수 있다. 예를 들어, CASD(158)는 (예컨대, CASD 액세스 키트(158k)를 이용하여) 보안 요소(145) 상의 소정 데이터에 서명한 뒤, 이러한 데이터를 디바이스(100)의 다른 부분(예컨대, 시스템(1)의 다른 서브시스템과 공유하기 위한 통신 컴포넌트(106))에 제공하도록 구성될 수 있다. 예를 들어, CASD(158)는 보안 요소(145)에 의해 제공된 임의의 데이터에 서명하여, 다른 서브시스템(예컨대, 상업적 개체 서브시스템(400))이 이러한 서명된 데이터가 보안 요소(145)에 의해 (예컨대, 상업적 개체 서브시스템(400)에서 연관된 CASD 키트(158k)를 이용하여) 서명되었음을 확인할 수 있도록 구성될 수 있다.

[0036]

추가적으로 또는 대안적으로, 도 2a에 도시된 바와 같이, 보안 요소(145)는 비접촉식 등록 서비스("CRS") 애플릿 또는 애플리케이션(151)을 포함할 수 있는데, 이들은 소정 보안 도메인 요소들의 수명 주기 상태(예컨대, 활성화, 비활성화, 잠금 등)를 변경하고, 소정 수명 주기 상태에 있는 소정 보안 도메인 요소들에 관한 소정 출력 정보(115o)를 디바이스(100)의 사용자와 (예컨대, 사용자 I/O 인터페이스(114a)를 통해) 공유하는 로컬 기능을 전자 디바이스(100)에 제공하도록 구성될 수 있다. 예를 들어, CRS 애플리케이션(151)은 보안 요소(145) 상의 각각의 보안 도메인 요소의 현재 수명 주기 상태의 리스트(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 보유할 수 있는 CRS 리스트(151t)를 포함할 수 있으며, CRS 애플리케이션(151)은 보안 요소(145)의 하나 이상의 보안 도메인 요소의 수명 주기 상태를 디바이스(100)의 애플리케이션과 공유하도록 구성될 수 있으며(예컨대, 임의의 적합한 애플리케이션 유형으로서, 예컨대, 운영 체제 애플리케이션(103) 및/또는 카드 관리 애플리케이션(103b) 내의 백그라운드 프로세스로서 실행될 수 있는 카드 관리 데몬("CMD") 애플리케이션(103a)과 같은 데몬(예컨대, 애플 링크에 의한 패스북(Passbook™) 또는 월렛(Wallet™) 애플리케이션) 및/또는 판매자 애플리케이션(113)(예컨대, 판매자 키(157) 및 판매자 식별자(167)와 연관될 수 있는 판매자 온라인 리소스) 및/또는 신분 서비스("IDS") 애플리케이션(103c)으로, 반드시 디바이스(100)의 상호작용하는 사용자의 제어하에 있을 필요는 없음), 이는 결과적으로 소정 수명 주기 상태 정보를 디바이스(100)의 사용자에게 출력 정보(115o)로서 I/O 인터페이스(114a) 및 사용자 인터페이스("UI") 애플리케이션(예컨대, 카드 관리 애플리케이션(103b)의 UI)를 통해 제공할 수 있고, 이는 사용자가 보안 도메인 요소의 수명 주기 상태를 변경하도록(예컨대, 금융 거래에 사용하기 위하여 특정 크리덴셜 애플릿의 상거래 크리덴셜을 인에이블하는 것과 같이 CRS 리스트(151t) 및 보안 도메인 요소의 수명 주기 상태를 업데이트함) 인에이블할 수 있다. 추가적으로 또는 대안적으로, CRS(151)는 CRS(151)와 연관된 신뢰 서비스 관리자(예컨대, 상업적 개체 서브시스템(400), 도 1a에 도시된 바와 같음)에 또한 알려질 수 있는 CRS 액세스 키(151k)를 포함할 수 있다. CRS 액세스 키(151k)는 상업적 개체 서브시스템(400)과 전자 디바이스(100)의 보안 요소(145) 간의 보안 전송을 인에이블하기 위하여 액세스 키(155a) 및/또는 액세스 키(155b)와 유사하게 및/또는 그를 대신하여 상업적 개체 서브시스템(400) 및 전자 디바이스(100)에 의해 이용될 수 있다.

[0037]

IDS 애플리케이션(103c)은 데몬과 같은, 운영 체제 애플리케이션(103) 및/또는 카드 관리 애플리케이션(103b) 내부의 백그라운드 프로세스로서 실행될 수 있고/있거나 CMD 애플리케이션(103a)에 의해 제공될 수 있는 임의의

적합한 애플리케이션 유형일 수 있고, 임의의 적합한 IDS 서비스에 대해 송신될 수 있는 IDS 메시지들을 듣고 응답하기 위한 IDS 관리자로서 동작할 수 있는데, 이는 임의의 적합한 메시징 서비스, 예컨대, 애플 링크에 의한 아이메시지(iMessage™), 또는 기타(예컨대, 애플 링크에 의한 페이스타임(FaceTime™) 또는 컨티뉴이티(Continuity™))에 유사할 수 있으며, 호스트 디바이스(100)의 IDS 애플리케이션(103c)과 다른 디바이스(예컨대, 클라이언트 디바이스)의 유사 IDS 애플리케이션 간의 메시지들의 고유한 엔드-투-엔드(end-to-end) 암호화를 인에이블할 수 있다. 이러한 메시지들은 통신하는 디바이스들의 하나 또는 둘 모두에 대하여 및/또는 통신하는 디바이스들의 특정 사용자들 중 한명 또는 둘 모두에 대하여 고유 식별자들을 이용하여 암호화될 수 있다. 이러한 메시지들은 로컬 링크 또는 실제 디바이스 대 디바이스 (예컨대, 피어 투 피어) 통신으로서 교환될 수 있거나, 또는 상업적 개체 서브시스템(400)을 통해 (예컨대, 신분 관리 시스템 컴포넌트(470)를 통해) 교환될 수 있다. 이러한 메시징은 데이터가 구조화된 포맷(예컨대, 프로토콜 버퍼) 및/또는 구조화되지 않은 포맷으로 교환되도록 할 수 있는 낮은 레이턴시 해결책으로서 인에이블될 수 있다. IDS 애플리케이션(103c)은 IDS 메시지가 수신될 때 실행되고 있지 않다면 자동으로 일어날 수 있다. IDS 애플리케이션(103c)은 적절한 사용자 인터페이스를 나타내고 수신된 IDS 통신의 요청된 데이터를 요청하는 디바이스로 인도하도록 동작할 수 있다. 호스트 디바이스의 IDS 애플리케이션(103c)은 클라이언트 디바이스로부터 초기 요청이 검출될 수 있을 때 카드 관리 애플리케이션(103b)의 카드 관리 데몬 애플리케이션(103a)을 깨우도록 동작할 수 있는데, 이를 통해 호스트 디바이스는 저전력 '슬립' 모드에서 동작할 수 있다. IDS 애플리케이션(103c)은 추가적으로 또는 대안적으로 이러한 요청에 대한 '타임 아웃'을 관리하도록 동작할 수 있는데, 클라이언트 디바이스로부터의 결제 요청이 호스트 디바이스 상에서 일정 기간 동안 아무런 작용이 없다면(예컨대, 60 초, 이러한 요청에 응답하는 능동적인 호스트 디바이스 사용자 상호작용이 없음), IDS 애플리케이션(103c)은 요청을 종료하는 결정을 내릴 수 있고, 이는 호스트 디바이스가 '취소' 상태를 생성하고 그것을 클라이언트 디바이스에 전달하도록 할 수 있고, 적절한 메시지를 (예컨대, 클라이언트 디바이스의 사용자에게 '타임 아웃 에러'를) 디스플레이할 수 있다.

[0038] 도 3 및 도 3a 내지 도 3d의 설명

[0039] 도 3에 도시된 바와 같이, 그리고 이하에서 더욱 상세히 기술되는 바와 같이, 전자 디바이스(100)의 특정 예는 아이폰(iPhone)™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. 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 도시된 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 판매자 온라인 리소스 애플리케이션과 같은 애플리케이션과 연관된 GUI(180)의 대응하는 스크린을 디스플레이하도록 구성될 수 있다. 예를 들어, "판매자 앱" 텍스트형 표시자(181)로 라벨링된 특정 아이콘(182)(즉, 특정 아이콘(183))이 디바이스(100)의 사용자에게 의해 선택되면, 디바이스(100)는 특정 제3자 판매자 애플리케이션(예컨대, 원시 애플리케이션 또는 하이브리드 애플리케이션)을 기동하거나 또는 다른 방식으로 그것에 액세스할 수 있다. 다른 예로서, "인터넷" 텍스트형 표시자로 라벨링된 특정 아이콘(182)(즉, 특정 아이콘(184))이 디바이스(100)의 사용자에게 의해 선택되면, 디바이스(100)는 다른 유형의 판매자 온라인 리소스를 디바이스(100)에 제공하기 위하여 특정 제3자 판매자의 웹 리소스의 URL로 인도될 수 있는 인터넷 브라우저 애플리케이션을 기동하거나 또는 다른 방식으로 그것에 액세스할 수 있다. 임의의 적합한 판매자 온라인 리소스가 액세스되면, 디바이스(100)는 특정 방식으로 디바이스(100)를 이용하여 그 판매자 온라인 리소스와 상호작용하기 위한 하나 이상의 툴 또는 특징부를 포함할 수 있는 특정 사용자 인터페이스의 스크린을 디스플레이하도록 동작할 수 있다(디바이스(100)의 임의의 보안 기능(예컨대, 판매자 서브시스템(200)에 디바이스(100)의 NFC 컴포넌트(120)의 크리덴셜(예컨대, 크리덴셜 SSD(154a)의 크리덴셜)로 결제함)을 임의로 수행하기 위하여 디바이스 사용자에게 의해 사용될 수 있는 임의의 적합한 애플리케이션(예컨대, 판매자 온라인 리소스(113))의 사용 시, 이러한 GUI(180)의 디스플레이들의 특정 예시들에 대한 도 3a 내지 도 3d를 참조). 각각의 애플리케이션에 대해, 스크린들이 디스플레이 출력 컴포넌트(112a) 상에 디스플레이될 수 있으며 다양한 사용자 인터페이스

스 요소를 포함할 수 있다. 추가적으로 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. 예를 들어, 일부 실시예들에서, 디바이스(100)는 거래에 자금을 지원하거나 또는 디바이스의 임의의 다른 적합한 보안 기능을 수행하기 위하여 결제 크리덴셜의 사용을 선택 및 인증하기 위한 GUI를 제공하도록 동작하는 사용자 인터페이스 컴포넌트를 포함하지 않지만, 대신 오디오 출력 컴포넌트 및 기계적 또는 기타 적합한 사용자 입력 컴포넌트들을 제공할 수 있다.

[0040] 도 4의 설명

[0041] 도 4를 이제 참조하면, 도 4는 시스템(1)의 상업적 개체 서브시스템(400)의 특정 실시예들에 대하여 더 상세하게 도시한다. 도 4에 도시된 바와 같이, 상업적 개체 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), 신분 관리 시스템("IDMS") 컴포넌트(470), 사기 시스템 컴포넌트(480), 하드웨어 보안 모듈("HSM") 컴포넌트(490), 저장 컴포넌트(420), 및/또는 하나 이상의 서버(410)를 포함할 수 있다. 상업적 개체 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 개체 서브시스템(400)의 하나의, 일부의, 또는 모든 컴포넌트들은 금융 기관 서브시스템(350) 및/또는 판매자 서브시스템(200)과 별개이고 그에 독립적일 수 있는 단일 상업적 개체(예컨대, 애플 사)에 의해 관리되고, 소유되고, 적어도 부분적으로 제어되고 그리고/또는 달리 제공될 수 있다. 새로운 보안 계층을 제공 및/또는 더 매끄러운 사용자 경험을 제공하기 위하여, 상업적 개체 서브시스템(400)의 컴포넌트들은 서로 그리고 금융 기관 서브시스템(350) 및/또는 전자 디바이스(100) 및/또는 판매자 서브시스템(200)과 집합적으로 상호작용할 수 있다.

[0042] 상업적 개체 서브시스템(400)의 SMP 브로커 컴포넌트(440)는 상업적 개체 사용자 계정으로 사용자 인증을 관리하도록 구성될 수 있다. SMP 브로커 컴포넌트(440)는 또한 디바이스(100) 상의 크리덴셜들의 수명 주기 및 발급을 관리하도록 구성될 수 있다. SMP 브로커 컴포넌트(440)는 디바이스(100) 상의 사용자 인터페이스 요소들(예컨대, GUI(180)의 요소들)을 제어할 수 있는 1차 종점(primary end point)일 수 있다. 최종 사용자 디바이스의 운영 체제 또는 다른 애플리케이션(예컨대, 디바이스(100)의 애플리케이션(103), 애플리케이션(113), 및/또는 애플리케이션(143))은 특정 애플리케이션 프로그래밍 인터페이스("API")를 호출하도록 구성될 수 있고, SMP 브로커(440)는 이러한 API들의 요청을 처리하여 디바이스(100)의 사용자 인터페이스를 유도할 수 있는 데이터로 응답하고/하거나 (예컨대, 상업적 개체 서브시스템(400)과 전자 디바이스(100) 간의 통신 경로(65)를 통해) 보안 요소(145)와 교환할 수 있는 애플리케이션 프로토콜 데이터 유닛("APDU")으로 응답하도록 구성될 수 있다. 그러한 APDU들은 금융 기관 서브시스템(350)으로부터 시스템(1)의 신뢰 서비스 관리자("TSM")(예컨대, 상업적 개체 서브시스템(400)과 금융 기관 서브시스템(350) 간의 통신 경로(55)의 TSM)를 통해 상업적 개체 서브시스템(400)에 의해 수신될 수 있다. 상업적 개체 서브시스템(400)의 SMP TSM 컴포넌트(450)는 금융 기관 서브시스템(350)으로부터 디바이스(100) 상의 크리덴셜 발급 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, 상업적 개체 서브시스템(400)과 금융 기관 서브시스템(350) 간의 보안 데이터 통신을 위하여 디바이스(100)의 보안 요소(145)와 TSM 간의 적절한 통신 및/또는 민감한 계좌 데이터의 발급을 하도록 SMP TSM 컴포넌트(450)를 인에이블할 수 있다.

[0043] SMP TSM 컴포넌트(450)는 HSM 컴포넌트(490)를 이용하여 그것의 키들을 보호하고 새로운 키들을 생성하도록 구성될 수 있다. 상업적 개체 서브시스템(400)의 SMP 암호 서비스 컴포넌트(460)는, 사용자 인증 및/또는 시스템(1)의 다양한 컴포넌트들 사이의 기밀 데이터 전송에 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 이용할 수 있다. SMP 암호 서비스 컴포넌트(460)의 결제 암호 서비스는 IDMS 컴포넌트(470)와 상호작용하여 파일 상(on-file) 신용 카드와 연관된 정보 또는 상업적 개체의 사용자 계정(예컨대, 애플 아이클라우드(Apple iCloud™) 계정)과 연관된 다른 유형들의 상거래 크리덴셜들을 검색하도록 구성될 수 있다. 그러한 결제 암호 서비스는, 그것의 사용자 계정들의 상업 크리덴셜들(예컨대, 신용 카드 번호들)을 설명하는 암호화되지 않은(clear) 텍스트(예컨대, 비-해싱된(non-hashed)) 정보를 메모리 내에 가질 수 있는 상업적 개체 서브시스템(400)의 유일한 컴포넌트이도록 구성될 수 있다. IDMS 컴포넌트(470)는 디바이스(100)와 다른 디바이스 간의 임의의 적합한 통신, 예컨대, 신분 서비스("IDS") 수송을 인에이블 및/또는 관리하도록 구성

될 수 있다(예컨대, 상업적-개체 특정 서비스(예컨대, 애플 인크의 아이메시지(iMessage™))를 이용함). 예를 들어, 소정 디바이스들은 자동으로 또는 수동으로 이러한 서비스에 등록될 수 있다(예컨대, 상업적 개체(400)의 에코-시스템 내의 모든 디바이스들이 자동으로 서비스에 등록될 수 있음). 이러한 서비스는 메시지들이 서비스를 이용하여(예컨대, 디바이스(100)의 IDS 애플리케이션(103c)을 이용하여) 송신될 수 있기 전에 활성 등록을 요구할 수 있는 엔드 투 엔드 암호화 메커니즘을 제공할 수 있다. IDMS 컴포넌트(470) 및/또는 임의의 다른 적합한 서버 또는 상업적 개체 서브시스템(400)의 일부분은 주어진 사용자 계정과 연관된 임의의 전자 디바이스들 또는 다른 것들 상에 발급된 임의의 크리덴셜들의 상태를 식별 또는 다른 방식으로 검색하도록 동작할 수 있어서, 상업적 개체 서브시스템(400)은 특정 사용자 계정과 연관된 특정 클라이언트 디바이스(예컨대, 상업적 개체 서브시스템(400)과 패밀리 계정의 다수의 디바이스들)에 이용가능할 수 있는 하나 이상의 비-원시 결제 크리덴셜들을 효율적으로 그리고 효과적으로 식별하도록 동작할 수 있다. 상업적 개체 서브시스템(400)의 상업적 개체 사기 시스템 컴포넌트(480)는, 상업 크리덴셜 및/또는 사용자에게 관하여 상업적 개체에 알려진 데이터에 기초하여(예를 들어, 상업적 개체와의 사용자 계정과 연관된 데이터(예컨대, 상업 크리덴셜 정보) 및/또는 상업적 개체의 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), 상업 크리덴셜에 대해 상업적 개체 사기 체크를 실행하도록 구성될 수 있다. 상업적 개체 사기 시스템 컴포넌트(480)는 다양한 인자 또는 임계치에 기초하여 크리덴셜에 대한 상업적 개체 사기 점수를 결정하도록 구성될 수 있다. 추가적으로 또는 대안적으로, 상업적 개체 서브시스템(400)은 스토어(420)를 포함할 수 있으며, 이는 디바이스(100)의 사용자들에 대한 다양한 서비스의 제공자일 수 있다(예를 들어, 디바이스(100)에 의해 재생되는 미디어를 판매/대여하기 위한 아이튠즈™ 스토어, 디바이스(100) 상에서 사용할 애플리케이션들을 판매/대여하기 위한 애플 앱 스토어™, 디바이스(100)로부터의 데이터를 저장 및/또는 다수의 사용자 디바이스 및/또는 다수의 사용자 프로필을 서로 연관시키기 위한 애플 아이클라우드™ 서비스, 다양한 애플 제품을 온라인에서 구입하기 위한 애플 온라인 스토어 등). 단지 하나의 예로서, 스토어(420)는 애플리케이션(113)을 관리하고 (예컨대, 통신 경로(65)를 통해) 디바이스(100)에 제공하도록 구성될 수 있는데, 애플리케이션(113)은 임의의 적합한 애플리케이션, 예컨대, बैंकिंग 애플리케이션, 상업적 판매자 애플리케이션, 이메일 애플리케이션, 텍스트 메시징 애플리케이션, 인터넷 애플리케이션, 카드 관리 애플리케이션, 또는 임의의 다른 적합한 통신 애플리케이션일 수 있다. 임의의 적합한 통신 프로토콜 또는 통신 프로토콜들의 조합이, 상업적 개체 서브시스템(400)의 다양한 컴포넌트들 사이에서 (예컨대, 도 4의 적어도 하나의 통신 경로(495)를 통해) 데이터를 전달하고/하거나 상업적 개체 서브시스템(400)과 시스템(1)의 다른 컴포넌트들 사이에서(예컨대, 도 1의 통신 경로(55)를 통한 금융 개체 서브시스템(350) 그리고/또는 도 1의 통신 경로(65)를 통한 전자 디바이스(100)) 데이터를 전달하기 위해 상업적 개체 서브시스템(400)에 의해 사용될 수 있다.

[0044] 도 5의 설명

[0045] 도 5는 보안 디바이스 기능에 대한 온라인 액세스를 확인하기 위한 도시화된 프로세스(500)의 흐름도이다. 전자 디바이스(100), 상업적 개체 서브시스템(400), 및 판매자 서브시스템(200)에 의해 구현되고 있는 프로세스(500)가 도시된다. 그러나, 프로세스(500)는 임의의 다른 적합한 컴포넌트들 또는 서브시스템들을 이용하여 구현될 수 있다는 것이 이해되어야 한다. 프로세스(500)는 판매자 서브시스템(200)에 의한 전자 디바이스(100)의 보안 기능에 대한 온라인 액세스를 인에이블하기 위하여 제3자 판매자 서브시스템(200)을 안전하고 효율적으로 확인하기 위한 매끄러운 사용자 경험을 제공할 수 있는데, 이러한 확인은, 예컨대, 판매자 서브시스템(200)과의 트랜잭션(예컨대, 온라인 결제 또는 비접촉식 근접성 기반 결제)에서 전자 디바이스(100) 상의 크리덴셜의 안전한 사용을 인에이블하거나 또는 판매자 서브시스템(200)에 의한 전자 디바이스(100)로부터의 임의의 다른 적합한 데이터(예컨대, 위치 데이터, 건강 데이터, 또는 임의의 기타 개인적 데이터 또는 유효하게 확인되지 않은 제3자 서브시스템과 공유되지 않도록 해야 하는 기타 데이터)의 보안 액세스를 인에이블하기 위한 상업적 개체 서브시스템(400)에 의한 판매자 서브시스템(200)의 확인이다. 용어 "판매자"는 판매자 서브시스템(200) 및/또는 그것의 임의의 특징부, 예컨대, 판매자 온라인 리소스 또는 키 또는 서버 또는 단말기 또는 식별자를 설명하는 데 활용될 수 있지만, 서브시스템(200)은 전자 디바이스(100)의 소유자 또는 사용자 및/또는 상업적(또는 관리) 개체 서브시스템(400)과 구분될 수 있는 임의의 적합한 제3자 개체에 의해 동작되는 임의의 적합한 서브시스템(예컨대, 프로세싱 서브시스템(예컨대, 데이터 프로세싱 서브시스템))일 수 있음이 이해될 것이다. 예를 들어, 판매자 서브시스템(200)은 전자 디바이스(100)의 보안 디바이스 기능에 액세스하거나 또는 다른 방식으로 이를 수신하거나 또는 이와 상호작용하려고 시도할 수 있는(예컨대, 판매자 온라인 리소스를 이용하여 데이터를 디바이스(100) 상에 로딩하고(예컨대, 디바이스(100) 상에 결제 크리덴셜을 발급함), 디바이스(100)로부터 데이터를 수신하고(예컨대, 디바이스(100)로부터 결제 크리덴셜 데이터 또는 의료 데이터 또는 위치 데이터 또는 연

락처 데이터 또는 개인 미디어 데이터에 액세스함), 및/또는 기타 등등) 임의의 적합한 제3자 서브시스템일 수 있다. 프로세스(500)는 디바이스(100)와 임의의 적합한 판매자 서브시스템의 임의의 적합한 웹 리소스 간의 임의의 적합한 데이터의 더 안전하고 신뢰하는 교환을 인에이블하도록 동작할 수 있다. 프로세스(500)는 이러한 데이터 통신을 인에이블하기 전에 임의의 적합한 웹 리소스 또는 다른 온라인 리소스가 상업적 개체 서브시스템(400)과 신뢰 관계를 갖는지 보장하기 위하여 그것을 확인하도록 동작할 수 있다.

[0046]

프로세스(500)의 단계(501)에서, 판매자 서브시스템(200)은 상업적 개체 서브시스템(400)에 등록될 수 있다. 언급된 바와 같이, 판매자 서브시스템(200)의 판매자 온라인 리소스(113)(예컨대, 원시 앱, 도메인/URL, 또는 임의의 다른 적합한 웹 리소스, 또는 간혹 판매자 단말기)는 특정 판매자 식별자(167) 및 특정 판매자 키(157)와 연관될 수 있는데, 이들은 각각 판매자 서브시스템(200)과 상업적 개체 서브시스템(400) 간에 임의의 적합한 방식으로 안전하게 공유될 수 있고, 이러한 연관성은 상업적 개체 서브시스템(400)에 액세스가능하게 할 수 있다(예컨대, 표(430)). 일부 실시예들에서, 원시 애플리케이션의 개발자(예컨대, 원시 애플리케이션 판매자 온라인 리소스(113))는 애플리케이션을 실행하는 전자 디바이스(100)의 보안 디바이스 기능에 대한 애플리케이션 액세스(예컨대, 푸시 메시징, 클라우드 저장, 보안 요소 크리덴셜 결재 등)를 허용하는 자격들의 시스템을 이용할 수 있는데, 자격들은 (예컨대, 애플리케이션 스토어(420) 내의 전개 및/또는 표(430) 내의 애플리케이션의 판매자 키(157) 및 판매자 식별자(167)를 안전하게 연관시키기 위하여) 애플리케이션을 인에이블하여 상업적 개체 서브시스템(400)에 의해 등록되도록 요구될 수 있는 코드 서명 프로세스의 일부로서 애플리케이션의 바이너리에 서명될 수 있고, 예를 들어, 판매자 식별자(167)는 애플리케이션의 자격의 일부를 형성할 수 있다. 이러한 원시 애플리케이션과 다르게, 웹 리소스들(예컨대, 웹사이트 판매자 온라인 리소스(113))은 (예컨대, 상업적 개체 서브시스템(400)에 의해) 전자 디바이스(100) 상에서 실행되도록 동작하는 원시 애플리케이션들에 제공될 수 있는 코드-서명 또는 유사 보호장치를 갖지 않을 수 있다. 대신에, 웹 리소스의 도메인의 소유권은 그 웹 리소스가 등록될 수 있기 전에 증명될 수 있다. 판매자 서브시스템(200)에 의해 소유되거나 또는 다른 방식으로 제어되는 웹사이트 판매자 온라인 리소스(113)를 등록하기 위하여, 이러한 소유권은 상업적 개체 서브시스템(400)이 그 판매자 온라인 리소스(113)를 등록하기 전에(예컨대, 상업적 개체 서브시스템(400)에 의한 향후 액세스를 위하여 특정 판매자 식별자(167) 및 특정 판매자 키(157)가 그 판매자 온라인 리소스(113)와 연관되고, 판매자 서브시스템(200)과 상업적 개체 서브시스템(400) 간에 공유되기 전(예컨대, 표(430))) 상업적 개체 서브시스템(400)에 증명되어야 한다. 예를 들어, 상업적 개체 서브시스템(400)에 등록될 판매자 온라인 리소스(113)의 도메인의 소유권을 증명하기 위하여, 도메인의 식별이 상업적 개체 서브시스템(400)에 제공될 수 있고, 상업적 개체 서브시스템(400)은 임의의 적합한 파일(예컨대, JSON 파일과 같은 정적 파일)을 판매자 서브시스템(200)에 제공할 수 있고, 판매자 서브시스템(200)은 (예컨대, 공유된 판매자 키(157)를 이용하여) 그 파일에 서명하고, 등록될 도메인 상의 공지된 경로에 그 파일을 호스팅할 수 있고, 이어서 상업적 개체 서브시스템(400)은 도메인으로부터 그 서명된 파일에 액세스하고 (예컨대, 공유된 판매자 키(157)를 이용하여) 파일에 서명해제하여 액세스된 파일이 판매자 서브시스템(200)과 공유된 파일과 매칭됨을 승인할 수 있다. 웹 리소스들을 등록하기 위한 일부 예시적인 프로세스들이 발명의 명칭이 "Sharing Account Data Between Different Interfaces To A Service"인 미국 특허 출원 공개 제2015/0350106호에 기재될 수 있고, 이는 본 명세서에 전체적으로 참조로서 포함된다. 임의의 적합한 프로세스 또는 프로세스들이 단계(502)에서 판매자 서브시스템(200)의 판매자 온라인 리소스(113)의 임의의 적합한 유형의 유효성을 상업적 개체 서브시스템(400)에 안전하게 등록하기 위하여 활용될 수 있고(예컨대, 디바이스 상에서 자체적으로 실행되거나 또는 원격으로 서버에 호스트되거나 또는 디바이스에 근접하게 위치하는, 임의의 원시 앱, 하이브리드 앱, 웹 리소스, 또는 심지어 전자 디바이스에 의해 활용될 판매자의 판매자 단말기), 이로써 판매자 온라인 리소스(113)와 연관된 적어도 하나의 판매자 식별자(167) 및 적어도 하나의 판매자 키(157)(예컨대, 대칭 또는 비대칭키 쌍)는 판매자 온라인 리소스(113)와 연관될 수 있고 향후 사용을 위해 판매자 서브시스템(200) 및 상업적 개체 서브시스템(400)(예컨대, 표(430) 내) 둘 모두에 액세스가능하게 될 수 있고, 임의의 적합한 데이터는 판매자 서브시스템(200)과 상업적 개체 서브시스템(400) 간에 임의의 이러한 프로세스 동안 임의의 적합한 방식으로 전달될 수 있다(예컨대, 애플리케이션(113), 키(157), 식별자(167), 및/또는 임의의 다른 적합한 데이터가 임의의 적합한 통신 프로토콜(들)을 이용하는 통신 경로(85)를 통해). 하나 이상의 판매자 식별자는 특정 판매자 온라인 리소스(113), 예컨대, 특정 판매자 온라인 리소스(113)와 고유하게 연관되는 제1 판매자 식별자(167) 및/또는 특정 판매자 서브시스템(200)의 각각의 판매자 온라인 리소스(113)와 연관된 제2 판매자 식별자(167)와 연관될 수 있다. 추가적으로 또는 대안적으로, 하나 이상의 판매자 키는 특정 판매자 식별자 또는 특정 판매자 온라인 리소스(113)와 연관될 수 있다. 단계(501)의 하나 이상의 인스턴스에서, 모든 그러한 판매자 키 및 판매자 식별자 연관성들이 상업적 개체 서브시스템(400)에 의해 저장되거나 또는 다른 방식으로 상업적 개체 서브시스템(400)에 (예컨대, 하나 이상의 표(430))

액세스가능할 수 있다.

[0047]

프로세스(500)의 단계(502)에서, 잠재적 트랜잭션 데이터는 등록된 판매자 온라인 리소스를 이용하여 판매자 서브시스템(200)과 전자 디바이스(100) 간에 교환될 수 있다. 예를 들어, 판매자 온라인 리소스 애플리케이션(113)을 실행하거나 또는 다른 방식으로 액세스하는 디바이스(100)와의 사용자 상호작용 동안(예컨대, 사용자가 온라인으로 판매자의 상품 또는 서비스를 쇼핑하는 동안 또는 사용자가 의료 전문가와 통신하는 동안) 일부 시점에, 잠재적 트랜잭션 데이터는 판매자 서브시스템(200)으로부터 또는 디바이스(100)와 판매자(또는 프로세서) 서브시스템(200)의 판매자(또는 프로세서) 간에 일어날 수 있는 잠재적 보안 데이터 트랜잭션에 관련된 임의의 적합한 데이터를 나타낼 수 있는 임의의 다른 적합한 개체로부터 디바이스(100)로 전달될 수 있으며, 임의의 적합한 데이터는 (i) 특정 판매자 정보, 예컨대, 판매자 온라인 리소스 애플리케이션(113)의 적어도 하나의 또는 각각의 판매자 식별자(167), (ii) 특정 트랜잭션 정보, 예컨대, 디바이스(100)와 판매자 서브시스템(200) 간에 공유될 특정 유형의 보안 데이터의 식별(예컨대, 금융 거래에 대한 통화 및 금액 및 결제 유형(예컨대, 디바이스(100) 상에 발급된 비자 결제 크리덴셜을 이용하여 5 미국 달러), 건강 트랜잭션에 대한 의료 데이터 유형 및 데이터 양(예컨대, 지난 3 일 동안 디바이스(100)에 의해 검출되거나 또는 다른 방식으로 획득된 특정 사용자의 심박수 데이터) 등), 및/또는 (iii) 고유 판매자 기반 트랜잭션 식별자(예컨대, 수행되고 있는 트랜잭션과의 연관성을 위해 판매자 서브시스템(200)에 의해 무작위로 또는 고유하게 생성될 수 있는, 다문자 영숫자 스트링과 같은 임의의 적합한 데이터 요소)를 포함하지만, 이에 한정되지 않는다. 이러한 잠재적 트랜잭션 데이터는, 구매하는 고객의 연락처 정보 필드(예컨대, 전화 번호, 이메일 주소, 우편 주소)와 같은 보안 데이터 트랜잭션을 완료하는 데 필요하거나 또는 적어도 사용될 수 있는 연관된 데이터를 갖거나 또는 갖지 않는 임의의 적합한 개수 및 유형의 데이터 필드들을 포함할 수 있으며, 일부 필드들은 이러한 잠재적 트랜잭션 데이터의 일부로서 추가되고 포함될 수 있고/있거나 일부 필드들은 이러한 잠재적 트랜잭션 데이터의 일부로서 추가되지 않을 수 있지만, 개방되어 있고 프로세스(500)의 뒷 부분에서 추가되기를 기다릴 수 있다. 단계(502)의 이러한 잠재적 트랜잭션 데이터는 본 명세서에서 PK데이터요청 또는 (예컨대, 금융 거래에 대한) PK결제요청이라고 지칭될 수 있다. 일부 실시예들에서, 사용자는 판매자 서브시스템(200)과 연관된 잠재적 트랜잭션 데이터가 단계(502)에서 디바이스(100)에 이용가능하게 되도록 디바이스(100)와 능동적으로 상호작용하지 않을 수 있다. 대신에, 예를 들어, 모두 자동으로 디바이스(100)의 사용자에게 의한 임의의 능동적인 상호작용 없이, 디바이스(100)는 특정 제품이 구매되어야 한다고 결정하고 특정 제품에 대한 적어도 하나의 특정 판매자로부터 연관된 트랜잭션 데이터를 획득하기 위하여 하나 이상의 판매자와 상호작용하도록 구성될 수 있다(예컨대, 디바이스(100)는 (예컨대, 더 많은 세탁 세제가 세탁기에 의해 필요함을 검출하거나 또는 사용자에게 의해 특정 날짜에 더 많은 세제를 사도록 사전설정된 캘린더 이벤트를 검출하는) 가전 제품이 구매되어야 한다고 결정하도록 구성될 수 있고, 자동으로 그 제품에 대하여 최고의 거래를 제공하는 특정 판매자를 식별할 수 있고, 판매자 온라인 리소스를 이용하여 자동으로 판매자와 상호작용하여 트랜잭션 데이터를 획득하여 판매자로부터 그 제품을 구매할 수 있는 가전 제품일 수 있음). 단계(502)의 잠재적 트랜잭션 데이터는 디바이스(100)가 잠재적 트랜잭션 데이터와 연관된 보안 데이터 트랜잭션(예컨대, 금융 거래에 자금을 제공)을 완료하기 위하여 안전하게 보안 디바이스 데이터(예컨대, 적절한 결제 크리덴셜 데이터)를 생성하고/하거나 이를 판매자 서브시스템(200)에 제공하는 데 필요한 모든 데이터를 포함할 수 있다. 이러한 잠재적 트랜잭션 데이터는 단계(502)에서 임의의 적합한 방식으로 판매자 서브시스템(200)에 의해 디바이스(100)로 전달될 수 있다(예컨대, 이러한 잠재적 트랜잭션 데이터는 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(15) 또는 임의의 적합한 통신 프로토콜을 이용하는 단말기(220)와 NFC 컴포넌트(120) 간의 비접촉식 근접성 기반 통신 채널을 통해 판매자 서브시스템(200)의 서버(210)로부터 디바이스(100)의 통신 컴포넌트(106)로 전송될 수 있음).

[0048]

프로세스(500)의 단계(504)에서, 판매자 온라인 리소스 확인 세션이 개시될 수 있다. 이는, 전자 디바이스(100)가 보안 데이터 트랜잭션(예컨대, 단계(502)의 잠재적 트랜잭션 데이터에 의해 식별된 보안 데이터 트랜잭션)이 발생해야 함을 나타내는 것에 응답하여(예컨대, 디바이스(100)의 사용자가 단계(502)의 판매자 온라인 리소스의 잠재적 트랜잭션 데이터에 의해 식별된 보안 데이터 트랜잭션을 수행하려는 사용자의 바람을 전달하기 위하여 판매자 온라인 리소스의 GUI 구성요소(예컨대, 라디오 버튼)를 선택하는 것에 응답하여, 또는 임의의 적합한 요구조건들이 충족되는 것에 자동으로 기초하여(예컨대, 단순히 단계(502)의 잠재적 트랜잭션 데이터가 디바이스(100)에 전달되는 것에 응답하여)) 일어날 수 있다. 판매자 온라인 리소스로 특정 보안 데이터 트랜잭션을 수행하려는 이러한 의도가 결정되면, 디바이스(100) 상의 판매자 온라인 리소스(113)는 데이터 트랜잭션 요청을 생성 및 카드 관리 애플리케이션(103b) 또는 디바이스(100) 상의 임의의 다른 적합한 디바이스 애플리케이션에 송신하도록 동작할 수 있고, 그 디바이스 애플리케이션(103b)은 단계(504)에서 판매자 확인 세션 개시 데이터를 생성 및 판매자 서브시스템(200)에 전달하도록 동작할 수 있다. 수행될 특정 보안 데이터 트랜잭션에

대한 판매자 온라인 리소스 확인 세션을 개시하기 위하여, 임의의 적합한 데이터가 단계(504)에서 전자 디바이스(100)에 의해 생성되고/되거나 판매자 확인 세션 개시 데이터로서 판매자 서브시스템(200)에 전달될 수 있다. 예를 들어, 디바이스(100)에 의해 확인 세션 식별자가 생성되고 단계(504)에서 판매자 확인 세션 개시 데이터의 적어도 일부분으로서 판매자 서브시스템(200)에 전달될 수 있는데, 이러한 확인 세션 식별자는 개시되고 있는 현재 판매자 온라인 리소스 확인 세션을 고유하게 식별(예컨대, 적어도 소정 기간 동안 판매자 서브시스템(200) 및/또는 상업적 개체 서브시스템(400)에 대한 이러한 것을 고유하게 식별)할 수 있는 임의의 적합한 영숫자 스트링 또는 임의의 다른 적합한 식별자일 수 있다. 디바이스(100)에 의해 생성되면, 확인 세션 식별자는 상업적 개체 서브시스템(400)에 대하여 디바이스(100)의 고유 식별자(예컨대, 디바이스 식별자(119) 또는 디바이스(100)에 대하여(예컨대, 상업적 개체 서브시스템(400)에 대하여) 고유할 수 있는 디바이스(100)의 보안 요소(145)의 고유 보안 요소 식별자)를 활용하여 확인 세션 식별자를 생성함으로써 고유할 수 있다. 추가적으로 또는 대안적으로, 단계(504)에서 판매자 확인 세션 개시 데이터의 적어도 일부분으로서 챌린지 요청 타겟 식별자(예컨대, Challenge Request URL)가 디바이스(100)에서 판매자 서브시스템(200)으로 전달될 수 있는데, 이러한 챌린지 요청 타겟 식별자는 판매자 서브시스템(200)이 판매자를 확인하기 위하여 통신할 개체를 식별할 수 있다(예컨대, URL은 수행될 특정 보안 데이터 트랜잭션에 대한 판매자 온라인 리소스를 확인하기 위하여 판매자 서브시스템(200)과 작업할 수 있는 상업적 개체 서브시스템(400)의 서버(410)를 식별함). 디바이스 애플리케이션(예컨대, 카드 관리 애플리케이션(103b)(예컨대, 지갑 애플리케이션))은 임의의 적합한 운영 체제의 일부 또는 애플리케이션 업데이트로서 프로그래밍되는 이러한 챌린지 요청 타겟 식별자를 가질 수 있는데, 애플리케이션 업데이트는 상업적 개체 서브시스템(400)에 의해 제어될 수 있어서 챌린지 요청 타겟 식별자가 디바이스(100) 상에서 상업적 개체 서브시스템(400)에 의해 임의의 적합한 시간에 업데이트될 수 있도록 한다. 추가적으로 또는 대안적으로, 이러한 판매자 확인 세션 개시 데이터는 임의의 다른 적합한 데이터, 예컨대, 스스로 확인하기 위한 판매자에 대한 요청을 나타내는 임의의 적합한 데이터, 디바이스(100)를 나타내는 임의의 적합한 데이터(예컨대, 디바이스 식별자(119)), 및/또는 수행될 특정 보안 데이터 트랜잭션을 나타내는 임의의 적합한 데이터(예컨대, 단계(502)의 잠재적 트랜잭션 데이터로부터의 임의의 적합한 데이터, 예컨대, 특정 판매자 정보(예컨대, 판매자 식별자(167)), 특정 트랜잭션 정보(예컨대, 금융 거래에 대한 통화 및 금액 및 결제 유형 또는 건강 트랜잭션에 대한 의료 데이터 유형 및 데이터 량), 및/또는 고유 판매자 기반 트랜잭션 식별자를 포함할 수 있다. 단계(504)에서 임의의 적합한 판매자 확인 세션 개시 데이터가 디바이스(100)에 의해 판매자 서브시스템(200)으로 임의의 적합한 방식으로 전달될 수 있다(예컨대, 이러한 판매자 확인 세션 개시 데이터는 디바이스(100)의 통신 컴포넌트(106)로부터 판매자 서브시스템(200)의 서버(210)로 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(15)를 통해 또는 임의의 적합한 통신 프로토콜을 이용하는 NFC 컴포넌트(120)와 단말기(220) 간의 비접촉식 근접성 기반 통신 채널을 통해 전송될 수 있음).

[0049]

프로세스(500)의 단계(506)에서, 판매자 서브시스템(200)이 단계(504)에서 확인 세션을 개시하기 위해 디바이스(100)로부터 임의의 적합한 판매자 확인 세션 개시 데이터를 수신하는 것에 응답하여, 판매자 서브시스템(200)은 판매자 온라인 리소스를 확인하기 위하여 상업적 개체 서브시스템(400)과 통신하도록 동작할 수 있다. 일부 실시예들에서, 단계(504)의 판매자 확인 세션 개시 데이터가 확인 세션 식별자를 포함하지 않는 경우, 판매자 서브시스템(200)은 개시되고 있는 현재 판매자 온라인 리소스 확인 세션을 고유하게 식별할 수 있는 이러한 확인 세션 식별자를 생성하도록 동작할 수 있다. 판매자 서브시스템(200)에 의해 생성되면, 판매자 서브시스템(200)이 동일한 확인 세션 식별자를 적어도 동일한 상업적 개체 서브시스템에 대하여 및/또는 동일한 판매자 식별자에 대하여 및/또는 세션 식별자가 상업적 개체 서브시스템에서 임의의 특정 프로세스에 계류중이 아님을 보장하는 데 적절한 소정 기간 내에, 두 번 사용하지 않음을 보장함으로써 확인 세션 식별자는 상업적 개체 서브시스템(400)에 대하여 고유할 수 있다. 단계(506)는 (예컨대, 단계들(502, 504)에서 식별된 바와 같이) 수행될 특정 보안 데이터 트랜잭션에 대한 판매자 온라인 리소스를 확인하도록 상업적 개체 서브시스템(400)을 인에이블할 수 있는 임의의 적합한 개수의 서브 프로세스들을 포함할 수 있다. 도 6의 프로세스(600)의 단계들(614 내지 622)에 대하여 상세하게 기재된 바와 같이, 단계(506)의 확인은, 판매자 서브시스템(200)이 상업적 개체 서브시스템(400)으로(예컨대, 단계(504)에서 디바이스(100)로부터의 판매자 확인 세션 개시 데이터에 의해 식별될 수 있는 것과 같이) 확인될 판매자 온라인 리소스와 연관된 판매자 식별자(예컨대, 단계(501)에서 등록된 것과 같은 판매자 식별자(167), 이는 판매자 온라인 웹 리소스의 도메인일 수 있음), 확인 세션 식별자(예컨대, 단계(504)에서 디바이스(100)에 의해 또는 단계(506)에서 판매자 서브시스템(200)에 의해 생성되는 것과 같음), 및 임의의 다른 적합한 데이터(예컨대, 디바이스(100)를 식별하는 데이터 및/또는 수행될 특정 보안 데이터 트랜잭션을 식별하는 데이터)를 포함할 수 있는 챌린지 요청을 전달하는 것을 포함할 수 있다. 이러한 챌린지 요청은 판매자 서브시스템(200)에 의해 (예컨대, HTTP 헤더에서 또는 다른 방식으로) 챌린지 요청의 판매자 식별

자와 연관된 판매자 키(예컨대, 단계(501)에서 판매자 식별자(167)를 이용하여 (예컨대, 확인될 판매자 온라인 리소스(113)에 대하여) 등록된 바와 같은 판매자 키(157))를 이용하여 서명될 수 있다. 상업적 개체 서브시스템(400)은 이러한 챌린지 요청을 수신하고, 챌린지 요청의 판매자 식별자(167)에 의해 (예컨대, (예컨대, 표(430) 내의 판매자 식별자(167)를 식별함으로써) 판매자 온라인 리소스(113)가 단계(501)에서 등록되었고, 여전히 유효함을 승인하기 위하여) 식별된 판매자 온라인 리소스(113)를 확인하고, 챌린지 요청의 서명을 (예컨대, 표(430)의 그 식별된 판매자 식별자(167)와 연관된 판매자 키(157)를 이용하여) 확인하도록 동작할 수 있다. 챌린지 요청의 구성요소들을 확인하는 것에 응답하여, 상업적 개체 서브시스템(400)은 챌린지 데이터(예컨대, 엔트로피를 통한 임의의 적합한 무작위 데이터)를 생성하고, 식별자 데이터에 대하여 챌린지 데이터를(예컨대, 챌린지 요청의 확인 세션 식별자 및 판매자의 판매자 식별자 중 하나 또는 둘 모두) 임의의 적합한 데이터 구조로 (예컨대, 표(430) 또는 다른 방식으로) 저장하고, 상업적 개체 서브시스템(400)에 의해 액세스가능한 판매자 키(157)(예컨대, 챌린지 요청의 서명을 확인하는 데 사용되는 표(430)의 판매자 키)를 이용하여 챌린지 데이터를 암호화하고, 이어서 암호화된 챌린지 데이터 및 임의의 다른 적합한 데이터, 예컨대, 챌린지 데이터를 암호화하는 데 사용되는 판매자 키의 해시(예컨대, 판매자 서브시스템(200)에 의해 적절한 판매자 키(157)(예컨대, 챌린지 데이터를 복호화하기 위한 판매자 서브시스템(200)의 개인키(157))를 식별하는 데 사용될 수 있는 표(430)의 공개 판매자 키(157)의 해시 버전, 이는 다수의 등록된 판매자 온라인 리소스들 및/또는 다수의 판매자 키들을 가질 수 있는 판매자를 지원하도록 제공될 수 있음), 챌린지 요청의 확인 세션 식별자 등을 함께 포함할 수 있는 챌린지 데이터를 판매자 서브시스템(200)에 전달할 수 있다. 이러한 챌린지 데이터를 수신하는 것에 응답하여, 판매자 서브시스템(200)은 적절한 판매자 키(157)(예컨대, 판매자 서브시스템(200)에 단계(501)에서 등록될 수 있었던 개인 판매자 키(157))를 이용하여 암호화된 챌린지 데이터를 복호화하고, 이어서 복호화된 챌린지 데이터 및 임의의 다른 적합한 데이터, 예컨대, 챌린지 요청의 확인 세션 식별자 및 적절한 판매자 식별자를 함께 포함하는 챌린지 응답 데이터를 상업적 개체 서브시스템(400)에 전달하도록 동작할 수 있고, 그 챌린지 응답은 판매자 서브시스템(200)에 의해(예컨대, HTTP 헤더에서 또는 다른 방식으로) 챌린지 요청의 판매자 식별자와 연관된 판매자 키(예컨대, 단계(501)에서 판매자 식별자(167)를 이용하여 (예컨대, 확인될 판매자 온라인 리소스(113)에 대하여) 등록된 바와 같은 판매자 키(157))를 이용하여 서명될 수 있다. 이러한 챌린지 응답 데이터를 수신하는 것에 응답하여, 상업적 개체 서브시스템(400)은 챌린지 응답의 서명을 (예컨대, 표(430)의 식별된 판매자 식별자(167)와 연관된 판매자 키(157)를 이용하여) 확인하고, 챌린지 응답의 복호화된 챌린지 데이터가 챌린지 응답의 확인 세션 식별자 및/또는 판매자의 식별자(예컨대, 표(430))에 대하여 저장됨을 승인하도록 동작할 수 있다. 일부 실시예들에서, 챌린지 데이터와 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두 간의 이러한 저장된 링크는 링크가 자동으로 소거되기 전에 제한된 길이의 시간 동안만 유지될 수 있어서, 판매자 서브시스템(200)은, 그것이 특정 확인 세션에 대한 판매자 온라인 리소스를 확인하기 위해서 챌린지 데이터를 수신한 뒤 적절한 챌린지 응답 데이터를 상업적 개체 서브시스템(400)에 송신해야 하는 소정 지속 시간에 제한될 수 있으며(예컨대, 상업적 개체 서브시스템(400)은 소정 기간 후에 챌린지 데이터와 상업적 개체 서브시스템(400)의 확인 세션 식별자 및/또는 판매자 식별자 간의 이러한 연관성을 제거하도록(예컨대, 링크가 생성되고 10 분 이하(또는 임의의 다른 적합한 기간) 후에 표(430)로부터의 링크를 제거) 동작할 수 있음), 이는 트랜잭션의 보안을 증가시킬 수 있다. 따라서, 단계(506)에서 수행될 특정 보안 데이터 트랜잭션에 대한 판매자 온라인 리소스의 확인(예컨대, 단계들(502, 504)에서 식별되는 바와 같이)은 상업적 개체 서브시스템(400)에서의 판매자 키와 판매자 식별자 간의 연관성을 이용하여 완료될 수 있다(예컨대, 단계(501)에서 등록된 바와 같음). 임의의 적합한 데이터는 판매자 서브시스템과 상업적 개체 서브시스템(400) 간에 단계(506)에서 임의의 적합한 방식으로 교환될 수 있다(예컨대, 이러한 데이터는 판매자 서브시스템(200)의 서버(210)와 상업적 개체 서브시스템(400)의 서버(410) 간에 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(85)를 통해 전송될 수 있음).

[0050]

단계(508)에서, 단계(504)에서 개시된 확인 세션에 기초하여 단계(506)에서 판매자 온라인 리소스를 확인하는 것에 응답하여, 상업적 개체 서브시스템(400)은 확인 데이터를 생성하고 그것을 식별자 데이터, 예컨대, 확인 세션의 확인 세션 식별자 및/또는 판매자 식별자에 대하여 저장할 수 있다. 예를 들어, 챌린지 응답의 서명을 확인하는 것에 응답하여 그리고 챌린지 데이터 및 챌린지 응답의 확인 세션 식별자 및/또는 판매자 식별자가 또한 상업적 개체 서브시스템(400)에서(예컨대, 표(430)에) 적절히 링크되어 있음을 승인하는 것에 응답하여, 단계(508)에서 상업적 개체 서브시스템(400)은 그 링크를 소모하고(예컨대, 상업적 개체 서브시스템(400)에서 챌린지 데이터와 확인 세션 식별자 및/또는 판매자 식별자 간의 이러한 연관성을 제거하고(예컨대, 표(430)로부터 링크를 제거함)), 확인 데이터(예컨대, 임의의 적합한 무작위 데이터(예컨대, 암호화 난스(cryptographic nonce)(예컨대, 엔트로피를 통한 임의의 적합한 무작위 데이터)))를 생성하고, 이어서 확인 데이터를 챌린지 요

청의 확인 세션 식별자 및/또는 챌린지 응답의 확인 세션 식별자에 대하여 또는 다른 방식으로 이와 관련하여 저장하고/하거나 판매자의 판매자 식별자에 대하여(예컨대, 임의의 적합한 데이터 구조로, 예컨대 표(430) 또는 다른 방식으로) 저장할 수 있다.

[0051]

단계(510)에서, 단계(506)에서 판매자 온라인 리소스를 확인하고, 이어서 단계(508)에서 임의의 적합한 확인 데이터를 확인 세션 식별자 및/또는 판매자 식별자에 대하여 저장하는 것에 응답하여, 상업적 개체 서브시스템(400)은 확인 응답 데이터를 전자 디바이스(100)에 전달할 수 있는데, 이러한 확인 응답 데이터는 임의의 적합한 데이터를 포함할 수 있으며, 임의의 적합한 데이터는 단계(508)의 확인 데이터, 단계(508)의 확인 세션 식별자, 단계(506)에서 확인된 판매자 온라인 리소스를 식별하는 데이터(예컨대, 판매자 식별자(167)), 및/또는 임의의 다른 적합한 데이터를 포함하지만, 이에 한정되지 않는다. 일부 실시예들에서, 도 5에 도시된 바와 같이, 이러한 확인 응답 데이터는 상업적 개체 서브시스템(400)으로부터 직접 전자 디바이스(100)로 (예컨대, 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(65)를 통해) 전달될 수 있는데, 전자 디바이스(100)를 식별하는 데이터(예컨대, 디바이스 식별자(119))는 (예컨대, 단계(502)에서 또는 다른 방식으로) 확인 세션 식별자와 연관되고 단계(506)의 확인과 연관되어 상업적 개체 서브시스템(400)이 확인 응답 데이터를 적절한 전자 디바이스(100)에 전달할 수 있도록 할 수 있다. 대안적으로, 일부 실시예들에서, 이러한 확인 응답 데이터는 상업적 개체 서브시스템(400)으로부터 전자 디바이스(100)로 판매자 서브시스템(200)을 통해 전달될 수 있는데, 이로써 판매자 서브시스템(200)은 상업적 개체 서브시스템(400)으로부터 (예컨대, 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(85)를 통해) 확인 응답 데이터를 수신하고, 이어서 확인 응답 데이터의 적어도 일부분을 전자 디바이스(100) 상으로 (예컨대, 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(15)를 통하거나 또는 비접촉식 근접성 기반 통신으로서) 전달할 수 있다. 이러한 확인 데이터는 상업적 개체 서브시스템(400)에 의해 (예컨대, HTTP 헤더에서 또는 다른 방식으로) 전자 디바이스(100)에 또한 액세스가능할 수 있는 상업적 개체 서브시스템(400)과 연관된 액세스 키(예컨대, 보안 요소(145)의 액세스 키(155a), 액세스 키(155b), CRS(151k), 및/또는 ISD 키(156k) 또는 디바이스 애플리케이션(예컨대, 카드 관리 애플리케이션(103b))에 알려질 수 있는 임의의 키)를 이용하여 서명될 수 있어서, 디바이스(100)는 서명된 확인 데이터를 수신하게 되면 서명을 확인하여 전자 디바이스(100)에 의해 신뢰받지 않는 다른 개체 서브시스템이 아닌, 상업적 개체 서브시스템(400)이 확인 데이터를 생성했음을 승인할 수 있다.

[0052]

프로세스(500)의 단계(512)에서, 보안 디바이스 데이터는 디바이스(100)에 의해 적어도 부분적으로 생성 또는 액세스될 수 있고, 이어서 단계(514)에서, 이러한 보안 디바이스 데이터는 단계(510)에서 수신된 확인 응답 데이터의 적어도 일부분 및 단계(502)의 잠재적 트랜잭션 데이터의 적어도 일부분과 함께 상업적 개체 서브시스템(400)으로 디바이스(100)에 의해 디바이스 트랜잭션 데이터로서 전달될 수 있다. 예를 들어, 단계(502)의 잠재적 트랜잭션 데이터에 사용되고 있는 판매자 온라인 리소스의 유효성을 나타낼 수 있는 단계(510)의 확인 응답 데이터를 수신하는 것에 응답하여, 디바이스(100)는 특정 보안 데이터 트랜잭션을 수행하기 위하여 판매자 서브시스템(200)과 공유될 보안 데이터를 단계(512)에서 획득하거나 또는 다른 방식으로 식별하도록 동작할 수 있다 (예컨대, 금융 거래에 사용하기 위한 결제 크리덴셜 데이터를 생성하거나 또는 건강 트랜잭션에 공유될 특정 건강 데이터를 수집함). 이어서, 단계(514)에서, 디바이스(100)는 단계(512)의 그 보안 데이터를, 확인 데이터 및 단계(510)의 확인 응답 데이터의 확인 세션 식별자 및 판매자 식별자와 함께 및/또는 수행될 잠재적 보안 데이터 트랜잭션에 관련된 임의의 적합한 데이터와 함께(예컨대, 단계(502)의 잠재적 트랜잭션 데이터, 예컨대, 특정 판매자 정보(예컨대, 판매자 식별자(167)), 특정 트랜잭션 정보(예컨대, 금융 거래에 대한 통화 및 금액 및 결제 유형 또는 건강 트랜잭션에 대한 의료 데이터 유형 및 데이터 량), 및/또는 고유 판매자 기반 트랜잭션 식별자에 의해 디바이스(100)에 제공될 수 있는 것과 같음) 상업적 개체 서브시스템(400)에 대한 디바이스 트랜잭션 데이터로서 전달할 수 있다. 따라서, 단계(514)에서 디바이스(100)로부터 상업적 개체 서브시스템(400)으로 전달된 디바이스 트랜잭션 데이터는 단계(502)의 일부 또는 모든 잠재적 트랜잭션 데이터뿐만 아니라 단계(512)의 보안 디바이스 데이터 및 단계(510)의 확인 응답 데이터를 포함할 수 있다.

[0053]

디바이스(100)은 단계(514)에서 디바이스 트랜잭션 데이터를 상업적 개체 서브시스템(400)에 전달하기 전에, 단계(514)의 디바이스 트랜잭션 데이터의 전부 또는 적어도 일부분을(예컨대, 단계(512)의 보안 디바이스 데이터) 상업적 개체 키를 이용하여 암호화할 수 있다. 예를 들어, 디바이스(100)는 디바이스 트랜잭션 데이터의 적어도 일부분을 보안 요소(145)의 액세스 키(155a), 액세스 키(155b), CRS(151k), CASD(158k), 및/또는 ISD 키(156k) 또는 (예컨대, 임의의 디바이스 애플리케이션(103)으로부터 또는 다른 방식으로 프로세서(102)로) 디바이스(100)에 액세스가능한 임의의 기타 키를 이용하여 암호화할 수 있고, 이는 또한 상업적 개체 서브시스템(400)(예컨대, 디바이스(100)와 상업적 개체 서브시스템(400) 간의 임의의 공유 비밀)에 액세스가능할 수 있다. 일부 실시예들에서, 이러한 상업적 개체 키 또는 액세스 키는 상업적 개체 서브시스템(400)의 체계와 연관된 상

업적 개체 공개키일 수 있고, 이를 이용하여 상업적 개체 서브시스템(400)은 연관된 상업적 개체 개인키에 액세스할 수 있다. 상업적 개체 서브시스템(400)은 이러한 상업적 개체 공개키를 디바이스(100)에 임의의 적합한 방식으로 제공할 수 있다. 디바이스 트랜잭션 데이터는, 적어도 부분적으로 암호화되고/되거나 임의의 적합한 상업적 개체 키에 의해 서명되어있는지 상관없이, 디바이스(100)에 의해 상업적 개체 서브시스템(400)으로 단계(540)에서 임의의 적합한 방식으로 전달될 수 있다(예컨대, 이러한 디바이스 트랜잭션 데이터는 디바이스(100)의 통신 컴포넌트(106)로부터 상업적 개체 서브시스템(400)의 서버(410)로 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(65)를 통해 전송될 수 있음).

[0054]

다음, 단계(514)에서 전달된 디바이스 트랜잭션 데이터를 수신한 후에, 프로세스(500)의 단계(516)는 상업적 개체 서브시스템(400)이 단계(514)에서 수신된, 수신된 디바이스 트랜잭션 데이터의 확인 데이터를 확인하는 것을 포함할 수 있다. 예를 들어, 이러한 디바이스 트랜잭션 데이터를 수신하는 것에 응답하여, 상업적 개체 서브시스템(400)은 단계(516)에서 디바이스 트랜잭션 데이터로부터 확인 응답 데이터를 식별하고, 그 수신된 확인 응답 데이터의 확인 데이터가 수신된 디바이스 트랜잭션 데이터(예컨대, 확인 응답 데이터)의 확인 세션 식별자에 대하여 및/또는 수신된 디바이스 트랜잭션 데이터(예컨대, 확인 응답 데이터)의 판매자 식별자에 대하여 저장되어 있음을(예컨대, 표(430)) 승인하도록 동작할 수 있다. 일부 실시예들에서, 확인 데이터와 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두 간의 이러한 저장된 링크는 링크가 자동으로 소거되기 전에 제한된 길이의 시간 동안만 유지될 수 있어서, 전자 디바이스(100)는, 그것이 단계(510)에서 확인 응답 데이터를 수신한 뒤, 확인된 판매자 온라인 리소스를 이용하여 특정 보안 데이터 트랜잭션을 수행하기 위하여 상업적 개체 서브시스템(400)에 의해 보호되는 디바이스 트랜잭션 데이터의 보안 디바이스 데이터를 인에이블하기 위하여 단계(514)에서 상업적 개체 서브시스템(400)에 디바이스 트랜잭션 데이터를 송신해야 하는 소정 지속 시간에 제한될 수 있으며(예컨대, 상업적 개체 서브시스템(400)은 소정 기간 후에 확인 데이터와 상업적 개체 서브시스템(400)의 확인 세션 식별자 및/또는 판매자 식별자 간의 이러한 연관성을 제거하도록(예컨대, 링크가 생성되고 10분(또는 임의의 다른 적합한 기간) 이내에 표(430)로부터의 링크를 제거) 동작할 수 있으며, 이는 트랜잭션의 보안을 증가시킬 수 있음). 추가적으로 또는 대안적으로, 확인 데이터와 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두 간의 저장된 링크는 또한 단계(508)에서 판매자 서브시스템(200)에 의해 단계(506) 동안(예컨대, 챌린지 요청의 일부분으로서) 상업적 개체 서브시스템(400)에 이용가능할 수 있는 임의의 적합한 특정 트랜잭션 정보, 예컨대, 디바이스(100)와 판매자 서브시스템(200) 간에 공유될 특정 유형의 보안 데이터의 식별(예컨대, 금융 거래에 대한 통화 및 금액 및 결제 유형(예컨대, 디바이스(100) 상에 발급된 비자 결제 크리덴셜을 이용하여 5 미국 달러), 건강 트랜잭션에 대한 의료 데이터 유형 및 데이터 량(예컨대, 지난 3 일 동안 디바이스(100)에 의해 검출되거나 또는 다른 방식으로 획득된 특정 사용자의 심박수 데이터) 등)과 연관될 수 있고, 유사한 특정 트랜잭션 정보는 또한 전자 디바이스(100)에 의해 단계(514)의 디바이스 트랜잭션 데이터의 일부로서 상업적 개체 서브시스템(400)에 이용가능할 수 있어서, 단계(516)는 또한 상업적 개체 서브시스템(400)이 단계(514)에서 수신된 확인 데이터에 대하여(예컨대, 단계(508)에서 표(430)에 저장된 바와 같이) 현재 저장된 특정 트랜잭션 정보가 적어도 단계(514)에서 수신된 특정 트랜잭션 정보와 특정 정도로 유사함을 승인하는 것을 포함할 수 있으며, 이는 트랜잭션의 보안을 증가시킬 수 있다. 예를 들어, 단계(508)에서, 특정 확인 데이터가 5 미국 달러의 금융 거래를 나타내는 잠재적 트랜잭션과 연관된 특정 트랜잭션 정보에 저장되지만, 상업적 개체 서브시스템(400)에 의해 단계(514)에서 특정 확인 데이터와 함께 수신된 특정 트랜잭션 정보가 2,000 미국 달러의 금융 거래를 나타내는 경우, 상업적 개체 서브시스템(400)은 \$5와 \$2,000 간의 불일치의 규모가 특정 임계치(예컨대, 5% 차 초과)보다 커서 디바이스 트랜잭션 데이터의 확인 데이터를 확인하도록 동작하지 않을 수 있다. 따라서, 단계(514)에서 수신된 확인 데이터 및 디바이스 트랜잭션 데이터의 확인 세션 식별자 및/또는 판매자 식별자가 상업적 개체 서브시스템(400)에서(예컨대, 표(430)) 활성 링크되어 있다고 승인되는 경우에도, 그 링크와 연관될 수 있는 다른 데이터가 디바이스 트랜잭션 데이터에 의해 충족되지 않는 경우 확인 데이터는 확인되지 않을 수 있다(예컨대, 확인 단계(506) 동안 식별된 보안 데이터 트랜잭션의 임의의 적합한 특성이 단계(514)의 디바이스 트랜잭션 데이터에서 식별된 것과 임의의 적합한 양만큼 상이한 경우(예컨대, 금융 거래 통화 가치의 10% 초과, 건강 데이터에 대한 타임 프레임의 10% 초과만큼 상이하고, 건강 데이터의 유형이 상이한 경우 등)).

[0055]

프로세스(500)의 단계(518)에서, 단계(516)에서 디바이스 트랜잭션 데이터의 확인 데이터를 확인하는 것에 응답하여, 상업적 개체 서브시스템(400)은 판매자 서브시스템(200)과의 공유 비밀을 이용하여 적어도 디바이스 트랜잭션 데이터의 보안 디바이스 데이터를 암호화함으로써 보안 디바이스 데이터가 판매자 서브시스템(200) 이외의 임의의 개체에 의해 수신 및 활용될 수 없도록 하여 단계(514)에서 수신된 디바이스 트랜잭션 데이터의 보안 디바이스 데이터를 추가로 안전하게 할 수 있다. 예를 들어, 확인 데이터 및 디바이스 트랜잭션 데이터의 확인

세션 식별자 및/또는 판매자 식별자가 또한 단계(516)에서 상업적 개체 서브시스템(400)(예컨대, 표(430))에 적절히 링크되었다고 승인함으로써 디바이스 트랜잭션 데이터의 확인 데이터를 확인하는 것에 응답하여, 상업적 개체 서브시스템(400)은 링크를 소진하고(예컨대, 상업적 개체 서브시스템(400)에서 확인 데이터와 확인 세션 식별자 및/또는 판매자 식별자 간의 이러한 연관성을 제거함(예컨대, 표(430)에서 링크를 제거함)) 디바이스 트랜잭션 데이터의 보안 디바이스 데이터를 추가로 안전하게 하기 위하여 단계(518)로 진행할 수 있다. 단계(514)의 디바이스 트랜잭션 데이터가 임의의 상업적 개체 키로 암호화되는 경우, 상업적 개체 서브시스템(400)은 단계(518)에서 이러한 데이터를 복호화하도록 동작할 수 있다(예컨대, 상업적 개체 서브시스템(400)의 서버(410)는 디바이스 트랜잭션 데이터를 수신하고 이어서 그 디바이스 트랜잭션 데이터를 (예컨대, 상업적 개체 서브시스템(400)의 액세스 키(155a), 액세스 키(155b), CRS(151k), CASD(158k), 및/또는 ISD 키(156k)를 이용하여) 복호화/서명해제할 수 있음). 디바이스(100)와 상업적 개체 서브시스템(400) 둘 모두에 알려진 상업적 개체 키를 이용하여 암호화/서명된 형태로 디바이스(100)와 상업적 개체 서브시스템(400) 간에 디바이스 트랜잭션 데이터를 교환함으로써, 프로세스(500)는 그 디바이스 트랜잭션 데이터의 통신이 상업적 개체 키에 액세스할 수 없는 개체에 의해 탈취 및 사용되는 것을 금지할 수 있다. 또한, 단계(518)에서, 상업적 개체 서브시스템(400)은 판매자 키(예컨대, 특정 트랜잭션이 자금을 지원받고 있는 판매자 서브시스템(200)과 연관될 수 있는 판매자 키(157))를 이용하여 디바이스 트랜잭션 데이터의 적어도 일부분을 암호화하거나 또는 다른 방식으로 리포맷(re-format)하도록 동작할 수 있다. 이러한 판매자 키는 상업적 개체 서브시스템(400)에 의해 결정될 수 있고, (예컨대, 단계(514)의 디바이스 트랜잭션 데이터의 판매자 식별자와 연관된 판매자 키를 식별함으로써) 표(430)를 통해 상업적 개체 서브시스템(400)에 액세스가능할 수 있다. 판매자 식별자는 상업적 개체 서브시스템(400)에 의해 단계(518)에서 수신 및 활용되어 상업적 개체 서브시스템(400)에 의해 액세스가능한 많은 판매자 키들 중 특정 키를 식별할 수 있고(예컨대, 상업적 개체 서브시스템(400)의 표(430)를 이용함으로써 판매자 키(157)), 이어서 상업적 개체 서브시스템(400)은 디바이스 트랜잭션 데이터의 적어도 일부분(예컨대, 적어도 디바이스 트랜잭션 데이터의 보안 디바이스 데이터)를 암호화하기 위하여 그 식별된 판매자 키를 사용할 수 있다. 이러한 보안 디바이스 데이터를 이러한 판매자 키(예컨대, 상업적 개체 서브시스템(400) 및 판매자 서브시스템(200)에 알려져 있지만 전자 디바이스(100) 또는 시스템(1)의 임의의 기타 서브시스템에 알려져 있지 않은 키)로 암호화함으로써, 이러한 보안 디바이스 데이터는 이러한 방식으로 지켜져서, 다른 개체에 의해 탈취되거나 의도하지 않은 목적에 사용되지 않고 상업적 개체 서브시스템(400)으로부터 판매자 서브시스템(200)으로 안전하게 전달될 수 있다. 상업적 개체 서브시스템(400)에 의해 단계(518)에서 적어도 디바이스 트랜잭션 데이터의 보안 디바이스 데이터를 암호화하는 데 활용된 판매자 키는 단계(506)에서 판매자 온라인 리소스의 확인 동안 상업적 개체 서브시스템(400)에 의해 챌린지 데이터를 암호화하는 데 사용되는 판매자 키(예컨대, 디바이스(100)에 의한 또는 상업적 개체 서브시스템(400) 및 판매자 서브시스템(200) 이외의 임의의 서브시스템에 의한 사용에 이용할 수 없는 키)와 동일한 키일 수 있다. 따라서, 상업적 개체 서브시스템(400)은 보안 데이터 트랜잭션에 특정된 판매자 확인 세션 동안 상업적 개체 서브시스템(400)에 의해 최근에 확인된 판매자 온라인 리소스를 이용하여 디바이스(100)와 판매자 서브시스템(200) 간의 보안 데이터 트랜잭션을 용이하게 하도록 동작할 수 있다(예컨대, 단계들(504, 506)의 확인 세션 및 단계들(516, 518)의 보안 데이터 트랜잭션은 동일한 확인 세션 식별자를 사용할 수 있는데, 이는 제한된 길이의 시간 동안 활성화 또는 다른 방식으로 인에이블될 수 있으며(예컨대, 확인 세션 식별자와 챌린지 데이터 간의 링크 및/또는 확인 세션 식별자와 확인 데이터 간의 링크는 상업적 개체 서브시스템(400)에서 제한된 길이의 시간 동안(예컨대, 임의의 적합한 길이의 시간, 예컨대 30 초 내지 10 분) 유효할 수 있음), 이는 트랜잭션의 보안을 증가시킬 수 있음).

[0056]

그 다음, 단계(520)에서, 프로세스(500)는 상업적 개체 서브시스템(400)이 단계(518)의 안전한 보안 디바이스 데이터를 디바이스(100)에 안전한 트랜잭션 데이터로서 전달하는 것을 포함할 수 있다. 예를 들어, 디바이스 트랜잭션 데이터의 이러한 판매자 키-암호화된 보안 디바이스 데이터는 단계(520)에서 안전한 트랜잭션 데이터의 적어도 일부분으로서 상업적 개체 서브시스템(400)으로부터 디바이스(100)로 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(65)를 통해 전송될 수 있다. 이러한 안전한 트랜잭션 데이터는 판매자 키-암호화된 보안 디바이스 데이터뿐만 아니라, 트랜잭션과 연관된 단계(502)의 임의의 적합한 데이터와 같은 임의의 적합한 데이터를 포함할 수 있으며, 임의의 적합한 데이터는, (i) 특정 판매자 정보, 예컨대, 단계(502)의 잠재적 트랜잭션 데이터를 제공했던 특정 판매자 서브시스템(200)을 식별할 수 있는 판매자 식별자의 식별, (ii) 특정 트랜잭션 정보, 예컨대, 금융 거래를 결제하는 데 사용될 특정 통화 또는 가치의 식별, (iii) 고유 판매자 기반 트랜잭션 식별자(예컨대, 수행되고 있는 트랜잭션과의 연관성에 대하여 판매자 서브시스템(200)에 의해 생성되는 바와 같음), (iv) 고유 디바이스-기반 트랜잭션 식별자(예컨대, 수행되고 있는 트랜잭션과의 연관성에 대하여 디바이스(100)에 의해 생성되는 바와 같음), (v) 확인 세션 식별자 등을 포함하지만, 이에 한정되지 않는다. 따라서,

단계(520)에서 상업적 개체 서브시스템(400)으로부터 디바이스(100)로 전달된 안전한 트랜잭션 데이터는 안전한 보안 디바이스 데이터뿐만 아니라 단계(502)의 일부 또는 모든 잠재적 트랜잭션 데이터를 포함할 수 있다.

[0057]

그 다음, 프로세스(500)의 단계(522)에서, 디바이스(100)는 단계(520)에서 상업적 개체 서브시스템(400)으로부터 전달된 안전한 트랜잭션 데이터를 수신할 수 있고, 그 안전한 트랜잭션 데이터를 판매자 서브시스템(200)과 임의의 적합한 방식으로 공유할 수 있다. 예를 들어, 이러한 안전한 트랜잭션 데이터는 디바이스(100)의 통신 컴포넌트(106)로부터 판매자 서브시스템(200)의 서버(210)로 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(15)를 통해 및/또는 NFC 컴포넌트(120)와 판매자 단말기(220) 간의 비접촉식 근접성 기반 통신으로서 전송될 수 있다. 단계(522)에서 디바이스(100)에 의해 판매자 서브시스템(200)에 (예컨대, 판매자 온라인 리소스(113)(예컨대, 단계(502)에서 사용되는 것과 동일한 리소스)를 이용하여) 전달될 수 있는 안전한 트랜잭션 데이터는 단계(520)의 판매자 키-암호화된 보안 디바이스 데이터뿐만 아니라, 트랜잭션과 연관된 임의의 적합한 데이터와 같은, 임의의 적합한 데이터를 포함할 수 있으며, 임의의 적합한 데이터는, (i) 특정 판매자 정보, 예컨대, 단계(502)의 잠재적 트랜잭션 데이터를 제공했던 특정 판매자 서브시스템(200)을 식별할 수 있는 판매자 식별자의 식별, (ii) 특정 트랜잭션 정보, 예컨대, 금융 거래를 결제하는 데 사용될 특정 통화 또는 가치의 식별, (iii) 고유 판매자 기반 트랜잭션 식별자(예컨대, 수행되고 있는 트랜잭션과의 연관성에 대하여 판매자 서브시스템(200)에 의해 생성되는 바와 같음), (iv) 고유 디바이스-기반 트랜잭션 식별자(예컨대, 수행되고 있는 트랜잭션과의 연관성에 대하여 디바이스(100)에 의해 생성되는 바와 같음), (v) 확인 세션 식별자 등을 포함하지만, 이에 한정되지 않는다. 따라서, 단계(522)에서 판매자 서브시스템(200)과 공유되는 안전한 트랜잭션 데이터는 적어도 단계(518)의 판매자 키-암호화된 보안 디바이스 데이터뿐만 아니라 단계(502)의 일부 또는 모든 잠재적 트랜잭션 데이터를 포함할 수 있다. 단계(522)에서 안전한 트랜잭션 데이터의 판매자 키-암호화된 보안 디바이스 데이터를 교환함으로써, 프로세스(500)는 판매자 서브시스템(200)에 대한 이러한 판매자 키-암호화된 보안 디바이스 데이터의 전달을 인에이블하여 특정 보안 데이터 트랜잭션을 용이하게 하면서, 단계(512)에서 디바이스(100)에 의해 생성되거나 또는 다른 방식으로 식별된 보안 디바이스 데이터가 판매자 키에 액세스할 수 없는 판매자(또는 프로세서) 개체(예컨대, 판매자 서브시스템(200) 이외의 판매자 서브시스템 또는 시스템(1)의 임의의 기타 서브시스템)에 의해 사용되는 것을 방지할 수 있다. 대안적으로, 도시되지 않았지만, 이러한 안전한 트랜잭션 데이터는 단계들(520, 522)에서 디바이스(100)를 통하지 않고 임의의 적합한 방식으로(예컨대, 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(85)를 통해) 상업적 개체 서브시스템(400)으로부터 판매자 서브시스템(200)으로 직접 전달될 수 있으며, 상업적 개체 서브시스템(400)은 단계(514)의 디바이스 트랜잭션 데이터의 임의의 판매자 식별자를 이용하여 타겟 판매자 서브시스템(200)을 식별할 수 있다. 안전한 트랜잭션 데이터의 판매자 키-암호화된 보안 디바이스 데이터가 판매자 서브시스템(200)에 의해 수신된 후에, 프로세스(500)는 판매자 서브시스템(200)이 임의의 적합한 목적(예컨대, 임의의 적합한 보안 디바이스 데이터 프로세싱 또는 렌더링)을 위하여 그 판매자 키-암호화된 보안 디바이스 데이터를 활용하는 것을 포함할 수 있다.

[0058]

도 5의 프로세스(500)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 추가적인 단계들이 추가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다. 프로세스(500)의 임의의 확인 단계가 실패한다면, 이러한 실패는 하나 이상의 적합한 개체에 전달될 수 있음이 이해될 것이다. 예를 들어, 판매자 온라인 리소스의 확인이 단계(506)에서 실패하고/하거나 확인 데이터의 확인이 단계(516)에서 실패한다면, 이러한 실패는 상업적 개체 서브시스템(400)에 의해 전자 디바이스(100)와 공유되어 디바이스(100)가 판매자 서브시스템(200)과의 잠재적 트랜잭션을 취소하고 잠재적으로 판매자 온라인 리소스를 디바이스(100)로부터 제거할 수 있다. 디바이스(100)의 사용자가 단계(512)에서 보안 데이터 트랜잭션에 사용할 소정 보안 데이터를 선택할 수 있는 후에, 프로세스(500)의 남은 단계들은 그 사용자에게 곧바로 일어날 수 있다(예컨대, 단계들(514 내지 522)이 디바이스(100)와 임의의 추가적인 사용자 상호작용 없이 일어날 수 있고 디바이스(100)의 사용자에게 즉시 보일 수 있음). 단계(512) 후에, 프로세스(500)는 디바이스(100)의 사용자에게, 보안 디바이스 데이터가 자동으로 즉시 판매자 서브시스템(200)에 송신되고, 트랜잭션의 상태가 디바이스(100)에 (예컨대, 판매자 서브시스템(200) 및/또는 상업적 개체 서브시스템(400)에 의해) 승인될 수 있는 것처럼 보일 수 있다. 추가적으로 또는 대안적으로, 판매자 온라인 리소스의 확인은 디바이스(100)에 곧바로 일어날 수 있다(예컨대, 단계(504)가 없는 경우에도 단계들(506 내지 510)이 디바이스(100)와 임의의 사용자 상호작용 없이 일어날 수 있고, 단계(502) 후에 디바이스(100)의 사용자에게 즉시 보일 수 있음). 대안적으로, 일부 실시예들에서, 프로세스(500)는 전체가 디바이스(100)의 사용자에게 곧바로 일어날 수 있다(예컨대, 디바이스(100)는 보안 디바이스 트랜잭션이 언제 일어나야 하는지 자동으로 결정하고, 확인 응답 데이터를 자동으로 수신하고/하거나 디바이스 트랜잭션 데이터를 자동으로 송신하고/하거나 디바이스(100)와 임의의 능동적인 사용자 상호작용 없이 보안 디바이스 트랜잭션에 대한 안전한 트랜잭션 데이터를 자동으로 수신하고/하거나 송신하도록

구성될 수 있음).

[0059] 도 6의 설명

[0060] 도 6은 금융 거래를 수행하기 위하여 보안 디바이스 기능에 대한 온라인 액세스를 확인하기 위한 도시화된 프로세스(600)의 흐름도이다. 프로세스(600)는 전자 디바이스(100), 판매자 서브시스템(200), 매수 은행 서브시스템(300), 상업적 개체 서브시스템(400), 및 금융 기관 서브시스템(350)에 의해 구현되는 것으로 도시된다. 그러나, 프로세스(600)는 임의의 다른 적합한 컴포넌트들 또는 서브시스템들을 이용하여 구현될 수 있다는 것이 이해되어야 한다. 프로세스(600)는 디바이스(100)로부터의 결제 크리덴셜을 이용하여 판매자 서브시스템(200)과 금융 거래를 안전하고 효율적으로 수행하기 위한 매끄러운 사용자 경험을 제공할 수 있다. 도 6의 프로세스(600)에 따라 금융 거래를 수행하기 위한 시스템(1)의 동작에 관한 다음의 논의를 용이하게 하기 위하여, 도 1 내지 도 4의 개략도들의 시스템(1)의 다양한 컴포넌트들, 및 이러한 트랜잭션 동안 디바이스(100)의 그래픽 사용자 인터페이스(예컨대, 판매자 온라인 리소스(113) 또는 디바이스(100)의 임의의 적합한 애플리케이션에 의해 제공될 수 있는 GUI)를 나타낼 수 있는 도 3 내지 도 3d의 스크린들(190 내지 190d)의 정면도를 참조하게 된다. 기술된 동작들은 매우 다양한 그래픽 요소 및 시각적 기법으로 달성될 수 있다. 따라서, 도 3 내지 도 3d의 실시예들은 본 명세서에서 채택된 정확한 사용자 인터페이스 규약으로 제한되도록 의도되지 않는다. 오히려, 실시예들은 매우 다양한 사용자 인터페이스 양식을 포함할 수 있다. 프로세스(600)는 적어도 부분적으로 판매자 서브시스템(200)에 의한 전자 디바이스(100)의 보안 결제 기능에 대한 액세스를 인에이블하기 위하여 판매자 서브시스템(200)을 확인하는 맥락에서 기재되지만, 많은 경우 프로세스(600)의 모든 부분이 제3자 서브시스템에 의한 디바이스(100)의 임의의 보안 기능에 대한 액세스를 인에이블하기 위하여 임의의 적합한 제3자 서브시스템을 확인하는 데 활용되는 것이 아닐 수 있음이 이해될 것이다(예컨대, 위치 데이터, 건강 데이터, 또는 임의의 기타 개인적인 데이터 또는 유효하게 확인되지 않은 제3자 서브시스템과 공유되거나 수신되어서는 안되는 다른 것들).

[0061] 프로세스(600)는 단계(602)에서 시작할 수 있으며, 액세스 데이터(652)(예컨대, 도 1a의 액세스 데이터(652))는 상업적 개체 서브시스템(400)에 의해 디바이스(100) 상에 발급될 수 있다. 예를 들어, 액세스 SSD(예컨대, SSD(154b))는 판매자 서브시스템(200)과 거래를 수행하기 위해 디바이스(100)를 더 안전하게 인에이블하기 위하여 상업적 개체 서브시스템(400)의 서버(410)로부터의 액세스 데이터(652)로서 디바이스(100)의 보안 요소(145) 상에 발급될 수 있다. 언급된 바와 같이, 액세스 SSD(154b)는 적어도 부분적으로 상업적 개체 서브시스템(400)으로부터 직접 디바이스(100)의 보안 요소(145) 상에 발급될 수 있다(예컨대, 상업적 개체 서브시스템(400)의 서버(410)와 디바이스(100)의 통신 컴포넌트(106) 간의 통신 경로(65)를 통하며, 이어서 통신 컴포넌트(106)로부터 보안 요소(145)로 (예컨대, 버스(118)를 통해) 전달될 수 있는 액세스 데이터(652)와 같음). 경로(65)를 통하는 액세스 데이터(652)는 디바이스(100)의 보안 요소(145) 상에서 액세스 SSD(154b)의 적어도 일부분 또는 전부로서 발급될 수 있고, 액세스 애플릿(153b) 및/또는 액세스 키(155b)를 포함할 수 있다. 단계(602)는 적어도 부분적으로 디바이스(100)가 초기에 (예컨대, 디바이스(100)가 사용자에게 판매되기 전에 상업적 개체 서브시스템(400)에 의해) 구성될 때 수행될 수 있다. 대안적으로 또는 추가적으로, 단계(602)는 적어도 부분적으로 디바이스(100)의 사용자가 초기에 NFC 컴포넌트(120)의 보안 요소(145)를 설정하는 것에 응답하여 수행될 수 있다. 추가적으로 또는 대안적으로, 액세스 데이터(652)는 보안 요소(145)의 ISD(152)에 대한 ISD 키(156k)를 포함할 수 있고, 상업적 개체 서브시스템(400)과 디바이스(100) 간의 보안 전송을 인에이블하기 위한 액세스 키(155b)에 추가적으로 또는 이에 대한 대안으로서 사용될 수 있다. 추가적으로 또는 대안적으로, 액세스 데이터(652)는 CRS(151)의 CRS(151k) 및/또는 디바이스(100)의 보안 요소(145)의 CASD(158)의 CASD(158k)를 포함할 수 있고, (예컨대, 임의의 적합한 상업적 개체 키 또는 상업적 개체 서브시스템(400)과 디바이스(100) 간의 공유 비밀로서 사용하기 위하여) 상업적 개체 서브시스템(400)과 디바이스(100) 간의 보안 전송을 인에이블하기 위하여 액세스 키(155b) 및/또는 액세스 키(155a) 및/또는 ISD 키(156k)에 추가적으로 또는 이에 대한 대안으로서 사용될 수 있다. 대안적으로 또는 추가적으로, 액세스 데이터(652)는 디바이스(100)의 보안 요소 상에 저장될 수 없지만 메모리(104)를 통해 프로세서(102)와 같은 디바이스(100)의 다른 부분들에 액세스가능할 수 있는, 임의의 다른 적합한 상업적 개체 키 또는 상업적 개체 서브시스템(400)과 디바이스(100) 간의 공유 비밀을 포함할 수 있다.

[0062] 프로세스(600)의 단계(604)에서, 금융(또는 발행자 또는 트랜잭션) 기관 서브시스템(350)은 크리덴셜 데이터(654)(예컨대, 도 1a의 크리덴셜 데이터(654))를 디바이스(100) 상에, 일부 실시예들에서, 상업적 개체 서브시스템(400)을 통해 발급할 수 있다. 예를 들어, 이러한 크리덴셜 데이터(654)는 적어도 부분적으로 금융 기관 서브시스템(350)으로부터 직접 디바이스(100)의 보안 요소(145) 상에 발급될 수 있다(예컨대, 금융 기관 서브시

시스템(350)과 디바이스(100) 간 도 1a의 통신 경로(75)를 통하며, 이는 통신 컴포넌트(106)를 통해 보안 요소(145)에 전달될 수 있음). 추가적으로 또는 대안적으로, 이러한 크리덴셜 데이터(654)는 적어도 부분적으로 금융 기관 서브시스템(350)으로부터 상업적 개체 서브시스템(400)을 통해 (예컨대, 금융 기관 서브시스템(350)과 상업적 개체 서브시스템(400) 간의 도 1a의 통신 경로(55)를 통하며, 이는 디바이스(100)에 크리덴셜 데이터(654)로서 상업적 개체 서브시스템(400)의 서버(410)와 디바이스(100)의 통신 컴포넌트(106) 간의 도 1a의 통신 경로(65)를 통해 전달될 수 있고, 이는 이어서 통신 컴포넌트(106)로부터 (예컨대, 버스(118)를 통해) 보안 요소(145)에 전달될 수 있음) 디바이스(100)의 보안 요소(145) 상에 발급될 수 있다. 경로(75) 및/또는 경로(65)를 통하는 크리덴셜 데이터(654)는 크리덴셜 SSD(154a)의 적어도 일부분 또는 전부로서 디바이스(100)의 보안 요소(145) 상에 발급될 수 있고, 크리덴셜 정보(161a) 및/또는 크리덴셜 키(155a') 및/또는 키(155ak)를 구비한 크리덴셜 애플릿(153a)을 포함할 수 있다. 단계(604)는 적어도 부분적으로 디바이스(100)의 사용자가 디바이스(100) 상에 발급될 특정 크리덴셜을 선택할 때 수행될 수 있다. 일부 실시예들에서, 크리덴셜 데이터(654)는 또한 액세스 키(155a)를 포함할 수 있는데, 이는 초기에 상업적 개체 서브시스템(400)으로부터 금융 기관 서브시스템(350)으로 발급될 수 있고/있거나 상업적 개체 서브시스템(400)에 의해 추가될 수 있다. 일부 실시예들에서, 이러한 크리덴셜 데이터(654)는 발급되고 있는 결제 크리덴셜의 크리덴셜 정보(예컨대, 애플릿(153a)의 크리덴셜 정보(161a))의 적어도 일부분으로서 기본 계좌 번호, AID(예컨대, SSD(154a)에 발급되고 있는 결제 크리덴셜의 데이터의 애플릿(153a)에 대한 AID(155aa)), SSD 식별자, 및/또는 SSD 카운터를 포함할 수 있다.

[0063] 디바이스(100) 상에 발급된 크리덴셜 데이터가 금융 또는 결제 크리덴셜이면, 그 크리덴셜을 이용하여 결제를 하는 데 필요한 모든 데이터, 예를 들어, 기본 계좌 번호("PAN"), 카드 보안 코드(예컨대, 카드 검증 코드("CVV")), PAN 만료일, 크리덴셜과 연관된 이름 등, 및 디바이스(100)가 적절한 암호 데이터(예컨대, 임의의 적합한 공유 비밀 및 임의의 적합한 암호화 알고리즘 또는 기능적 출력이 적어도 부분적으로 공유 비밀에 의해 결정될 수 있는 암호)를 생성하도록 동작할 수 있는 다른 데이터를 포함할 수 있다. 사용자의 "실제" 크리덴셜 또는 실제 PAN 또는 자금지원 PAN("F-PAN") 대신에 "가상" 크리덴셜 또는 가상 PAN 또는 디바이스 PAN("D-PAN")이 디바이스(100) 상에 발급될 수 있다. 예를 들어, 크리덴셜이 디바이스(100) 상에 발급될 것으로 결정되면, 실제 크리덴셜 대신에 가상 크리덴셜이 생성되고, 실제 크리덴셜에 링크되며, 디바이스(100) 상에 발급되도록, (예컨대, 금융 기관 서브시스템(350)에 의해, 상업적 개체 서브시스템(400)에 의해, 그리고/또는 디바이스(100)의 사용자에 의해) 요청될 수 있다. 가상 크리덴셜과 실제 크리덴셜의 이러한 생성 및 링크연결은, 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 가상-연결 표(312)(예컨대, 도 1a에 도시된 바와 같음)를 정의 및 저장할 수 있는데, 이는 실제 크리덴셜과 가상 크리덴셜 간의 연관성을 생성하여, 임의의 시간에 가상 크리덴셜이 (예컨대, 디바이스(100) 상에 발급된 이후) 디바이스(100)에 의해 판매자 서브시스템(200)과의 금융 거래에 활용되도록 하고, 결제 네트워크 서브시스템(360)은 그 가상 크리덴셜을 나타내는 임의의 수신된 데이터를 확인하기 위한 인가 또는 확인 요청 또는 다른 방식의 시도를 수신할 수 있고(예컨대, 단계(638)에서 데이터(688)를 수신하는 것에 응답하여 단계(640)에서) 표(312)에 의해 결정된 바와 같이 가상 크리덴셜과 연관된 실제 크리덴셜의 관점에서 그 확인 시도 요청의 분석을 수행할 수 있다. 대안적으로, 이러한 표는 적절한 발행 은행 서브시스템(370) 또는 금융 기관 서브시스템(350)에 의해 액세스가능한 임의의 다른 적합한 서브시스템에 의해 액세스 및/또는 유사하게 이용될 수 있다. 디바이스(100) 상에 실제 크리덴셜 대신에 가상 크리덴셜을 발급함으로써, 금융 기관 서브시스템(350)은 가상 크리덴셜이 비인가 사용자에 의해 탈취될 경우 일어날 수 있는 사기 행각을 제한하도록 구성될 수 있는데, 그 이유는 결제 네트워크 서브시스템(360)이 단지 소정 트랜잭션들 동안 가상 크리덴셜을 실제 크리덴셜에 연결하기 위하여 표(312)를 활용하도록 구성될 수 있기 때문이다.

[0064] 프로세스(600)의 단계(606)에서, 상업적 개체 서브시스템(400)은 판매자 서브시스템(200)을 등록할 수 있다. 예를 들어, 프로세스(500)의 단계(501)에 대하여 기재한 바와 같이, 단계(606)에서, 판매자 서브시스템(200)의 판매자 온라인 리소스(113)(예컨대, 웹사이트, 도메인/URL, 또는 임의의 다른 적합한 웹 리소스, 또는 간혹 판매자 단말기)는 적어도 하나의 특정 판매자 식별자(167) 및 적어도 하나의 특정 판매자 키(157)와 연관될 수 있는데, 이들은 각각 판매자 서브시스템(200)과 상업적 개체 서브시스템(400) 간에 임의의 적합한 방식으로 안전하게 공유될 수 있고, 이러한 연관성은 상업적 개체 서브시스템(400)에 액세스가능하게 할 수 있어서(예컨대, 표(430)) 판매자 온라인 리소스(113)는 상업적 개체 서브시스템(400)에 등록될 수 있다. 일부 실시예들에서, 온라인-리소스 결제 프로그램에 참가하기 위하여, 판매자는 상업적 개체 서브시스템(400)의 상업적 개체에 의해 실행되는 프로그램의 구성원으로서 등록하고/하거나 판매자 증명서를 획득하도록 요구받을 수 있다. 판매자는 증명서 또는 등록의 기타 적합한 증명이 없으면 결제 데이터를 수신하지 못할 수 있다. 이러한 판매자 키(들)

및/또는 판매자 식별자(들)가 어떻게 또는 어디서 생성 및/또는 관리될 수 있는지 상관없이, 판매자 서브시스템(200) 및 상업적 개체 서브시스템(400) 둘 모두는 임의의 판매자 키 쌍의 판매자 키의 버전을 (예컨대, 판매자 서브시스템(200) 및 상업적 개체 서브시스템(400)의 각각의 보안 요소에) 저장할 수 있다. 이는 상업적 개체 서브시스템(400)과 판매자 서브시스템(200) 간의 공유 비밀을 인에이블하여 그들 사이에 데이터를 안전하게 교환하도록 할 수 있다. 일부 실시예들에서, 디바이스(100)는 디바이스(100) 상의 그 키를 이용하여 결제 데이터를 안전하게 암호화하기 위한 이러한 판매자 키를 구비할 수 있다.

[0065]

프로세스(600)의 단계(608)에서, 디바이스(100)는 판매자의 온라인 리소스(658)(예컨대, 도 1a의 판매자 온라인 리소스(113)(예컨대, 단계(606)에서 등록되는 바와 같이))에 액세스할 수 있다. 도 1a에 도시된 바와 같이, 판매자의 리소스 애플리케이션(113)은 상업적 개체 서브시스템(400)으로부터(예컨대, 애플리케이션 스토어(420)로부터) 디바이스(100) 상으로 로딩될 수 있다. 예를 들어, 도 3에 도시된 바와 같이, 디바이스(100)의 사용자는 I/O 컴포넌트(114a)의 터치 스크린 입력 컴포넌트(110f)를 이용하여 GUI(180)의 특정 스크린(190)의 "판매자 앱" 아이콘(183)을 선택할 수 있고, 이 선택은 디바이스(100)에 의해 사용자에게 판매자의 제3자 애플리케이션(113)과 상호작용할 수 있는 능력을 제공하기 위한 개시 이벤트로서 인식될 수 있다(예컨대, 디바이스(100)에 의해 상업적 개체 서브시스템(400)을 통해 액세스될 수 있었던 적어도 부분적으로 디바이스(100) 상에서 실행되는 원시 애플리케이션(예컨대, 애플리케이션 스토어(420)의 등록된 판매자 온라인 리소스와 같음)). 대안적으로 또는 추가적으로, 이러한 판매자의 리소스(658)는 디바이스(100)에 의해 판매자 서브시스템(200)으로부터 직접 (예컨대, 서버(210) 또는 단말기(220)를 통해) 액세스될 수 있다. 판매자 애플리케이션 아이콘의 이러한 선택에 응답하여, GUI는 디바이스(100)가 사용자로 하여금 애플리케이션(113)과 상호작용하도록 (예컨대, 구매를 위해 판매자로부터 상업적으로 입수가능한 아이템들을 정독하거나 또는 판매자 또는 다른 것과 공유할 소정 건강 데이터 또는 위치 데이터를 결정하도록) 인에이블할 수 있는 상호작용 스크린을 제공할 수 있다. 대안적으로, 단계(608)는 디바이스(100)가 판매자 서브시스템(200)으로부터의 판매자의 웹 리소스와 같은 판매자의 리소스(658)에 (예컨대, 판매자 서버(210) 또는 적어도 부분적으로 판매자 개체에 의해 제어되는 임의의 서버를 통해) 디바이스(100)의 인터넷 애플리케이션을 이용하여 액세스하는 것을 포함할 수 있는데, 이는 또한 "인터넷" 아이콘(예컨대, 도 3의 GUI(180)의 특정 스크린(190)의 아이콘(184)), 또는 사용자에게 판매자의 제3자 원시 애플리케이션 대신에 판매자의 웹페이지 또는 기타 웹 리소스와 상호작용할 수 있는 능력을 제공하기 위한 웹화면을 구비한 하이브리드 애플리케이션에 의해 선택가능할 수 있다. 대안적으로, 단계(608)는 능동적인 사용자 입력 없이 판매자 온라인 리소스(113)와 같이 리소스(658)에 임의의 적합한 자동 액세스하는 것을 포함할 수 있다(예컨대, 디바이스(100)는 임의의 적합한 이벤트를 검출하는 것, 예컨대, 자율 가전 제품 디바이스(100)가 특정 공급이 낮은 상태로 실행되고 있음을 검출하는 것에 응답하여(예컨대, 세탁기 디바이스(100)가 세탁 세제의 낮은 공급을 검출하는 것에 응답함) 리소스(658)와 자동으로 상호작용하도록 동작할 수 있음).

[0066]

그 다음, 단계(610)에서, 디바이스(100)는 액세스된 판매자 리소스로부터 잠재적 트랜잭션 데이터(660)를 수신할 수 있다(예컨대, 프로세스(500)의 단계(502)에 대하여 기재된 바와 같음). 예를 들어, 도 1a에 도시된 바와 같이, 디바이스(100)가 판매자의 리소스(113)(예컨대, 제3자 애플리케이션 또는 웹사이트 또는 판매자의 임의의 다른 적합한 온라인 리소스(예컨대, 리소스(658)))와 상호작용할 때, 잠재적 트랜잭션 데이터(660)가 판매자 서브시스템(200)으로부터(예컨대, 판매자 서버(210)로부터) 디바이스(100)에 제공될 수 있다. 대안적으로 또는 추가적으로, 잠재적 트랜잭션 데이터(660)의 적어도 일부분은 디바이스(100)에 있는 애플리케이션(113)을 통해 (예컨대, 애플리케이션(113)이 메모리 컴포넌트에 저장되거나 또는 디바이스(100)의 프로세서(102)에 의해 실행 중일 때) 디바이스(100)에 의해 국부적으로 액세스가능할 수 있고, 데이터가 단계(610)에서 판매자 서버(210)로부터 디바이스(100)로 능동적으로 송신되는 것이 아니다. 예를 들어, 애플리케이션(113)이 초기에 디바이스(100) 상에 저장될 수 있을 때(예컨대, 판매자의 리소스(658)와 같이 단계(608)에서(예컨대, 애플리케이션 스토어(420)로부터 로딩됨)), 잠재적 트랜잭션 데이터(660)의 적어도 일부는 판매자 서브시스템(200)에 의해 디바이스(100)에 제공되는 어떠한 추가적인 정보 없이 초기에 저장된 애플리케이션(113)에 의해 생성될 수 있다. 잠재적 트랜잭션 데이터(660)는 디바이스(100)의 사용자와 판매자 서브시스템(200)의 판매자 간에 일어날 잠재적 금융 거래의 임의의 적합한 특성들을 나타내는 임의의 적합한 데이터를 포함할 수 있으며, 임의의 적합한 데이터는, (i) 특정 판매자 정보, 예컨대, 고유 판매자 식별자(예컨대, 매수 은행 판매자 식별자 및/또는 상업적 개체 판매자 식별자(예컨대, 단계(610)에서 등록될 수 있는 판매자 식별자(167))) 및/또는 사용되고 있는 특정 판매자 리소스(예컨대, 특정 판매자 애플리케이션(113))의 식별, (ii) 특정 트랜잭션 정보, 예컨대, 트랜잭션에 대한 결제에 사용될 특정 통화의 식별(예컨대, 엔, 파운드, 달러 등) 및/또는 트랜잭션에 결제될 특정 통화량의 식별 및/또는 구매 또는 대여 또는 다른 방식으로 결제될 특정 제품 또는 서비스의 식별 및/또는 사용될 기본 또는 초기 배송 주소의 식별, (iii) 트랜잭션의 판매자에게 허용가능한 하나 이상의 유형의 결제 방법을 나타내

는 정보(예컨대, 구매에 사용될 결제 카드들의 리스트(예컨대, 마스터카드 또는 가능하지만 비자는 안됨)), 및/또는 (iv) 고유 판매자 기반 트랜잭션 식별자(예컨대, 수행되고 있는 트랜잭션과의 연관성을 위해 판매자 서브시스템(200)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 자의 영숫자 스트링과 같은 임의의 적합한 데이터 요소를 포함하지만, 이에 한정되지 않는다. 이러한 잠재적 트랜잭션 데이터(660)는, 구매하는 고객의 연락처 정보 필드(예컨대, 전화 번호, 이메일 주소, 우편 주소)와 같은 금융 거래를 완료하는 데 필요하거나 또는 적어도 사용될 수 있는 연관된 데이터를 갖거나 또는 갖지 않는 임의의 적합한 개수 및 유형의 데이터 필드들을 포함할 수 있으며, 일부 필드들은 이러한 잠재적 트랜잭션 데이터(660)의 일부로서 추가되고 포함될 수 있고/있거나 일부 필드들은 이러한 잠재적 트랜잭션 데이터(660)의 일부로서 추가되지 않을 수 있지만, 개방되어 있고 프로세스(600) 동안 추가되기를 기다릴 수 있다. 단계(610)의 이러한 잠재적 트랜잭션 데이터(660)는 본 명세서에서 PK데이터요청 또는 (예컨대, 금융 거래에 대한) PK결제요청이라고 지칭될 수 있다. 대안적으로, 언급된 바와 같이, 사용자는 판매자 서브시스템(200)과 연관된 잠재적 트랜잭션 데이터(660)가 단계(610)에서 디바이스(100)에 이용가능하게 되도록 디바이스(100)와 능동적으로 상호작용하지 않을 수 있다.

[0067]

보안 결제 데이터의 통신을 위하여, 잠재적 트랜잭션 데이터(660)는 디바이스(100)가 제품 및/또는 서비스의 구매를 위한 결제 토큰을 생성하도록 하는 판매자 리소스의 요청을 포함할 수 있고, 잠재적 트랜잭션에 관한 임의의 적합한 정보, 예를 들어, 판매자의 결제 프로세싱 능력, 결제량, 및 통화 코드에 관한 정보를 포괄할 수 있다. 잠재적 트랜잭션 데이터(660)는 또한 판매자에 의해 지원될 수 있는 하나 이상의 결제 네트워크(예컨대, 결제 네트워크(들)(360))의 리스트를 포함하여, 디바이스(100)는 이러한 열거된 하나 이상의 결제 네트워크 중 어느 하나가 디바이스(100) 상에 또는 클라이언트로서 디바이스(100)에 이용가능한 임의의 적합한 호스트 디바이스 상에 인가된 결제 크리덴셜을 갖는지 결정하도록 구성될 수 있다. 일부 실시예들에서, 도 3a에 도시된 바와 같이, 이러한 잠재적 트랜잭션 데이터(660)는 디바이스(100)에 의해 액세스될 수 있고, 예를 들어, 디바이스(100)의 GUI는 스크린(190a)을 제공할 수 있으며, 판매자의 리소스는 트랜잭션 데이터(660)를 이용하여 디바이스(100)의 사용자에게 잠재적 트랜잭션과 연관된 임의의 적합한 정보, 예컨대, 정보(307a)를 이용하여 판매자의 이름(예컨대, "판매자 A"), 정보(307b)를 이용하여 제품의 이름(예컨대, "제품 B"), 정보(307c)를 이용하여 가격(예컨대, "가격 C"), 및/또는 정보(307d)를 이용한 초기 배송 데이터(예컨대, "주소 D")를 보여줄 수 있다. 판매자 서브시스템(200)에 의해 디바이스(100)에 제공될 수 있는 잠재적 트랜잭션 데이터(660)는 이러한 정보들(307a, 307b, 307c, 및/또는 307d)을 나타낼 수 있다. 디바이스(100)의 사용자는 디바이스(100) 및 스크린(190a)과 상호작용하여 이러한 정보의 소정 부분들(예컨대, 배송 주소 등)을 조정할 수 있는데, 이는 (예컨대, 단계(610)의 다른 인스턴스에서) 판매자 서브시스템(200)에 의해 업데이트된 잠재적 트랜잭션 데이터가 생성되고 공유되도록 요구할 수 있다. 또한 도 3a에 도시되고 아래 더 상세하게 기재된 바와 같이, 스크린(190a)은 또한 보안 결제 프롬프트(309)를 포함할 수 있다. 잠재적 트랜잭션 데이터(660)의 적어도 일부분은 판매자 서브시스템(200)으로부터 디바이스(100)로 도 1a의 통신 경로(15)를 통해 제공될 수 있고, 디바이스(100)의 통신 컴포넌트(106)에 의해 수신될 수 있다. 통신 컴포넌트(106)는 이 잠재적 트랜잭션 데이터(660)를 프로세서(102)(예컨대, 디바이스(100) 상의 사용자 인터페이스의 일부로서 (예컨대, 정보(307a 내지 307d 및 309)에 대하여) 스크린(190a) 상에 디스플레이하기 위하여) 및/또는 보안 요소(145)로 전달할 수 있다. 예를 들어, 보안 요소(145)는 디바이스(100)와 판매자 서브시스템(200) 간의 금융 거래를 안전하게 인에이블하기 위하여 이러한 잠재적 트랜잭션 데이터(660)의 적어도 일부분을 활용할 수 있다. 일부 실시예들에서, 잠재적 트랜잭션 데이터(660)는 판매자 결제 요청 데이터 및/또는 URL(uniform resource locator) 또는 임의의 다른 적합한 참조 문자열 및/또는 길의 문자열로서 참조될 수 있다.

[0068]

프로세스(600)의 단계(612)에서, 판매자 온라인 리소스 확인 세션이 개시될 수 있다. 프로세스(500)의 단계(504)에 대하여 언급된 바와 같이, 단계(612)는 전자 디바이스(100)가 보안 데이터 트랜잭션(예컨대, 단계(610)의 잠재적 트랜잭션 데이터(660)에 의해 식별된 보안 데이터 트랜잭션(예컨대, 금융 거래))이 일어날 것임을 나타내는 것에 응답하여 일어날 수 있다. 이 알림은, 단계(610)의 판매자 온라인 리소스의 잠재적 트랜잭션 데이터(660)에 의해 식별된 보안 데이터 트랜잭션을 수행하려는 사용자의 바람을 전달하기 위해 디바이스(100)의 사용자가 판매자 온라인 리소스의 GUI 구성요소(예컨대, 라디오 버튼), 예컨대, 도 3a의 보안 결제 프롬프트(309)를 선택하는 것에 응답하여 일어날 수 있다. 대안적으로, 이 알림은 임의의 적합한 요구조건들이 충족되는 것에 기초하여(예컨대, 단순히 단계(610)의 잠재적 트랜잭션 데이터(660)가 디바이스(100)에 전달되는 것에 응답하여) 자동으로 일어날 수 있다. 예를 들어, 이 알림이 일어나면, 판매자 온라인 리소스(113)(예컨대, 웹 리소스를 위한 웹 키트)는 보안 데이터 트랜잭션 요청을 카드 관리 애플리케이션(103b)에 송신하도록 동작할 수 있고(예컨대, 결제 보안 데이터 트랜잭션을 위한 패스 키트), 및 디바이스(100)(예컨대, 카드 관리 애플리케이션(103b) 또는 디바이스(100)의 임의의 다른 적합한 애플리케이션)는 이어서 이러한 보안 데이터 트랜잭션 요청

을 수신 및 프로세싱하도록 동작할 수 있고, 이에 응답하여, 이어서 단계(612)에서 판매자 온라인 리소스 확인 세션 개시 데이터(662)를 생성 및 판매자 서브시스템(200)에 전달하도록 동작할 수 있다.

[0069]

수행될 특정 보안 데이터 트랜잭션에 대한 판매자 온라인 리소스 확인 세션을 개시하기 위하여, 임의의 적합한 데이터가 단계(612)에서 전자 디바이스(100)에 의해 생성되고/되거나 판매자 온라인 리소스 확인 세션 개시 데이터(662)로서 판매자 서브시스템(200)에 전달될 수 있다(예컨대, 데이터(660)에 의해 식별된 금융 거래 및/또는 도 3a의 스크린(190a)). 예를 들어, 디바이스(100)에 의해 확인 세션 식별자가 생성되고 단계(612)에서 판매자 온라인 리소스 확인 세션 개시 데이터(662)의 적어도 일부분으로서 판매자 서브시스템(200)에 전달될 수 있는데, 이러한 확인 세션 식별자는 개시되고 있는 현재 판매자 온라인 리소스 확인 세션을 고유하게 식별(예컨대, 적어도 소정 기간 동안 판매자 서브시스템(200) 및/또는 상업적 개체 서브시스템(400)에 대한 이러한 세션을 고유하게 식별)할 수 있는 임의의 적합한 영숫자 스트링 또는 임의의 다른 적합한 식별자일 수 있다. 추가적으로 또는 대안적으로, 단계(612)에서 판매자 온라인 리소스 확인 세션 개시 데이터(662)의 적어도 일부분으로서 챌린지 요청 타겟 식별자(예컨대, Challenge Request URL)가 디바이스(100)에서 판매자 서브시스템(200)으로 전달될 수 있는데, 이러한 챌린지 요청 타겟 식별자는 판매자 서브시스템(200)이 판매자를 확인하기 위하여 통신할 개체를 식별할 수 있다(예컨대, URL은 수행될 특정 보안 데이터 트랜잭션에 대한 판매자 온라인 리소스를 확인하기 위하여 판매자 서브시스템(200)과 작업할 상업적 개체 서브시스템(400)의 서버(410)를 식별함). 디바이스 애플리케이션(예컨대, 카드 관리 애플리케이션(103b))은 임의의 적합한 운영 체제의 일부 또는 애플리케이션 업데이트로서 프로그래밍되는 이러한 챌린지 요청 타겟 식별자를 가질 수 있는데, 애플리케이션 업데이트는 상업적 개체 서브시스템(400)에 의해 제어될 수 있어서 챌린지 요청 타겟 식별자가 디바이스(100) 상에서 상업적 개체 서브시스템(400)에 의해 임의의 적합한 시간에 업데이트될 수 있도록 한다. 추가적으로 또는 대안적으로, 이러한 판매자 온라인 리소스 확인 세션 개시 데이터(662)는, 임의의 다른 적합한 데이터, 예컨대, 자체적으로 및/또는 단계(608)에서 액세스되고 단계(610)에서 잠재적 트랜잭션 데이터(660)를 수신하도록 활용되는 특정 판매자 온라인 리소스를 확인하도록 판매자에 대한 요청을 나타내는 임의의 적합한 데이터, 디바이스(100)를 나타내는 임의의 적합한 데이터(예컨대, 디바이스 식별자(119)), 및/또는 수행될 특정 보안 데이터 트랜잭션을 나타내는 임의의 적합한 데이터(예컨대, 단계(610)의 잠재적 트랜잭션 데이터(660)의 임의의 적합한 데이터, 예컨대, 특정 판매자 정보(예컨대, 판매자 온라인 리소스의 판매자 식별자(167)), 특정 트랜잭션 정보(예컨대, 금융 거래에 대한 통화 및 금액 및 결제 유형), 및/또는 고유 판매자 기반 트랜잭션 식별자를 포함할 수 있다. 단계(612)에서 임의의 적합한 판매자 온라인 리소스 확인 세션 개시 데이터(662)가 디바이스(100)에 의해 판매자 서브시스템(200)으로 임의의 적합한 방식으로 전달될 수 있다(예컨대, 이러한 판매자 온라인 리소스 확인 세션 개시 데이터(662)는 디바이스(100)의 통신 컴포넌트(106)로부터 판매자 서브시스템(200)의 서버(210)로 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(15)를 통해 또는 임의의 적합한 통신 프로토콜을 이용하는 단말기(220)와 NFC 컴포넌트(120) 간의 비접촉식 근접성 기반 통신 채널을 통해 전송될 수 있음).

[0070]

프로세스(600)의 단계(614)에서, 판매자 서브시스템(200)이 판매자 온라인 리소스(113)의 확인 세션을 개시하기 위해 단계(612)에서 디바이스(100)로부터 임의의 적합한 판매자 온라인 리소스 확인 세션 개시 데이터(662)를 수신하는 것에 응답하여, 판매자 서브시스템(200)은 수행될 특정 보안 데이터 트랜잭션(예컨대, 단계(610) 및/또는 단계(612)에서 식별된 바와 같은 금융 결제 트랜잭션)에 대한 판매자 온라인 리소스를 확인하기 위하여 임의의 적합한 챌린지 요청 데이터(664)를 상업적 개체 서브시스템(400)에 전달하도록 동작할 수 있다. 단계(614)에서 판매자 서브시스템(200)으로부터 상업적 개체 서브시스템(400)으로 전달되는 챌린지 요청 데이터(664)는 상업적 개체 서브시스템(400)에 대한 판매자 서브시스템(200)(예컨대, 판매자 리소스(113))의 유효성을 증명하려고 시도하기 위한 임의의 적합한 데이터를 포함할 수 있으며, 임의의 적합한 데이터는 확인될 판매자 온라인 리소스와 연관된 판매자 식별자(예컨대, 단계(606)에서 등록된 것과 같은 적어도 하나의 판매자 식별자(167), 이는 판매자 온라인 웹 리소스의 도메인일 수 있음), 확인 세션 식별자(예컨대, 단계(504)에서 디바이스(100)에 의해 또는 단계(506)에서 판매자 서브시스템(200)에 의해 생성되는 것과 같음), 및 임의의 다른 적합한 데이터(예컨대, 디바이스(100)를 식별하는 데이터 및/또는 수행될 특정 보안 데이터 트랜잭션을 식별하는 데이터)를 포함할 수 있지만, 이에 한정되지 않는다. 예를 들어, 챌린지 요청 데이터(664)의 판매자 식별자는 현재 판매자 온라인 리소스 확인 세션을 개시한 단계(610)에서 사용된 판매자 온라인 리소스와 연관된 임의의 적합한 판매자 식별자(167)일 수 있다. 단계(612)의 판매자 온라인 리소스 확인 세션 개시 데이터(662)는 확인 세션 식별자(예컨대, 디바이스(100)에 의해 생성된 바와 같음)를 포함하고, 그 확인 세션 식별자는 단계(614)에서 판매자 서브시스템에 의해 챌린지 요청 데이터(664)의 적어도 일부분으로서 제공될 수 있다. 그러나, 단계(612)의 판매자 온라인 리소스 확인 세션 개시 데이터(662)가 확인 세션 식별자를 포함하지 않거나 또는 임의의 단계(612)의 임의의 판매자 온라인 리소스 확인 세션 개시 데이터(662)에 응답하지 않고 판매자 온라인 리소스 확인

세션이 판매자 서브시스템(200)에 의해 (예컨대, 단계(610)의 잠재적 트랜잭션 데이터(660)를 전달하는 것에 응답하여) 자동으로 개시되는 경우, 판매자 서브시스템(200)은 개시되고 있는 현재 판매자 온라인 리소스 확인 세션을 고유하게 식별할 수 있는 이러한 확인 세션 식별자를 생성하도록 동작할 수 있고, 단계(614)에서 확인 세션 식별자를 챌린지 요청 데이터(664)의 적어도 일부분으로서 포함하도록 동작할 수 있다. 일부 실시예들에서, 수행될 보안 데이터 트랜잭션(예컨대, 단계(610) 및/또는 단계(612)에서 식별된 것으로서 금융 결제 트랜잭션)에 특정한 것에 구체적일 수 있는 임의의 적합한 추가적인 정보가 단계(614)에서 챌린지 요청 데이터(664)의 적어도 일부분으로서 제공될 수 있는데, 임의의 적합한 추가적인 정보는 잠재적 트랜잭션 데이터의 정보(307b)의 "제품 B"를 나타내는 정보, 잠재적 트랜잭션 데이터의 정보(307c)의 "가격 C", 잠재적 트랜잭션 데이터의 정보(307d)의 배송 데이터 "주소 D", 잠재적 트랜잭션 데이터의 결제 크리덴셜 식별 "크리덴셜 X" 정보(313), 및/또는 상업적 개체 서브시스템(400)과 적절하게 공유될 수 있는, 수행될 보안 데이터 트랜잭션과 연관된 임의의 다른 적합한 정보 (예컨대, 데이터 중 임의의 것에 관한 임의의 프라이버시 문제의 관점에서), 수행될 보안 데이터 트랜잭션이 건강 데이터 트랜잭션인 경우 실제 심박수 정보가 아닌 "지난 3 일간의 심박수 정보"를 포함하지만, 이에 한정되지 않는다. 보안 데이터 트랜잭션에 특정한 것에 구체적일 수 있는 이러한 정보는, 본 명세서에서 잠재적 트랜잭션 식별 정보로서 지칭될 수 있는데, 보안의 임의의 추가적인 계층(들)을 현재 데이터 트랜잭션 프로세스에 제공하고/하거나 향후 데이터 트랜잭션들을 위한 임의의 추가적인 보안(예컨대, 사기 검출) 서비스를 제공하기 위하여 프로세스(600)의 임의의 적합한 부분들에서 사용될 수 있다. 챌린지 요청 데이터(664)는 판매자 서브시스템(200)에 의해 (예컨대, HTTP 헤더에서 또는 다른 방식으로) 판매자 서브시스템(200)에 이용가능하고 챌린지 요청의 판매자 식별자와 연관된 판매자 키(예컨대, 단계(606)에서 판매자 식별자(167)로 (예컨대, 확인될 판매자 온라인 리소스(113)에 대하여) 등록되는 것과 같은 판매자 키(157))로 서명되어 챌린지 요청 데이터(664)가 판매자 온라인 리소스(113)를 확인하기 위하여 상업적 개체 서브시스템(400)에 의해 효과적으로 활용될 수 있다. 임의의 적합한 챌린지 요청 데이터(664)는 단계(614)에서 판매자 서브시스템(200)에 의해 상업적 개체 서브시스템(400)으로 임의의 적합한 방식으로 전달될 수 있다(예컨대, 이러한 챌린지 요청 데이터(664)는 판매자 서브시스템(200)의 서버(210)로부터 상업적 개체 서브시스템(400)의 서버(410)로 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(85)를 통해 전송될 수 있음). 챌린지 요청 데이터(664)의 이러한 통신은 단계(612)에서 판매자 온라인 리소스 확인 세션 개시 데이터(662)의 적어도 일부분으로서 디바이스(100)로부터 판매자 서브시스템(200)으로 전달될 수 있는 챌린지 요청 타겟 식별자(예컨대, 챌린지 요청 URL)에 기초하여 상업적 개체 서브시스템(400)으로 적절히 주소지정될 수 있다. 대안적으로 또는 추가적으로, 챌린지 요청 데이터(664)의 이러한 통신은 챌린지 요청 타겟 식별자(예컨대, 챌린지 요청 URL)에 기초하여 상업적 개체 서브시스템(400)에 적절히 주소지정될 수 있는데, 챌린지 요청 타겟 식별자는 판매자 서브시스템(200)에 이용가능하고 단계(610)의 잠재적 트랜잭션 데이터(660)와 연관될 수 있다(예컨대, 상업적 개체 서브시스템(400)을 식별하는 식별자는 임의의 코드(예컨대, 웹 리소스에 대한 자바 스크립트 코드)와 연관될 수 있거나 또는 다른 방식으로 임의의 적합한 "보안 트랜잭션" 프롬프트를 판매자 온라인 리소스에 제공하기 위해(예컨대, 도 3a의 보안 결제 프롬프트(309)) 판매자 서브시스템(200)에 이용가능할 수 있음).

[0071] 프로세스(600)의 단계(616)에서, 상업적 개체 서브시스템(400)이 단계(614)에서 판매자 서브시스템(200)으로부터 임의의 적합한 챌린지 요청 데이터(664)를 수신하는 것에 응답하여, 상업적 개체 서브시스템(400)은 챌린지 요청의 판매자 식별자(167)에 의해 식별되는 판매자 온라인 리소스(113)를 확인하도록 동작할 수 있다. 예를 들어, 단계(616)에서, 상업적 개체 서브시스템(400)은 수신된 챌린지 요청 데이터(664)의 판매자 식별자(167)에 의해 식별된 판매자 온라인 리소스(113)가 상업적 개체 서브시스템(400)에서 유효한 등록된 판매자 온라인 리소스임을 승인하도록 시도하도록 동작할 수 있고, 이는 표(430)의 그 판매자 식별자(167)를 식별하고(예컨대, 판매자 식별자(167)가 상업적 개체 서브시스템(400)에 (예컨대, 단계(606)에서) 등록되었고 이러한 등록이 여전히 유효함을 결정함(예컨대, 그 상업적 개체 서브시스템(400)이 표(430)에서 판매자 식별자(167)를 제거하지 않았거나 또는 의심스럽거나 또는 다른 방식으로 더 이상 신뢰하지 않아서 플래그 표시된 판매자 식별자(167)를 표(430)에서 제거하지 않았거나 및/또는 (예컨대, 표(430) 내의) 판매자 식별자(167)와 연관된 증명서가 여전히 유효함) 및/또는 판매자 식별자(167)와 연관되거나 또는 그에 의해 식별된 도메인을 식별하고, (예컨대, 단계(501) 및/또는 단계(606)에 대하여 기재된 바와 같이) 그 도메인 상에 호스팅될 수 있는 파일을 재검증함으로써 그 도메인을 재검증하여 확인될 수 있는데, 이러한 재검증은 대안적으로 또는 추가적으로 상업적 개체 서브시스템(400)에 의해 임의의 적합한 시간에(예컨대, 주기적으로 또는 다른 방식으로) 수행될 수 있고, 데이터(664)를 수신하는 것에 응답하여 단계(616)에서 반드시 수행되는 것은 아니다. 추가적으로 또는 대안적으로, 단계(616)에서, 상업적 개체 서브시스템(400)은 수신된 챌린지 요청 데이터(664)의 서명을 확인하려고 시도하도록 동작할 수 있는데, 이는 표(430) 내의 수신된 챌린지 요청 데이터(664)의 판매자 식별자(167)와 연관되거나 또는 다

른 방식으로 상업적 개체 서브시스템(400)에서 연관될 수 있는 (예컨대, 단계(606)의 등록 동안 만들어졌을 수 있는 연관성) 판매자 키(157)를 식별하고, 이어서 그 식별된 판매자 키(157)를 활용하여 수신된 챌린지 요청 데이터(664)의 서명을 확인함으로써 (예컨대, 상업적 개체 서브시스템(400)에 액세스가능한 판매자 키(157)가 단계(614)에서 챌린지 요청 데이터(664)를 상업적 개체 서브시스템(400)에 전달하기 전에 판매자 서브시스템(200)에 의해 챌린지 요청 데이터(664)를 서명하는 데 사용되었을 수 있는 판매자 서브시스템(200)에 액세스가능한 판매자 키(157)를 포함하는 페어링된 키 세트 중 하나임을(예컨대, 키들 중 하나는 공개키이고 다른 하나는 페어링된 키 세트의 개인키일 수 있음) 승인함) 수행될 수 있는데, 이는 판매자 서브시스템(200)에 의해 프로세스(600)의 뒷 부분(들)에서의 사용(예컨대, 단계(636)에서, 판매자 서브시스템(200)은 상업적 개체 서브시스템(400)에 의해 이전에 암호화된 데이터를 복호화할 수 있음)에 필요할 수 있는 판매자 키(157)의 판매자 서브시스템(200)에 의한 소유를 보장할 수 있다. 상업적 개체 서브시스템(400)에 의한 수신된 챌린지 요청 데이터(664)의 임의의 적합한 확인 후(예컨대, 판매자 식별자 및/또는 수신된 챌린지 요청 데이터(664)의 서명의 확인 후), 상업적 개체 서브시스템(400)은 또한, 단계(616)에서, 임의의 적합한 챌린지 데이터를 생성하고 그 챌린지 데이터를 수신된 챌린지 요청 데이터(664)의 임의의 적합한 식별자 데이터에 대해 저장하도록 동작할 수 있다. 예를 들어, 수신된 챌린지 요청 데이터(664)의 임의의 적합한 확인 후, 상업적 개체 서브시스템(400)은 임의의 적합한 챌린지 데이터(예컨대, 엔트로피를 통한 임의의 적합한 무작위 데이터)를 생성하고 이어서 그 챌린지 데이터를 챌린지 요청 데이터(664)의 확인 세션 식별자 및 챌린지 요청 데이터(664)의 판매자 식별자 중 하나 또는 둘 모두에 대해 상업적 개체 서브시스템(400)에 액세스가능한 임의의 적합한 데이터 구조로 (예컨대, 표(430)에 또는 다른 방식으로) 저장하도록 동작할 수 있다. 이러한 챌린지 데이터와 확인 세션의 식별자 데이터(예컨대, 확인 세션 식별자 및/또는 챌린지 요청 데이터(664)의 판매자 식별자) 간의 이러한 저장된 링크 또는 연관성은 나중에 상업적 개체 서브시스템(400)에 의해 사용되어 추가로 (예컨대, 단계(622)에서) 확인 세션의 판매자 온라인 리소스를 확인하고/하거나 추가적으로 (예컨대, 단계(630)에서) 수행될 보안 데이터 트랜잭션을 보호할 수 있다. 또한, 일부 실시예들에서, 챌린지 요청 데이터(664)의 임의의 또는 모든 잠재적 트랜잭션 식별 정보는 또한 챌린지 데이터 및 식별자 데이터에 대하여 저장되거나 또는 다른 방식으로 그것들과 연관될 수 있다.

[0072] 프로세스(600)의 단계(618)에서, 상업적 개체 서브시스템(400)이 단계(616)에서 수신된 챌린지 요청 데이터(664)를 확인하고 확인 세션의 식별자 데이터에 대하여 챌린지 데이터를 생성하는 것에 응답하여, 상업적 개체 서브시스템(400)은 임의의 적합한 키를 이용하여 또는 다른 방식으로 단계(616)의 챌린지 데이터를 암호화하도록 동작할 수 있고, 이어서 그 암호화된 챌린지 데이터를 챌린지 데이터(668)로서 임의의 다른 적합한 데이터와 함께 판매자 서브시스템(200)에 전달하도록 동작할 수 있다. 예를 들어, 상업적 개체 서브시스템(400)은 상업적 개체 서브시스템(400)에 액세스가능하고 수신된 챌린지 요청 데이터(664)의 판매자 식별자(167)와 연관될 수 있는(예컨대, 표(430)에서 또는 다른 방식으로 상업적 개체 서브시스템(400)에서(예컨대, 단계(606)의 등록 동안 만들어졌을 수 있는 연관성)) 임의의 적합한 판매자 키(157)를 이용하여 챌린지 데이터를 암호화할 수 있고, 상업적 개체 서브시스템(400)에 의해 단계(618)에서 챌린지 데이터의 암호화를 위해 사용되는 이러한 판매자 키(157)는 단계(616)에서 상업적 개체 서브시스템(400)에 의해 챌린지 요청 데이터(664)를 확인하는 데 사용되었을 수 있는 판매자 키(157)와 동일한 판매자 키(157)이거나 또는 상이한 판매자 키(157)일 수 있다. 이러한 암호화된 챌린지 데이터뿐만 아니라, 단계(618)에서 상업적 개체 서브시스템(400)에 의해 판매자 서브시스템(200)으로 전달된 챌린지 데이터(668)의 일부분으로서 임의의 다른 적합한 데이터가 포함될 수 있으며, 임의의 다른 적합한 데이터는, 상업적 개체 서브시스템(400)에 의해 챌린지 데이터를 암호화하는 데 사용되는 판매자 키(157)의 해시(예컨대, 판매자 서브시스템(200)에 의해 수신되고 적절한 판매자 키(157)(예컨대, 챌린지 데이터를 복호화하기 위한 판매자 서브시스템(200)의 개인키(157))를 식별하는 데 사용될 수 있는 표(430)의 공개 판매자 키(157)의 해시 버전, 이는 다수의 등록된 판매자 온라인 리소스들 및/또는 다수의 판매자 키들을 가질 수 있는 판매자를 지원하도록 제공될 수 있음), 챌린지 요청 데이터(664)의 확인 세션 식별자, 챌린지 요청 데이터(664)의 판매자 식별자, 상업적 개체 서브시스템(400)에서(예컨대, 표(430)에서) 상업적 개체 서브시스템(400)에 의해 챌린지 데이터의 암호화에 사용되는 판매자 키(157)와 연관되는 판매자 식별자 등을 포함하지만, 이에 한정되지 않는다. 임의의 적합한 챌린지 데이터(668)는 상업적 개체 서브시스템(400)에 의해 판매자 서브시스템(200)으로 단계(618)에서 임의의 적합한 방식으로 전달될 수 있다(예컨대, 이러한 챌린지 데이터(668)는 상업적 개체 서브시스템(400)의 서버(410)로부터 판매자 서브시스템(200)의 서버(210)로 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(85)를 통해 전송될 수 있음).

[0073] 프로세스(600)의 단계(620)에서, 판매자 서브시스템(200)이 단계(618)에서 이러한 챌린지 데이터(668)를 수신하는 것에 응답하여, 판매자 서브시스템(200)은 수신된 챌린지 데이터(668)를 프로세싱하고, 이어서 현재 확인 세

션 동안 판매자 서브시스템(200)을 추가로 확인하기 위하여 챌린지 응답 데이터(670)를 생성하고 상업적 개체 서브시스템(400)에 전달하도록 동작할 수 있다. 예를 들어, 단계(620)에서, 판매자 서브시스템(200)은 판매자 서브시스템(200)에 이용가능한 임의의 적합한 판매자 키(157)를 이용하여 수신된 챌린지 데이터(668)의 암호화된 챌린지 데이터를 복호화하도록 동작할 수 있다(예컨대, (예컨대, 현재 확인 세션 동안 확인되는 판매자 온라인 리소스(113)에 대하여) 단계(606)에서 판매자 식별자(167)로 등록되는 것과 같은 판매자 키(157)). 단계(620)에서 판매자 서브시스템(200)에 의해 암호화된 챌린지 데이터의 복호화에 사용되는 이러한 판매자 키(157)는 판매자 서브시스템(200)에 의해 챌린지 데이터(668)의 임의의 해시 키 정보를 이용하여 및/또는 챌린지 데이터(668)의 임의의 판매자 식별자를 이용하여 및/또는 임의의 챌린지 요청 데이터(664)의 판매자 식별자를 이용하여(예컨대, 데이터(664) 및 데이터(668)의 공통 세션 식별자와 연관될 수 있음) 식별될 수 있다. 단계(620)에서 판매자 서브시스템(200)에 의해 암호화된 챌린지 데이터의 복호화에 사용되는 이러한 판매자 키(157)는 단계(614)에서 판매자 서브시스템(200)에 의해 챌린지 요청 데이터(664)에 서명하는 데 사용되었을 수 있는 판매자 키(157)와 동일한 판매자 키(157)이거나 또는 상이한 판매자 키(157)일 수 있다. 수신된 챌린지 데이터(668)의 암호화된 챌린지 데이터를 복호화한 후, 판매자 서브시스템(200)은 또한 단계(620)에서 챌린지 응답 데이터(670)를 생성하고 판매자 서브시스템(200)으로부터 상업적 개체 서브시스템(400)으로 전달하도록 동작할 수 있는데, 챌린지 응답 데이터(670)는 상업적 개체 서브시스템(400)에 대한 판매자 서브시스템(200)(예컨대, 판매자 리소스(113))의 유효성을 증명하도록 추가로 시도하기 위하여 판매자 서브시스템(200)에 의해 복호화되는 챌린지 데이터를 임의의 다른 적합한 데이터와 함께 포함할 수 있으며, 임의의 다른 적합한 데이터는, 현재 확인 세션의 확인 세션 식별자(예컨대, 챌린지 요청 데이터(664)의 유효 세션 식별자 및/또는 수신된 챌린지 데이터(668)의 유효 세션 식별자), 현재 확인 세션에 의해 확인되는 판매자 온라인 리소스와 연관된 판매자 식별자(예컨대, 챌린지 요청 데이터(664)의 판매자 식별자로서, 판매자 식별자는 상업적 개체 서브시스템(400)에서 (예컨대, 표(430)에서) 챌린지 데이터 등의 암호화를 위하여 상업적 개체 서브시스템(400)에 의해 사용된 판매자 키(157)와 연관됨), 단계(614)의 챌린지 요청 데이터(664)에 포함되었거나 또는 포함되지 않았을 수 있는, 수행될 보안 데이터 트랜잭션에 대한 임의의 또는 모든 적합한 잠재적 트랜잭션 식별 정보 등을 포함하지만, 이에 한정되지 않는다. 챌린지 응답 데이터(670)는 판매자 서브시스템(200)에 의해 (예컨대, HTTP 헤더에서 또는 다른 방식으로) 판매자 서브시스템(200)에 이용가능한 판매자 키(예컨대, 단계(606)에서 (예컨대, 현재 확인되고 있는 판매자 온라인 리소스(113)에 대하여) 판매자 식별자(167)로 등록된 판매자 키(157))를 이용하여 서명되어 챌린지 응답 데이터(670)는 추가로 판매자 온라인 리소스(113)를 확인하기 위하여 상업적 개체 서브시스템(400)에 의해 효과적으로 활용될 수 있다. 단계(620)에서 챌린지 응답 데이터(670)에 서명하기 위하여 판매자 서브시스템(200)에 의해 사용될 수 있는 이러한 판매자 키(157)는 단계(614)에서 판매자 서브시스템(200)에 의해 챌린지 요청 데이터(664)에 서명하는 데 사용되었을 수 있는 판매자 키(157)와 동일한 판매자 키(157)이거나 또는 상이한 판매자 키(157)일 수 있다. 추가적으로 또는 대안적으로, 단계(620)에서 챌린지 응답 데이터(670)에 서명하기 위하여 판매자 서브시스템(200)에 의해 사용될 수 있는 이러한 판매자 키(157)는 단계(620)에서 판매자 서브시스템(200)에 의해 암호화된 챌린지 데이터를 복호화하는 데 사용되었을 수 있는 판매자 키(157)와 동일한 판매자 키(157)이거나 또는 상이한 판매자 키(157)일 수 있다. 임의의 적합한 챌린지 응답 데이터(670)는 단계(620)에서 판매자 서브시스템(200)에 의해 상업적 개체 서브시스템(400)으로 임의의 적합한 방식으로 전달될 수 있다(예컨대, 이러한 챌린지 응답 데이터(670)는 판매자 서브시스템(200)의 서버(210)로부터 상업적 개체 서브시스템(400)의 서버(410)로 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(85)를 통해 전송될 수 있음).

[0074]

프로세스(600)의 단계(622)에서, 상업적 개체 서브시스템(400)이 단계(620)에서 임의의 적합한 챌린지 응답 데이터(670)를 판매자 서브시스템(200)으로부터 수신하는 것에 응답하여, 상업적 개체 서브시스템(400)은 현재 확인 세션에서 관심있는 추가적으로 판매자 서브시스템(200) 및 그것의 판매자 온라인 리소스를 확인하도록 동작할 수 있다. 예를 들어, 단계(622)에서, 상업적 개체 서브시스템(400)은 수신된 챌린지 응답 데이터(670)의 서명을 확인하도록 시도하도록 동작할 수 있는데, 이는 표(430)의 수신된 챌린지 응답 데이터(670)의 확인 세션 식별자와 연관될 수 있거나 또는 표(430)의 수신된 챌린지 응답 데이터(670)의 판매자 식별자(167)와 연관될 수 있거나 또는 다른 방식으로 상업적 개체 서브시스템(400)에서 연관될 수 있는 (예컨대, 단계(606)의 등록 동안 만들어졌을 수 있는 연관성) 판매자 키(157)를 식별하고, 이어서 그 식별된 판매자 키(157)를 활용하여 수신된 챌린지 응답 데이터(670)의 서명을 확인함으로써(예컨대, 상업적 개체 서브시스템(400)에 액세스가능한 판매자 키(157)가 단계(620)에서 챌린지 응답 데이터(670)를 상업적 개체 서브시스템(400)에 전달하기 전에 판매자 서브시스템(200)에 의해 챌린지 응답 데이터(670)에 서명하는 데 사용되었을 수 있는, 판매자 서브시스템(200)에 액세스가능한 판매자 키(157)를 포함하는 페어링된 키 세트 중 하나임을 승인함(예컨대, 키들 중 하나는 공개키

일 수 있고 다른 하나는 페어링된 키 세트의 개인키일 수 있음)) 수행될 수 있다. 단계(622)에서 챌린지 응답 데이터(670)의 서명을 확인하기 위해 상업적 개체 서브시스템(400)에 의해 사용될 수 있는 이러한 판매자 키(157)는 단계(616)에서 챌린지 요청 데이터(664)의 서명을 확인하기 위하여 상업적 개체 서브시스템(400)에 의해 사용되었을 수 있는 판매자 키(157)와 동일한 판매자 키(157)이거나, 또는 상이한 판매자 키(157)일 수 있고/있거나 단계(622)에서 챌린지 응답 데이터(670)의 서명을 확인하기 위하여 상업적 개체 서브시스템(400)에 의해 사용되었을 수 있는 이러한 판매자 키(157)는 단계(618)에서 챌린지 데이터를 암호화하기 위하여 상업적 개체 서브시스템(400)에 의해 사용되었을 수 있는 판매자 키(157)와 동일한 판매자 키(157)이거나, 또는 상이한 판매자 키(157)일 수 있다. 추가적으로 또는 대안적으로, 단계(622)에서, 상업적 개체 서브시스템(400)은 수신된 챌린지 응답 데이터(670)의 복호화된 챌린지 데이터가 유효한 챌린지 데이터임을 승인하도록 시도하도록 동작할 수 있다. 예를 들어, 상업적 개체 서브시스템(400)은 수신된 챌린지 응답 데이터(670)의 복호화된 챌린지 데이터가 상업적 개체 서브시스템(400)에 (예컨대, 표(430)에) 현재 저장되어 있거나 또는 다른 방식으로 독립적으로 액세스가능함을 승인하도록 시도하도록 동작할 수 있다. 일부 실시예들에서, 상업적 개체 서브시스템(400)은 표(430)에 현재 저장되어 있는 동일한 챌린지 데이터를 식별함으로써 수신된 챌린지 응답 데이터(670)의 복호화된 챌린지 데이터의 유효성을 결정할 수 있다. 대안적으로, 상업적 개체 서브시스템(400)은 수신된 챌린지 응답 데이터(670)의 임의의 적합한 식별자 데이터에 대하여(예컨대, 확인 세션 식별자 또는 판매자 식별자에 대하여) 단계(616)에서 표(430)에 저장되었을 수 있는, 표(430)에 현재 저장된 것과 동일한 챌린지 데이터를 식별함으로써 수신된 챌린지 응답 데이터(670)의 복호화된 챌린지 데이터의 유효성을 결정할 수 있다. 일부 실시예들에서, 챌린지 데이터와 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두 간의 이러한 저장된 링크, 또는 이러한 저장된 챌린지 데이터 자체는 링크 또는 저장된 데이터가 자동으로 소거되기 전에 제한된 길이의 시간 동안만 상업적 개체 서브시스템(400)에 의해 유지될 수 있어서, 판매자 서브시스템(200)은 특정 확인 세션에 대한 판매자 온라인 리소스를 확인하기 위하여 챌린지 데이터(668)를 수신하고 이어서 적절한 챌린지 응답 데이터(670)를 상업적 개체 서브시스템(400)에 송신해야 하는 소정 지속 시간에 제한될 수 있다 (예컨대, 상업적 개체 서브시스템(400)은 소정 기간 후에 상업적 개체 서브시스템(400)에서 챌린지 데이터와 확인 세션 식별자 및/또는 판매자 식별자 간의 이러한 연관성을 제거하도록(예컨대, 링크 또는 챌린지 데이터가 생성된 후 10 분 이내에 표(430)에서 링크 또는 챌린지 데이터를 제거함) 동작할 수 있고, 이는 트랜잭션의 보안을 증가시킬 수 있음). 따라서, (예컨대, 단계(610) 및/또는 단계(612)에서 식별된 바와 같이) 수행될 특정 보안 데이터 트랜잭션에 대한 판매자 온라인 리소스의 확인이 임의의 또는 모든 단계들(614 내지 622)에서 상업적 개체 서브시스템(400)에서 (예컨대, 단계(608)에서 등록된 바와 같이) 판매자 키와 판매자 식별자 간의 하나 이상의 연관성을 이용하여 완료될 수 있다.

[0075] 상업적 개체 서브시스템(400)에 의한 수신된 챌린지 응답 데이터(670)의 임의의 적합한 확인 후(예컨대, 수신된 챌린지 응답 데이터(670)의 서명의 확인 후 및/또는 수신된 챌린지 응답 데이터(670)의 복호화된 챌린지 데이터의 확인 후), 상업적 개체 서브시스템(400)은 또한, 단계(622)에서, 임의의 적합한 확인 데이터르 생성하고, 그 확인 데이터를 수신된 챌린지 요청 데이터(664)의 임의의 적합한 식별자 데이터 및/또는 수신된 챌린지 응답 데이터(670)의 임의의 적합한 식별자 데이터에 대하여 저장하도록 동작할 수 있다. 예를 들어, 수신된 챌린지 요청 데이터(664)의 임의의 적합한 확인 후 및/또는 수신된 챌린지 응답 데이터(670)의 임의의 적합한 확인 후, 상업적 개체 서브시스템(400)은 임의의 적합한 확인 데이터(예컨대, 엔트로피 및/또는 임의의 적합한 암호화 난수를 통한 임의의 적합한 무작위 데이터)를 생성하고 이어서 그 확인 데이터를 챌린지 요청 데이터(664)와 챌린지 응답 데이터(670) 중 임의의 하나 또는 둘 모두의 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두에 대하여 상업적 개체 서브시스템(400)에 액세스 가능한 임의의 적합한 데이터 구조로 (예컨대, 표(430)에 또는 다른 방식으로) 저장하도록 동작할 수 있다. 이러한 저장된 링크 또는 이러한 확인 데이터와 확인 세션의 식별자 데이터 간의 연관성(예컨대, 확인 세션 식별자 및/또는 챌린지 요청 데이터(664)의 판매자 식별자 및/또는 챌린지 응답 데이터(670)의 판매자 식별자)은 나중에 상업적 개체 서브시스템(400)에 의해 사용되어 추가로 (예컨대, 단계(630)에서) 수행될 보안 데이터 트랜잭션을 보호할 수 있다. 또한, 일부 실시예들에서, 챌린지 요청 데이터(664) 및/또는 챌린지 응답 데이터(670)의 임의의 또는 모든 잠재적 트랜잭션 식별 정보는 또한 확인 데이터 및 식별자 데이터에 대하여 저장되거나 또는 다른 방식으로 그것들과 연관될 수 있다.

[0076] 챌린지 데이터가 상업적 개체 서브시스템(400)의 (예컨대, 표(430) 내의) 식별자 정보(예컨대, 확인 세션 식별자 및/또는 판매자 식별자 정보)와 링크되어 있음을 승인함으로써 수신된 챌린지 응답 데이터(670)의 복호화된 챌린지 데이터를 확인하는 것에 응답하여, 상업적 개체 서브시스템(400)은, 단계(622)에서, 그 링크를 소진하고 (예컨대, 상업적 개체 서브시스템(400)에서 챌린지 데이터와 확인 세션 식별자 및/또는 판매자 식별자 간의 이러한 연관성을 제거함(예컨대, 표(430)로부터 링크를 제거함)), 확인 데이터(예컨대, 임의의 적합한 무작위 데

이터(예컨대, 암호화 난스(예컨대, 엔트로피를 통한 임의의 적합한 무작위 데이터)))를 생성하고, 이어서 확인 데이터를 임의의 적합한 식별자 정보(예컨대, 챌린지 요청 및/또는 챌린지 응답의 확인 세션 식별자 및/또는 챌린지 요청 및/또는 챌린지 응답의 판매자 식별자)에 대하여 또는 그것들과 다른 방식으로 연관지어 상업적 개체 서브시스템(400)에서 (예컨대, 표(430)와 같은 임의의 적합한 데이터 구조로 또는 다른 방식으로) 저장하도록 동작할 수 있다. 대안적으로, 챌린지 데이터가 상업적 개체 서브시스템(400)의(예컨대, 표(430) 내의) 식별자 정보(예컨대, 확인 세션 식별자 및/또는 판매자 식별자 정보)와 링크되어 있음을 승인함으로써 수신된 챌린지 응답 데이터(670)의 복호화된 챌린지 데이터를 확인하는 것에 응답하여, 상업적 개체 서브시스템(400)은, 단계(622)에서, 그 링크를 유지하거나 또는 다른 방식으로 그 링크를 업데이트하고(예컨대, 상업적 개체 서브시스템(400)에서 (예컨대, 표(430) 내의) 그 링크와 연관될 수 있는 임의의 타이머를 리셋하거나 또는 링크와의 연관성에 대한 임의의 추가적인 잠재적 트랜잭션 식별 정보를 추가함)), 이어서 그 링크의 챌린지 데이터(예컨대, 단계(616)에서 생성됨)를 단계(622)에서 다른 방식으로 생성될 수 있는 확인 데이터와 같이 활용하도록 동작할 수 있다. 일부 실시예들에서, 챌린지 데이터 및 확인 데이터는, 단계들(618 내지 622)에서의 챌린지 데이터의 사용이 단계들(624 내지 630)에서의 확인 데이터의 사용과 상이할 수 있음에 따라 크기 또는 임의의 다른 적합한 특성 또는 특성들에 대하여 상이할 수 있다.

[0077]

프로세스(600)의 단계(624)에서, 상업적 개체 서브시스템(400)이 단계(622)에서 수신된 챌린지 요청 데이터(664)를 확인하고/하거나 수신된 챌린지 응답 데이터(670)를 확인하고, 확인 세션의 식별자 데이터에 대하여 확인 데이터를 생성 또는 다른 방식으로 정의하는 것에 응답하여, 상업적 개체 서브시스템(400)은 임의의 적합한 확인 응답 데이터(674)를 생성하고 전달하도록 동작할 수 있다. 예를 들어, 확인 응답 데이터(674)는 단계(622)의 확인 데이터를 임의의 다른 적합한 데이터와 함께 포함할 수 있는데, 임의의 다른 적합한 데이터는 확인 세션 식별자(예컨대, 챌린지 요청 데이터(664) 및/또는 챌린지 응답 데이터(670)의 확인 세션 식별자 및/또는 다른 방식으로 확인 세션과 연관될 수 있는 확인 세션 식별자), 판매자 식별자(예컨대, 챌린지 요청 데이터(664) 및/또는 챌린지 응답 데이터(670)의 판매자 식별자 및/또는 상업적 개체 서브시스템(400)에서(예컨대, 표(430) 내의) 확인 세션 동안 확인된 판매자 온라인 리소스와 다른 방식으로 연관될 수 있는 판매자 식별자) 등을 포함하지만, 이에 한정되지 않는다. 일부 실시예들에서, 도 6에 도시된 바와 같이, 이러한 확인 응답 데이터(674)는 상업적 개체 서브시스템(400)으로부터 직접 전자 디바이스(100)로(예컨대, 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(65)를 통해) 전달될 수 있는데, 전자 디바이스(100)를 식별하는 데이터(예컨대, 디바이스 식별자(119))는 확인 세션 개시 데이터(662) 및/또는 챌린지 요청 데이터(664) 및/또는 챌린지 응답 데이터(670) 또는 다른 것과 연관되거나 또는 다른 방식으로 포함되어 상업적 개체 서브시스템(400)이 확인 응답 데이터(674)를 적절한 전자 디바이스(100)에 전달할 수 있도록 할 수 있다. 대안적으로, 일부 실시예들에서, 확인 응답 데이터(674)는 상업적 개체 서브시스템(400)으로부터 전자 디바이스(100)로 판매자 서브시스템(200)을 통해 전달될 수 있는데, 이로써 판매자 서브시스템(200)은 상업적 개체 서브시스템(400)으로부터 (예컨대, 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(85)를 통해) 확인 응답 데이터(674)를 수신하고, 이어서 확인 응답 데이터(674)의 적어도 일부분을 전자 디바이스(100) 상으로 (예컨대, 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(15)를 통하거나 또는 비접촉식 근접성 기반 통신으로서) 전달하여, 상업적 개체 서브시스템(400)이 단계(624)에서 디바이스(100)와 직접 보안 통신 채널을 구축할 필요가 없을 수 있다. 확인 응답 데이터(674)는 상업적 개체 서브시스템(400)에 의해(예컨대, HTTP 헤더에서 또는 다른 방식으로) 또한 전자 디바이스(100)에 액세스가능할 수 있는 상업적 개체 서브시스템(400)과 연관된 액세스 키(예컨대, 보안 요소(145)의 액세스 키(155a), 액세스 키(155b), CRS(151k), 및/또는 ISD 키(156k) 또는 디바이스 애플리케이션(예컨대, 카드 관리 애플리케이션(103b))에 알려질 수 있는 임의의 키)를 이용하여 서명될 수 있어서, 디바이스(100)는 서명된 확인 데이터를 수신하게 되면 서명을 확인하여 전자 디바이스(100)에 의해 신뢰받지 않는 다른 개체 서브시스템이 아닌, 상업적 개체 서브시스템(400)이 확인 응답 데이터(674)를 생성했음을 승인할 수 있고/있거나 서명된 확인 데이터는 이러한 액세스 키에 액세스할 수 없는 개체(예컨대, 서명된 확인 데이터를 상업적 개체 서브시스템(400)으로부터 디바이스(100)로 전달하는 데 사용될 수 있는 판매자 서브시스템(200))에 의해 활용될 수 없다.

[0078]

언급한 바와 같이, 단계(610)의 판매자 온라인 리소스의 잠재적 트랜잭션 데이터(660)에 의해 식별된 보안 데이터 트랜잭션을 수행하려는 사용자의 바람을 전달하기 위해 디바이스(100)의 사용자는 판매자 온라인 리소스의 GUI 구성요소(예컨대, 라디오 버튼), 예컨대, 도 3a의 보안 결제 프롬프트(309)를 선택할 수 있다. 도 3b에 도시된 바와 같이, 디바이스(100) 및/또는 판매자 온라인 리소스(113)는 도 3a의 스크린(190a)의 보안 결제 프롬프트(309)의 선택을 수신하는 것에 단독으로 또는 또한 디바이스(100)가 단계(624)에서 확인 세션 실패가 아님을 나타낼 수 있는 확인 응답 데이터(674)를 수신하는 것을 추가적으로 응답하여 스크린(190b)을 제공하도록 구

성되고/되거나, 디바이스(100)가 디바이스(100)에 의해 단계(612)에서 확인 세션 개시 데이터(662)의 일부분으로서 생성되었을 수 있는 세션 식별자와 수신된 확인 응답 데이터(674)의 일부분으로서 제공될 수 있는 세션 식별자 간의 일관성(예컨대, 단계(625)에서)을 검증하는 것에 응답하여 스크린(190b)을 제공하도록 구성될 수 있는데, 이는 응답 데이터(674)가 확인 세션 개시 데이터(662)와 프로세스(600)의 동일한 확인 세션의 일부로서 연관됨을 승인하도록 디바이스(100)를 인에이블할 수 있다(예컨대, 디바이스(100)는 확인 세션 개시 데이터(662)의 세션 식별자를 판매자 서브시스템(200)의 판매자 식별자와 조합하여 저장할 수 있고(예컨대, 단계(612)) 이어서 그 저장된 데이터 조합을 확인 응답 데이터(674)의 세션 식별자 및 판매자 식별자와 비교하여(예컨대, 단계(625)) 프로세스(600)의 남은 과정을 허용하기 전에 적절한 매칭을 보장할 수 있고, 디바이스(100)는 단계(612)에서 디바이스(100)에 의해 생성된 임의의 세션 식별자가 단계(612)에서 개시되는 세션 동안 특정 판매자 서브시스템 또는 확인될 판매자 온라인 리소스에 고유함을 보장하도록 동작할 수 있음). 임의의 이벤트에서, 도 3b에 도시된 바와 같이, 스크린(190b)은 사용자에게 디바이스(100)와 상호작용하여 하나 이상의 방법으로 특정 결제 소스 또는 구매를 하기 위하여 디바이스(100)에 이용가능할 수 있는 크리덴셜을 선택하도록 촉구할 수 있다. 예를 들어, 도시된 바와 같이, 스크린(190b)은 디바이스(100)에 이용가능할 수 있는 잠재적인 다수의 결제 소스들 중 하나를 선택하도록 사용자를 인에이블할 수 있는 결제 소스 선택 프롬프트(311)를 포함할 수 있다. 결제 소스 선택 프롬프트(311)는 판매자에 의해 지원되는 결제 네트워크들과 연관된 크리덴셜들을 이용하는 결제 소스들만을 포함할 수 있거나(예컨대, 잠재적 트랜잭션 데이터(660)에 의해 결정될 수 있고, 이는 위에서 언급된 바와 같음) 또는 디바이스(100)에 이용가능한 모든 결제 소스들은 단지 허용가능한 결제 네트워크들과 연관된 것들만이 사용자에게 의해 선택될 수 있음을 보여줄 수 있다. 결제 소스 선택 프롬프트(311)는 임의의 적합한 결제 소스들(예컨대, 프롬프트(311)의 결제 옵션 식별자(311a)에 의해 표시될 수 있는 "크리덴셜 X"를 이용한 결제 방법, 프롬프트(311)의 결제 옵션 식별자(311b)에 의해 표시될 수 있는 "크리덴셜 Y"를 이용하는 결제 방법 등)을 포함할 수 있는데, 임의의 적합한 결제 소스들은, 디바이스(100)의 보안 요소에 원래 있던 임의의 적합한 결제 크리덴셜들 및/또는 디바이스(100)(예컨대, 클라이언트 디바이스와 같이 디바이스(100)에 대한 호스트 디바이스의 역할을 할 수 있는 다른 디바이스)에 액세스가능한 임의의 이용가능한 결제 소스들의 임의의 적합한 비-원시 결제 크리덴셜들을 포함하지만, 이에 한정되지 않는다. 단지 일 특정 예로서, 도 3c에 도시된 바와 같이, 디바이스(100)는 도 3b의 결제 소스 선택 프롬프트(311)의 식별자(311a)의 "크리덴셜 X"의 사용자 선택을 수신하는 것에 응답하여 스크린(190c)을 제공하도록 구성될 수 있다. 도 3c의 스크린(190c)은 선택되거나 또는 크리덴셜 식별자 정보(313)를 이용하여 자동으로 식별된 기본 크리덴셜을 식별할 수 있고, 디바이스(100)의 사용자에게 디바이스(100)와 상호작용하여 하나 이상의 방법으로 사용자 및 그것의 의도를 인증하고 선택된 크리덴셜을 활용하도록 촉구할 수 있다. 이것은, 디바이스(100)의 보안 요소에 액세스하여, 크리덴셜이 구매에 사용되도록 하기 위하여 사용자에게 (예컨대, 도 3c의 인증 프롬프트(315)를 이용하여) 개인 식별 번호("PIN") 입력 또는 생체인식 센서와의 사용자 상호작용을 통해 사용자 인증을 입력하도록 촉구하는 것을 포함할 수 있다. 판매자 온라인 리소스 확인 세션은 (예컨대, 단계(612) 및/또는 단계(614)에서) 임의의 적합한 이벤트에 기초하여, 예컨대, 잠재적 트랜잭션 데이터(660)가 전달되는 것에 응답하여 및/또는 스크린(190a)이 제시되는 것에 응답하여 및/또는 도 3a의 스크린(190a)의 보안 결제 프롬프트(309)의 사용자 선택에 응답하여 및/또는 도 3b의 결제 소스 선택 프롬프트(311)의 특정 크리덴셜의 사용자 선택에 응답하여 및/또는 도 3c의 스크린(190c)의 제시에 응답하여 개시될 수 있다. 도 3b의 결제 소스 선택 프롬프트(311)는 임의의 적합한 순간에, 예컨대, 단계들(612 내지 624)에서 (예컨대, 단계들(612 내지 614) 전에 또는 그 동안 또는 그것들 중 임의의 단계에서) 일어날 수 있는 임의의 확인 세션의 상태에 상관없이 도 3a의 스크린(190a)의 보안 결제 프롬프트(309)의 사용자 선택에 응답하여 및/또는 도 3a의 스크린(190a)의 보안 결제 프롬프트(309)의 사용자 선택뿐만 아니라 단계(624)에서 확인 응답 데이터(674)의 수신에 응답하여 제시될 수 있으며, 이는 확인 세션 실패 없음을 나타낼 수 있다. 도 3c의 인증 프롬프트(315)는 임의의 적합한 순간에, 예컨대, 단계들(612 내지 624)에서 (예컨대, 단계들(612 내지 614) 전에 또는 그 동안 또는 그것들 중 임의의 단계에서) 일어날 수 있는 임의의 확인 세션의 상태에 상관없이 결제 소스 선택 프롬프트(311)의 결제 식별자의 사용자 선택을 수신하는 것에 응답하여 및/또는 결제 소스 선택 프롬프트(311)의 결제 식별자의 사용자 선택을 수신하는 것 뿐만 아니라 단계(624)에서 확인 응답 데이터(674)의 수신에 응답하여 제시될 수 있으며, 이는 확인 세션 실패 없음을 나타낼 수 있고/있거나 스크린(190c)은 단계(624)에서 확인 응답 데이터(674)의 수신 전에 제시될 수 있지만, 도 3c의 인증 프롬프트(315)는 단계(624)에서 확인 응답 데이터(674)의 수신 후까지 사용을 위해 인에이블되지 않을 수 있다.

[0079] 디바이스(100)의 사용자가 단계(610)에서 수신된 잠재적 트랜잭션 데이터(660)(예컨대, 결제 요청 데이터)에 응답하여 잠재적 트랜잭션에 자금을 공급하는 데 사용하기 위한 특정 결제 크리덴셜을 선택 또는 승인을 하려고

하고 또한 할 수 있으며, 확인 응답 데이터(674)(예컨대, 단계들(612 내지 622)의 판매자 온라인 리소스 확인 세션의 성공을 나타낼 수 있는 데이터)가 단계(624)에서 전자 디바이스(100)에 의해 수신된 경우, 프로세스(600)는 단계(625)로 진행할 수 있는데, 여기서 프로세스(600)는, (예컨대, 단계(625)에서, 위에 언급된) 임의의 세션 식별자 일관성이 식별된 후에, 디바이스(100)의 사용자에게 의해 잠재적 트랜잭션 데이터(660)에 기초하여 (예컨대, 도 3c의 인증 프롬프트(315)의 사용자 선택을 통해) 특정 판매자, 제품, 가격, 및 배송 목적지에 대한 잠재적 트랜잭션을 수행하기 위하여 특정 크리덴셜을 활용하는 의도 및 인증을 수신하는 것을 포함할 수 있다. 액세스 SSD(154b)는 디바이스(100)의 애플릿(153b)을 이용하여 이러한 인증이 다른 SSD들(154)(예컨대, 크리덴셜 SSD(154a))이 상거래 크리덴셜 데이터 통신에 그것의 크리덴셜 정보를 인에이블하는 데 사용되도록 하기 전에 일어났는지 결정할 수 있다. 단계(625)의 단지 하나의 예로서, 액세스 SSD(154b)의 애플릿(153b)은 (예컨대, 사용자에게 의해 디바이스(100)의 임의의 애플리케이션(예컨대, 디바이스(100)의 판매자 리소스(113) 및/또는 카드 관리 애플리케이션(103b))과 상호작용에 사용될 수 있는, 도 3의 생체인식 입력 컴포넌트(110i)와 같은 하나 이상의 입력 컴포넌트(110)를 통해 디바이스(100)의 사용자의 의도 및 로컬 인증을 결정하도록 구성될 수 있고, 이러한 결정에 응답하여, (예컨대, 크리덴셜 SSD(154a)의 크리덴셜을 이용하여) 결제 트랜잭션을 수행하기 위하여 다른 특정 SSD를 인에이블하도록 구성될 수 있다. 일부 실시예들에서, 이러한 결정 이후, 그러나 이러한 인에이블먼트 전에, 디바이스(100)의 GUI는 (예컨대, 도 3c의 프롬프트(315)와 유사한 프롬프트를 이용하여) 디바이스(100)의 사용자에게 디바이스(100)와 상호작용하여 하나 이상의 방법으로 최종적으로 선택되고 인가된 크리덴셜을 이용하여 결제를 개시하도록 촉구할 수 있는 다른 스크린(미도시)을 제공하도록 구성될 수 있다. 디바이스(100)의 사용자는 단계(610)의 잠재적 트랜잭션 데이터(660)(예컨대, 스크린들(190a 내지 190c)의 "판매자 A" 및 "제품 B" 및 "가격 C" 및 "배송 D")에 의해 식별된 잠재적 트랜잭션에 자금을 공급하기 위하여 디바이스(100)에 원래 있던 특정 결제 크리덴셜의 사용을 위해 단계(625)에서 의도 및 인증을 제공할 수 있다. 그러나, 대안적으로, 프로세스(600)는 임의의 의도 및 인증이 단계(625)에서 제공될 수 있기 전에 잠재적 트랜잭션의 하나 이상의 특성을 조정하도록 디바이스(100)의 사용자를 인에이블할 수 있다(예컨대, 배송 주소 정보가 스크린(190a 및/또는 190b) 상에서 업데이트되거나 또는 판매자 서브시스템(200)과 디바이스(100) 간에 교환되는 추가적인 업데이트된 잠재적 트랜잭션 데이터(660)에 걸쳐 다른 것들도 업데이트됨).

[0080]

그 다음, 잠재적 트랜잭션 데이터(660)의 특정 결제 요청 데이터를 수신하는 것에 응답하여 특정 결제 크리덴셜에 대한 의도 및 인증이 단계(625)에서 수신되면, 프로세스(600)의 단계들(626 내지 628)은 디바이스(100)가 상업적 개체 서브시스템(400)에 의한 사용을 위해 디바이스 트랜잭션 데이터(678)를 생성, 암호화, 및 전송하는 것을 포함할 수 있다(예컨대, 프로세스(500)의 단계들(512, 514)에 대하여 기재된 바와 같음). 디바이스(100)의 보안 요소(145) 상의 크리덴셜 SSD(154a)의 크리덴셜이 (예컨대, 단계(625)에서) 선택, 인증, 및/금융 거래에서의 사용이 인에이블되면, 디바이스(100)의 보안 요소(145)(예컨대, NFC 컴포넌트(120)의 프로세서 모듈(142))는 상업적 개체 서브시스템(400)에 의한 사용을 위하여 그 선택된 크리덴셜의 소정 크리덴셜 데이터를 생성 및 암호화할 수 있다. 예를 들어, 크리덴셜 SSD(154a)의 디바이스 결제 크리덴셜 데이터(675)(예컨대, SSD(154a)의 결제 카드 데이터(예컨대, 선택된 "크리덴셜 X"와 연관될 수 있음)), 예컨대, 토큰 데이터 및 암호 데이터가 생성되고/되거나 단계(626)에서 적어도 토큰 데이터 및 암호 데이터를 포함하는 디바이스 결제 크리덴셜 데이터(676)로서 크리덴셜 키(155a')를 이용하여 적어도 부분적으로 암호화될 수 있어서, 이러한 암호화된 디바이스 결제 크리덴셜 데이터(676)는 디바이스 결제 크리덴셜 데이터(675)에 액세스하기 위하여 그 크리덴셜 키(155a')에 대한 액세스를 갖는 개체(예컨대, 금융 기관 서브시스템(350))에 의해서만 복호화될 수 있다. 이러한 결제 크리덴셜 데이터(675)는 디바이스(100)의 특정 보안 요소 크리덴셜(예컨대, SSD(154a)의 크리덴셜)의 적절한 소유권을 안전하게 증명하도록 동작할 수 있는 임의의 적합한 데이터를 포함할 수 있으며, 임의의 적합한 데이터는 (i) 토큰 데이터(예컨대, SSD(154a)의 크리덴셜 정보(161a)의 DPAN, DPAN 만료일, 및/또는 CVV) 및 (ii) 암호 데이터(예컨대, 보안 요소(145)에 의해 SSD(154a)와 금융 기관 서브시스템(350)의 공유 비밀(예컨대, 키(155a'))을 이용하여 생성될 수 있는 암호 및 임의의 다른 적합한 정보(예컨대, 일부 또는 모든 토큰 데이터, 디바이스(100)를 식별하는 정보, 단계(610)의 일부 또는 모든 잠재적 트랜잭션 데이터(660), 예컨대 비용 및/또는 통화를 식별하는 정보, 임의의 적합한 카운터 값, 난스(예컨대, 확인 응답 데이터(674)의 확인 데이터의 난스) 등), 임의의 다른 적합한 정보는 디바이스(100)에 이용가능할 수 있고 또한 공유 비밀을 이용하여 암호 데이터를 독립적으로 생성하기 위하여 금융 기관 서브시스템(350)에 이용가능하게 될 수 있음)를 포함하지만, 이에 한정되지 않는다. 따라서, 결제 크리덴셜 데이터(675)는 크리덴셜을 이용하여 결제를 하는데 필요한 모든 데이터, 예를 들어, 기본 계좌 번호(예컨대, 실제 F-PAN 또는 가상 D-PAN), 카드 보안 코드(예컨대, 카드 검증 코드("CVV")), 만료일, 크리덴셜과 연관된 이름, 연관된 암호 데이터(예컨대, 보안 요소(145)와 금융 기관 서브시스템(350) 간의 공유 비밀 및 임의의 다른 적합한 정보를 이용하여 생성된 암호) 등을 포함

할 수 있다. 일부 실시예들에서, 크리덴셜 SSD(154a)의 일부 또는 모든 결제 크리덴셜 데이터(675)가 단계(626)에서 크리덴셜 키(155a')를 이용하여 암호화된 결제 크리덴셜 데이터(676)로서 암호화되면, 그 암호화된 결제 크리덴셜 데이터(676)는, 단독으로 또는 해당 잠재적 트랜잭션 데이터(660)의 모든 부분이 아닌 경우 적어도 제1 부분(예컨대, 판매자의 식별, 가격 금액의 식별, 통화 및/또는 배송 및/또는 제품의 식별, 및/또는 고유 판매자 기반 트랜잭션 식별자 및/또는 고유 사용자 디바이스-기반 트랜잭션 식별자 및/또는 기타 등등을 포함할 수 있는 일부 또는 모든 잠재적 트랜잭션 데이터(660)), 일부 또는 모든 확인 응답 데이터(674), 및/또는 임의의 다른 적합한 정보(예컨대, 임의의 디바이스(100)를 식별하는 정보 자체(예컨대, 디바이스 식별자(119)), 임의의 특정 디바이스-기반 트랜잭션 식별자 등)과 함께, 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 및/또는 CASD(158k)에 의해 서명되어) 단계(627)에서 보안 디바이스 데이터(677)로서 암호화될 수 있다. 예를 들어, 디바이스(100)의 보안 요소(145)(예컨대, NFC 컴포넌트(120)의 프로세서 모듈(142))는 액세스 정보를 이용하여 데이터(660) 및/또는 데이터(674)로부터의 판매자의 식별(예컨대, 판매자의 식별 또는 구매에 사용되는 그것의 리소스, 예컨대, 애플리케이션(113))뿐만 아니라, 또한 구매량의 식별 및/또는 데이터(660)로부터의 통화 코드, 및 SSD(154a)의 암호화된 결제 크리덴셜 데이터(675)(예컨대, 암호화된 결제 크리덴셜 데이터(676))를 보안 디바이스 데이터(677)로 암호화할 수 있다. 일부 실시예들에서, 크리덴셜 SSD(154a)의 결제 크리덴셜 데이터(675)(예컨대, SSD(154a)의 결제 카드 데이터, 예를 들어, 토큰 데이터 및 암호 데이터)는 (예컨대, 단계(626)에서 데이터(676)로서) 크리덴셜 키를 이용하여 생성되지만, (예컨대, 단계(627)에서 데이터(677)로서) 상업적 개체 키 또는 액세스 키를 이용하여 암호화되기 전에 암호화되지 않으며, 대신에, 이러한 결제 크리덴셜 데이터(675)는 (예컨대, 단계(627)에서 데이터(677)로서) 상업적 개체 키 또는 액세스 키를 이용하여 암호화될 수 있고, 이로써 이러한 실시예들에서, 데이터(676)에 대한 임의의 향후 참조는 또한 임의의 크리덴셜 키로 암호화되지 않은 데이터(675)를 참조할 수 있다. 일부 실시예들에서, 이러한 상업적 개체 키 또는 액세스 키는 상업적 개체 서버시스템(400)의 체계와 연관된 상업적 개체 공개키일 수 있고, 이를 이용하여 상업적 개체 서버시스템(400)은 연관된 상업적 개체 개인키에 액세스할 수 있다. 상업적 개체 서버시스템(400)은 이러한 상업적 개체 공개키를 금융 기관 서버시스템(350)에 제공할 수 있고, 이어서 금융 기관 서버시스템(350)은 그 상업적 개체 공개키를 디바이스(100)와 공유할 수 있다(예컨대, 크리덴셜 데이터를 디바이스(100)에 발급할 때(예컨대, 프로세스(600)의 단계(654)에서)).

[0081]

그 다음, 보안 디바이스 데이터(677)는 임의의 추가적인 정보, 예컨대 적어도 일부의 잠재적 트랜잭션 데이터(660) 또는 잠재적 트랜잭션 식별 정보(예컨대, 판매자의 식별, 가격 금액의 식별, 통화의 식별, 고유 판매자 기반 트랜잭션 식별자, 제품/서비스의 식별 등) 및/또는 확인 응답 데이터(674)의 적어도 일부분 또는 전부 및/또는 임의의 다른 적합한 정보(예컨대, 임의의 디바이스(100)를 식별하는 정보 자체, 고유 디바이스-기반 트랜잭션 식별자 등)와 함께 단계(628)에서 디바이스 트랜잭션 데이터(678)로서 디바이스(100)에서 상업적 개체 서버시스템(400)으로 함께 전송될 수 있다(예컨대, 프로세스(500)의 단계(514)에 대하여 기재된 바와 같음). 따라서, 디바이스 트랜잭션 데이터(678)의 적어도 일부분들(예컨대, 확인 응답 데이터(674)가 있거나 또는 없는 보안 디바이스 데이터(677))은 오직 암호화에 사용된 그 액세스 정보에 대한 액세스를 갖는, 디바이스 트랜잭션 데이터(678)의 보안 디바이스 데이터(677)(예컨대, 상업적 개체 서버시스템(400))를 생성했던 개체에 의해서 복호화될 수 있다(예컨대, 액세스 키(155a), 액세스 키(155b), ISD 키(156k), CRS(151k), 및/또는 CASD(158k)). 이러한 디바이스 트랜잭션 데이터(678)는 단계들(626 내지 628)에서 생성될 수 있고 이어서 단계(628)에서 상업적 개체 서버시스템(400)으로 (예컨대, 보안 요소(145)로부터 또는 다른 방식으로, 통신 컴포넌트(106) 및 통신 경로(65)를 통해) 전송될 수 있다. 단계들(626, 627, 628)은 디바이스(100)의 보안 요소(145)로부터 생성되고 디바이스 트랜잭션 데이터(678)의 일부로서 전송되는 임의의 크리덴셜 데이터가 먼저 디바이스(100)의 다른 부분에 의해(예컨대, 프로세서(102)에 의해) 복호화될 수 없는 방법으로 암호화되었음을 보장할 수 있다. 즉, 디바이스 트랜잭션 데이터(678)의 결제 크리덴셜 데이터(675)는 그것의 보안 요소 외부에 있는 디바이스(100)의 어떠한 부분에 노출되거나 또는 액세스불가능할 수 있는 크리덴셜 키(155a')를 이용하여 암호화된 디바이스 결제 크리덴셜 데이터(676)처럼 암호화될 수 있다. 또한, 트랜잭션 데이터(678)의 이러한 디바이스 결제 크리덴셜 데이터(676)는 그것의 보안 요소 외부에 있는 디바이스(100)의 어떠한 부분에 노출되거나 또는 액세스 불가능한 액세스 키(예컨대, 액세스 키(155a, 155b, 156k, 151k, 및/또는 158k)(예컨대, 본 명세서에서 "액세스 정보"로서 지칭됨))를 이용하여 보안 디바이스 데이터(677)처럼 암호화될 수 있다.

[0082]

그 다음, 단계(629)에서, 프로세스(600)는 상업적 개체 서버시스템(400)이 디바이스 트랜잭션 데이터(678)의 적어도 일부분을 수신하고 복호화하는 것을 포함할 수 있다. 예를 들어, 상업적 개체 서버시스템(400)은 디바이스 트랜잭션 데이터(678)를 수신할 수 있고 이어서 상업적 개체 서버시스템(400)에 이용가능한 액세스 정보(예

컨대, 155a, 155b, 156k, 151k, 및/또는 158k)를 이용하여 디바이스 트랜잭션 데이터(678)의 보안 디바이스 데이터(677)를 복호화할 수 있다. 이는 상업적 개체 서브시스템(400)이 또한 (예컨대, 암호화된 디바이스 결제 크리덴셜 데이터(676)로서) 결제 크리덴셜 데이터(675)를 암호화된 상태에서 유지하면서 (예컨대, 복호화된 보안 디바이스 데이터(677)로부터) 판매자의 암호화되지 않은 식별을 결정하도록 인에이블할 수 있는데, 그 이유는 상업적 개체 서브시스템(400)은 크리덴셜 키(155a')에 액세스할 수 없기 때문인데, 그 크리덴셜 키(155a')를 이용하여 이러한 디바이스 결제 크리덴셜 데이터(675)가 디바이스(100)의 보안 요소(145)에 의해 단계(626)에서 암호화된 디바이스 결제 크리덴셜 데이터(676)처럼 암호화되었을 수 있다. 추가적으로 또는 대안적으로, 판매자는 보안 디바이스 데이터(677)와 함께 디바이스 트랜잭션 데이터(678)에 포함되었을 수 있는 추가적인 데이터에 의해 식별될 수 있다. 디바이스 트랜잭션 데이터(678)는 디바이스(100) 또는 적어도 그것의 보안 요소를 식별하는 정보를 포함할 수 있어서, 디바이스 트랜잭션 데이터(678)가 상업적 개체 서브시스템(400)에 의해 수신되면, 상업적 개체 서브시스템(400)은 어떤 액세스 정보(예컨대, 액세스 정보(155a, 155b, 156k, 151k, 및/또는 158k) 중 어떤 것)가 단계(629)에서 사용될 지 알 수 있다. 예를 들어, 상업적 개체 서브시스템(400)은 다수의 액세스 키들(155a/155b) 및/또는 다수의 ISD 키들(156k)에 액세스할 수 있고, 이들의 각각은 특정 디바이스(100) 또는 특정 보안 요소에 특정할 수 있다.

[0083]

또한, 단계(629) 전후로, 단계(628)에서 전달된 디바이스 트랜잭션 데이터(678)를 수신한 후에, 프로세스(600)의 단계(629)는 상업적 개체 서브시스템(400)이 디바이스(100)가 디바이스 트랜잭션 데이터(678)에 포함했을 수 있는 확인 응답 데이터(674)의 확인 데이터를 확인하는 것을 포함할 수 있다. 예를 들어, 이러한 디바이스 트랜잭션 데이터(678)를 수신하는 것에 응답하여, 상업적 개체 서브시스템(400)은 확인 응답 데이터(674)의 적어도 일부분 또는 전부를 그 디바이스 트랜잭션 데이터(678)로부터 식별하고, 단계(630)에서 (예컨대, 프로세스(500)의 단계(516)에 유사하게) 그 수신된 디바이스 트랜잭션 데이터(678)의 확인 데이터가 현재 상업적 개체 서브시스템(400)에 저장되어 있음을 승인하거나, 또는, 더 구체적으로, 일부 실시예들에서, 그 수신된 디바이스 트랜잭션 데이터(678)의 확인 데이터가 현재 상업적 개체 서브시스템(400)에서 수신된 디바이스 트랜잭션 데이터(678)의 확인 세션 식별자 및/또는 수신된 디바이스 트랜잭션 데이터(678)의 판매자 식별자에 대하여 (예컨대, 표(430) 내에) 저장되어 있음을 승인하도록 동작할 수 있다. 일부 실시예들에서, 확인 데이터와 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두 간의 이러한 저장된 링크는 링크가 자동으로 소거되기 전에 제한된 길이의 시간 동안만 유지될 수 있어서, 전자 디바이스(100)는, 그것이 단계(624)에서 확인 응답 데이터(674)를 수신한 뒤, 확인된 판매자 온라인 리소스를 이용하여 특정 보안 데이터 트랜잭션을 수행하기 위하여 상업적 개체 서브시스템(400)에 의해 보호되는 디바이스 트랜잭션 데이터(678)의 보안 디바이스 데이터(677)를 인에이블하기 위하여 단계(628)에서 상업적 개체 서브시스템(400)에 디바이스 트랜잭션 데이터(678)를 송신해야 하는 소정 지속 시간에 제한될 수 있다(예컨대, 상업적 개체 서브시스템(400)은 소정 기간 후에 확인 데이터와 상업적 개체 서브시스템(400)의 확인 세션 식별자 및/또는 판매자 식별자 간의 이러한 연관성을 제거하도록(예컨대, 링크가 생성되고 10 분 이내에 표(430)로부터의 링크를 제거) 동작할 수 있음), 이는 트랜잭션의 보안을 증가시킬 수 있음). 추가적으로 또는 대안적으로, 확인 데이터와 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두 간의 저장된 링크는 또한 단계(622)에서 판매자 서브시스템(200)에 의해 단계들(614, 620) 중 하나 이상 동안 (예컨대, 챌린지 요청 데이터(664) 및/또는 챌린지 응답 데이터(670)의 일부분처럼) 상업적 개체 서브시스템(400)에 이용가능하게 될 수 있는 임의의 적합한 특정 잠재적 트랜잭션 식별 정보와 연관될 수 있고 (예컨대, 디바이스(100)와 판매자 서브시스템(200) 간에 공유될 특정 유형의 보안 데이터(예컨대, 금융 거래에 대한 통화 및 금액 및 결제 유형)의 식별), 유사한 특정 잠재적 트랜잭션 식별 정보는 또한 전자 디바이스(100)에 의해 단계(628)의 디바이스 트랜잭션 데이터(678)의 일부분처럼 상업적 개체 서브시스템(400)에 이용가능하게 될 수 있어서, 단계(630)는 또한 상업적 개체 서브시스템(400)이 (예컨대, 단계(616) 및/또는 단계(622)에서 표(430)에 저장된 것처럼) 단계(614) 및/또는 단계(620)에서 수신된 확인 데이터에 대하여 현재 저장된 특정 잠재적 트랜잭션 식별 정보가 단계(628)에서 수신된 특정 잠재적 트랜잭션 식별 정보와 적어도 유사하다고 승인하는 것을 포함할 수 있다. 예를 들어, 단계(622)에서, 특정 확인 데이터가 5 미국 달러의 금융 거래를 나타내는 잠재적 트랜잭션과 연관된 특정 잠재적 트랜잭션 식별 정보에 대하여 저장되지만, 상업적 개체 서브시스템(400)에 의해 단계(628)에서 특정 확인 데이터와 함께 수신된 특정 잠재적 트랜잭션 식별 정보가 2,000 미국 달러의 금융 거래를 나타내는 경우, 상업적 개체 서브시스템(400)은 \$5와 \$2,000 간의 불일치의 규모로 인해 디바이스 트랜잭션 데이터(678)의 확인 데이터를 확인하도록 동작하지 않을 수 있다. 따라서, 단계(628)에서 수신된 확인 데이터 및 디바이스 트랜잭션 데이터(678)의 확인 세션 식별자 및/또는 판매자 식별자가 상업적 개체 서브시스템(400)에(예컨대, 표(430) 내에) 능동적으로 링크되어 있음이 승인될 수 있는 경우에도, 확인 데이터는, 그 링크와 연관될 수 있는 다른 데이터가 디바이스 트랜잭션 데이터(678)에 의해 충족되지 않는 경우(예컨

대, 단계들(616 내지 622) 동안 식별되는 보안 데이터 트랜잭션의 임의의 적합한 특성이 단계(628)의 디바이스 트랜잭션 데이터(678)에서 식별된 것과 임의의 적합한 양만큼(예컨대, 특정 데이터 유형의 백분을 변동, 예컨대 금융 거래 통화 가치의 10% 이상 또는 건강 데이터에 대한 타임 프레임의 10% 이상) 상이하거나 또는 특정 유형(예컨대, 상이한 유형들의 데이터가 식별되거나, 예를 들어 건강 데이터의 유형이 식별된 데이터의 두 인스턴스 간에 상이하거나(예컨대, 심박수 데이터와 계보(miles walked) 데이터, 또는 생체인식 데이터와 결제 데이터 등) 및/또는 거래에 사용되고 있는 통화의 유형이 식별된 데이터의 두 인스턴스 간에 상이하거나(예컨대, 달러와 엔 등) 및/또는 상품의 배달을 위한 결제 트랜잭션의 배송 주소의 위치가 상이함) 만큼 상이한 경우) 확인되지 않을 수 있다. 데이터 비교는 예상 표준에서 벗어난 소정 인스턴스들을 검출(예컨대, 그 때까지 단지 결제 크리덴셜 데이터를 트랜잭션한 판매자에 의한 첫번째 바이오데이터의 트랜잭션을 검출하는 등)하기 위하여 특정 판매자에 대한 특정 트랜잭션에 대하여 실제로 수신된 데이터와 누적된 과거 데이터 간에 이루어질 수 있으며, 잠재적 트랜잭션 식별 정보는 판매자에 의한 사기를 확인 또는 검출하는 데 사용될 수 있으며 반드시 사용자 디바이스에 대하여 사용되는 것은 아니다(예컨대, 누적 데이터는 판매자에 대해 추적될 수 있지만, 최종 사용자들의 프라이버시 염려를 존중하는 소정 경우들에서 디바이스에 대하여 추적되지 않음).

[0084]

그 다음, 단계(631)에서, 프로세스(600)는 상업적 개체 서브시스템(400)이 결제 요청 데이터(610) 및/또는 확인 세션에 의해 및, 그에 따라, 디바이스 트랜잭션 데이터(678)에 의해 식별되었을 수 있는 판매자와 연관된 판매자 키(예컨대, 판매자 키(157))를 식별하고, 이어서 그 판매자 키를 이용하여 디바이스 트랜잭션 데이터(678)의 적어도 일부분을 재암호화하는 것을 포함할 수 있다. 즉, 단계(629)에서 적합한 액세스 정보를 이용하여 디바이스 트랜잭션 데이터(678)의 적어도 일부분을 복호화한 후(예컨대, 보안 디바이스 데이터(677)를 복호화하여 디바이스 결제 크리덴셜 데이터(676) 및 보안 디바이스 데이터(677)에 암호화되었을 수 있는 임의의 기타 정보(예컨대, 확인 응답 데이터(674))를 현실화한 후), 상업적 개체 서브시스템(400)은 이어서, 단계(631)에서, 디바이스 트랜잭션 데이터(678)의 적어도 일부분(예컨대, 디바이스 결제 크리덴셜 데이터(676)의 토큰 데이터 및/또는 암호 데이터)을 디바이스 트랜잭션 데이터(678)에서 식별된 판매자 정보와 연관될 수 있거나 또는 단계(630)에서 확인된 링크된 확인 데이터와 연관되도록 표(430)에서 식별될 수 있는 적절한 판매자 키를 이용하여 재암호화할 수 있다. 예를 들어, 이러한 판매자 키(예컨대, 판매자 키(157))는 디바이스 트랜잭션 데이터(678)를 이용하여 식별된 상업적 개체 판매자 정보를 도 1a의 표(430)의 데이터와 비교함으로써 결정될 수 있다. 이렇게 적절한 판매자 키가 결정되면, 상업적 개체 서브시스템(400)은 그 판매자 키(예컨대, 판매자 키(157))를 이용하여 디바이스 트랜잭션 데이터(678)의 적어도 일부분(예컨대, 디바이스 결제 크리덴셜 데이터(676)의 토큰 데이터 및/또는 암호 데이터)을 암호화된 판매자 크리덴셜 데이터(681)처럼 재암호화할 수 있다. 예를 들어, 암호화된 판매자 크리덴셜 데이터(681)는 적어도 디바이스 트랜잭션 데이터(678)로부터의 암호화된 디바이스 결제 크리덴셜 데이터(676)뿐만 아니라 임의의 적합한 트랜잭션 데이터, 예컨대 구매량 데이터 또는 디바이스 트랜잭션 데이터(678) 및/또는 잠재적 트랜잭션 데이터(660)로부터의 또는 이에 기초하는 기타 적합한 트랜잭션 데이터를 포함할 수 있다. 디바이스 트랜잭션 데이터(678)로부터의 판매자 식별 정보는 암호화된 판매자 크리덴셜 데이터(681)에 포함될 필요가 없을 수 있는데, 왜냐하면 그 판매자 식별은 암호화된 판매자 크리덴셜 데이터(681)가 단계(631)에서 암호화될 때 사용한 판매자 키를 결정하는 데 이미 사용되었을 수 있기 때문이다. 암호화된 판매자 크리덴셜 데이터(681)는, 판매자 서브시스템(200)에 의해 수신되면, 그 서브시스템(200)이 상업적 개체 서브시스템(400)을 이러한 암호화된 판매자 크리덴셜 데이터(681)의 생성자로서 설정할 수 있도록 상업적 개체 서브시스템(400)에 의해 서명될 수 있고/있거나 이러한 암호화된 판매자 크리덴셜 데이터(681)가 서명된 이후에 변경되지 않았음을 보장하도록 판매자 서브시스템(200)을 인에이블할 수 있다. 이러한 암호화된 판매자 크리덴셜 데이터(681)는 단계(631)에서 생성되고, 단계(632)에서(예컨대, 상업적 개체 서브시스템(400)의 서버(410)로부터 디바이스(100)의 통신 컴포넌트(106)로 도 1a의 경로(65)를 통해) 안전한 트랜잭션 데이터(682)처럼 임의의 다른 적합한 데이터와 함께 디바이스(100)로 전송될 수 있다.

[0085]

단계들(631, 632)은 상업적 개체 서브시스템(400)으로부터 전송된 크리덴셜 데이터가 도 1a의 안전한 트랜잭션 데이터(682)의 일부(예컨대, 암호화된 판매자 크리덴셜 데이터(681)의 토큰 데이터 및/또는 암호 데이터)로서 보안 요소(145) 이외의 디바이스(100)의 일부분에 의해 복호화될 수 없는 방법으로 암호화될 수 있도록 보장하도록 동작할 수 있다. 즉, 안전한 트랜잭션 데이터(682)의 크리덴셜 데이터(예컨대, 암호화된 판매자 크리덴셜 데이터(681)의 토큰 데이터 및/또는 암호 데이터)는 디바이스(100)의 어떠한 부분에 의해, 예컨대, 일부 실시예들에서, 보안 요소(145)에 의해 노출되거나 또는 다른 방식으로 액세스 불가능한 판매자 키(예컨대, 판매자 키(157))를 이용하여 암호화될 수 있다. 또한, 안전한 트랜잭션 데이터(682)의 크리덴셜 데이터(예컨대, 암호화된 판매자 크리덴셜 데이터(681)의 토큰 데이터 및/또는 암호 데이터)는 보안 요소(145) 밖에 있는 디바이스(100)의 어떠한 부분에도 노출되거나 또는 다른 방식으로 액세스 불가능한 크리덴셜 키(155a')를 이용하여(예

컨대, 단계(626)에서) 암호화될 수 있다.

[0086] 안전한 트랜잭션 데이터(682)는 이어서 단계(634)에서 판매자 서브시스템(200) 상에 안전한 트랜잭션 데이터(684)처럼 (예컨대, 통신 경로(15)를 통해 또는 비접촉식 근접성 기반 통신(5)으로서) 전달될 수 있다. 대안적으로, 판매자 크리덴셜 데이터(681)는 디바이스(100)를 통해 전달되지 않고 (미도시) 상업적 개체 서브시스템(400)으로부터 판매자 서브시스템(200)으로 전달될 수 있다. 잠재적 트랜잭션 데이터(660) 중 하나, 일부, 또는 모든 부분들은 디바이스(100) 및/또는 상업적 개체 서브시스템(400)을 통해 안전한 트랜잭션 데이터(682) 및/또는 안전한 트랜잭션 데이터(684)로 전달되어, 잠재적 트랜잭션의 소정의 식별자들이 프로세스(600) 동안 개체들의 각각에 의해 식별될 수 있으며, 소정의 식별자들은, (i) 특정 판매자 정보, 예컨대, 판매자의 고유 판매자 식별자(즉, "판매자 A") 및/또는 사용중인 특정 판매자 리소스의 식별(예컨대, 특정 판매자 애플리케이션(113')), (ii) 특정 트랜잭션 정보, 예컨대, 트랜잭션 결제에 사용될 특정 통화의 식별(예컨대, 엔, 파운드, 달러 등) 및/또는 트랜잭션에 결제할 특정 통화량의 식별(즉, "가격 C") 및/또는 구매 또는 대여 또는 다른 방식으로 결제할 특정 제품 또는 서비스의 식별(즉, "제품 B") 및/또는 사용될 기본 또는 초기 배송 주소의 식별(즉, "배송 D"), (iii) 트랜잭션에 대하여 판매자에게 허용가능한(예컨대, 구매에 사용될 수 있는 결제 카드들의 리스트(예컨대, 마스터카드는 가능하지만 비자는 불가)) 또는 디바이스(100)에 의해 선택되는(즉, "크리덴셜 X") 하나 이상의 유형의 결제 방법을 나타내는 정보, (iv) 고유 판매자 기반 트랜잭션 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행되고 있는 트랜잭션과의 연관성을 위하여 판매자 서브시스템(200)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 자 영숫자 스트링), (v) 고유 사용자 디바이스-기반 트랜잭션 식별자(예컨대, 임의의 적합한 데이터 요소, 예컨대, 수행되고 있는 트랜잭션과의 연관성을 위하여 디바이스(100)에 의해 무작위로 또는 고유하게 생성될 수 있는 3 또는 4 자 영숫자 스트링), (vi) 고유 판매자 온라인 리소스 확인 세션 식별자) 등을 포함하지만, 이에 한정되지 않는다.

[0087] 결제 크리덴셜 데이터(675/676)를 포함하는 판매자 크리덴셜 데이터(681)가 판매자 서브시스템(200)에 의해 (예컨대, 단계(634)의 안전한 트랜잭션 데이터(684)처럼) 수신되면, 프로세스(600)는 또한 단계(636)를 포함할 수 있으며, 여기서 판매자 서브시스템(200)은 결제 데이터(686)를 생성하여 매수 은행 서브시스템(300)에 전송하도록 구성될 수 있고(예컨대, 도 1a의 판매자 서브시스템(200)과 매수 은행 서브시스템(300) 간의 통신 경로(25)를 통해), 데이터(686)는 디바이스(100)의 안전한 디바이스 결제 크리덴셜 데이터 및 제품 또는 서비스에 대한 판매자의 구매 가격을 나타낼 수 있는 결제 정보 및 인가 요청을 포함할 수 있다(예컨대, 안전한 트랜잭션 데이터(684)에 포함되거나 또는 다른 방식으로 그것과 연관될 수 있거나 또는 판매자 서브시스템(200)에 의해 알려진 바와 같이 다른 방식으로 트랜잭션과 연관될 수 있음(예컨대, 잠재적 트랜잭션 데이터(660)에 의함(예컨대, 고유 트랜잭션 식별자에 기초함))). 예를 들어, 단계(636)에서, 판매자 서브시스템(200)은 그것의 알려진 판매자 키(157)를 이용하여 적어도 부분적으로 안전한 트랜잭션 데이터(684)의 판매자 크리덴셜 데이터(681)를 복호화할 수 있으며, 결제 데이터(686)는 크리덴셜 SSD(154a)의 안전한 결제 크리덴셜 데이터를 포함할 수 있는데, 결제 크리덴셜 데이터는 그것의 크리덴셜 키(155a')(예컨대, 데이터(676))로 암호화되지만 금융 기관 서브시스템(350)에 이용불가능한 키로 암호화되지 않는다.

[0088] 결제 데이터(686)가 단계(636)에서 매수 은행 서브시스템(300)으로 전송되면, 단계(638)에서, 매수 은행 서브시스템(300)은 결제 데이터(686)로부터의 인가 요청 정보를 금융 기관 서브시스템(350)으로 인가 요청 데이터(688)로서 (예컨대, 도 1a의 매수 은행 서브시스템(300)과 금융 기관 서브시스템(350) 간 통신 경로(35)를 통해) 전달할 수 있다. 그 다음, 단계(640)에서, 금융 기관 서브시스템(350)의 발행 은행 서브시스템(370)이 인가 요청을 수신하면(예컨대, 단계(640)에서 데이터(688)처럼 매수 은행 서브시스템(300)으로부터 직접, 또는 데이터(405)처럼 결제 네트워크 서브시스템(360)을 통해 간접적으로), 결제 정보(예컨대, 디바이스(100)의 보안 요소(145)에 의한 크리덴셜 키(155a')(예컨대, 데이터(676))에 의해 암호화된 디바이스(100)의 결제 크리덴셜 데이터(675)) 및 구매량(이들은 각각 인가 요청 데이터(688), 및 데이터(682, 684, 및/또는 686)에 포함될 수 있음)은 (예컨대, 크리덴셜 키(155a'))를 이용하여 금융 기관 서브시스템(350)에서) 복호화되고 분석되어 상거래 크리덴셜과 연관된 계좌의 크레딧이 구매량을 커버할 정도로 충분한지 결정할 수 있다. 충분한 자금이 없는 경우, 발행 은행 서브시스템(370)은 부정적인 인가 응답을 매수 은행 서브시스템(300)에 전송함으로써 요청된 트랜잭션을 거절할 수 있다. 그러나, 충분한 자금이 존재하는 경우, 발행 은행 서브시스템(370)은 긍정적인 인가 응답을 매수 은행 서브시스템(300)에 전송함으로써 요청된 트랜잭션을 승인할 수 있고, 금융 거래는 완료될 수 있다. 두 유형의 인가 응답이 프로세스(600)의 단계(640)에서 사용자 금융 서브시스템(350)에 의해 매수 은행 서브시스템(300)으로 인가 응답 트랜잭션 상태 데이터(690)로서 (예컨대, 발행 은행 서브시스템(370)으로부터 매수 은행 서브시스템(300)으로 통신 경로(35)를 통해 직접, 또는 발행 은행 서브시스템(370)으로부터 도 1a의 통신 경로(45)를 통해 결제 네트워크 서브시스템(360)에 제공될 수 있는 인가 응답 데이터(415)에 기초하여 결

제 네트워크 서브시스템(360)으로부터 매수 은행 서브시스템(300)으로) 제공될 수 있다. 그 다음, 단계(640)에서 인가 응답 트랜잭션 상태 데이터(690)를 수신하는 것에 응답하여, 프로세스(600)는 또한 매수 은행 서브시스템(300) 또는 임의의 다른 적합한 서브시스템이 이러한 인가 응답 트랜잭션 상태 데이터를 판매자 서브시스템(200)과 인가 응답 트랜잭션 상태 데이터(692)로서 단계(642)에서 공유하는 것을 포함할 수 있으며, 이는 이어서 디바이스(100)와 (예컨대, 판매자 리소스를 이용하여 또는 다른 방식으로) 승인된 트랜잭션 상태 데이터(694)로서 단계(644)에서 공유될 수 있다. 이러한 확인된 트랜잭션 상태 데이터는 임의의 적합한 승인 데이터, 예컨대, 도 3d의 스크린(190d)의 승인 데이터(317)를 디바이스(100)에 제공하도록 구성될 수 있다. 트랜잭션이 성공하는 경우, 승인된 트랜잭션 상태 데이터는 단계(644)에서 디바이스(100)의 트랜잭션을 종료하도록 동작할 수 있다. 추가적으로 또는 대안적으로, 트랜잭션이 성공하지 않은 경우, 승인된 트랜잭션 상태 데이터는 트랜잭션을 종료하도록 동작하거나 또는 동작하지 않을 수 있다(예컨대, 유효한 자금이 이용가능하지 않거나 또는 디바이스가 사기로 식별되는 경우 트랜잭션을 종료하지만, 유효하지 않은 배송 주소가 결정되는 경우 계속 열어 놓고 업데이트를 허용함). 임의의 비-트랜잭션-종료 트랜잭션 상태 데이터는 결제 프로세스로 하여금 프로세스가 애플리케이션에 의해 취소되거나, 프로세스가 사용자에게 의해 취소되거나, 또는 프로세스가 완료될 때까지 계속되도록 할 수 있다.

[0089] 따라서, 판매자 서브시스템(200)은 안전한 트랜잭션 데이터(684) 또는 판매자 크리덴셜 데이터(681)의 임의의 기타 전달자를 임의의 적합한 방법으로 프로세싱하도록 구성될 수 있다. 예를 들어, 디바이스 결제 크리덴셜 데이터를 판매자 크리덴셜 데이터(681)로부터 획득하기 위하여, 판매자 서브시스템(200)은 수신된 판매자 크리덴셜 데이터(681)의 서명 특성이 유효한지 그리고 상업적 개체 서브시스템(400)이 그 서명의 서명자인지 검증할 수 있다. 판매자 서브시스템(200)은 임의의 적합한 기술을 사용하여 어떤 판매자 키(예컨대, 어떤 판매자 공개 키(157))가 상업적 개체 서브시스템(400)에 의해 판매자 크리덴셜 데이터(681)를 구성하는 데 사용되었을 수 있는지 결정할 수 있다. 이어서, 판매자 서브시스템(200)은 대응하는 판매자 개인키(예컨대, 판매자 서브시스템(200)에서의 판매자 개인키(157))를 검색할 수 있고, 그 검색된 키를 이용하여 암호화된 판매자 크리덴셜 데이터(681)를 압축해제 및/또는 복호화하여 암호화된 데이터(676)를 복구할 수 있다. 이어서 이러한 데이터(676)는 적절한 결제 네트워크(360)에 제공될 수 있고, 이는 금융 기관 서브시스템(350)의 적절한 크리덴셜 키(155a')를 이용하여 암호화된 디바이스 결제 크리덴셜 데이터(676)를 압축해제 및/또는 복호화하여 디바이스 결제 크리덴셜 데이터(675)를 복구할 수 있다(예컨대, 디바이스 결제 크리덴셜 데이터(675)의 토큰 데이터 및/또는 암호 데이터를 복구하여 디바이스 결제 크리덴셜 데이터(675)를 확인하기 위하여 (예컨대, 수신된 디바이스 결제 크리덴셜 데이터(675)의 토큰 데이터에 기초하여 암호 데이터를 독립적으로 생성하고, 그 생성된 암호 데이터를 수신된 디바이스 결제 크리덴셜 데이터(675)의 암호 데이터와 비교하고, 비교 결과에 기초하여 트랜잭션을 확인하거나 또는 거절함)).

[0090] 도 6의 프로세스(600)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 추가적인 단계들이 추가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다. 도시되지 않았지만, 안전한 트랜잭션 데이터는 상업적 개체 서브시스템(400)으로부터 판매자 서브시스템(200)으로 직접(예컨대, 단계들(632, 634)에서 통신 경로(85)를 통해 그리고 디바이스(100)를 통하지 않고) 또는 금융 기관 서브시스템(350)에 직접(예컨대, 단계들(632 내지 638)에서 통신 경로(55)를 통해 그리고 디바이스(100)를 통하지 않고/않거나 판매자 서브시스템(200)을 통하지 않고/않거나 매수 은행(300)을 통하지 않고) 전달될 수 있다. 추가적으로 또는 대안적으로, 도시되지 않았지만, 안전한 트랜잭션 데이터는 디바이스(100)로부터 금융 기관 서브시스템(350)으로 직접(예컨대, 판매자 서브시스템(200)을 통하지 않고) 전달될 수 있다. 프로세스(600)의 임의의 확인 단계가 실패한다면, 이러한 실패는 하나 이상의 적합한 개체에 전달될 수 있음이 이해될 것이다. 예를 들어, 챌린지 요청 데이터(664)의 확인이 단계(616)에서 실패하고/하거나 챌린지 응답 데이터(670)의 확인이 단계(622)에서 실패하고/하거나 디바이스 트랜잭션 데이터(678)의 확인 응답 데이터(674)의 확인 데이터의 확인이 단계(630)에서 실패한다면, 이러한 실패는 상업적 개체 서브시스템(400)에 의해 판매자 서브시스템(200) 및/또는 전자 디바이스(100)와 공유되어 디바이스(100)가 판매자 서브시스템(200)과의 잠재적 트랜잭션을 취소하고 잠재적으로 판매자 온라인 리소스를 디바이스(100)로부터 제거할 수 있다. 디바이스(100)의 사용자가 단계(625)에서 보안 데이터 트랜잭션에 사용할 소정 보안 데이터(예컨대, 특정 결제 크리덴셜의 소정 결제 크리덴셜 데이터)를 선택할 수 있는 후에, 프로세스(600)의 남은 단계들은 그 사용자에게 곧바로 일어날 수 있다(예컨대, 단계들(626 내지 644)이 디바이스(100)와 임의의 추가적인 사용자 상호작용 없이 일어날 수 있고 디바이스(100)의 사용자에게 즉시 보일 수 있음). 프로세스(600)는 디바이스(100)의 사용자에게, 단계(625) 후에, 보안 디바이스 데이터가 자동으로 즉시 판매자 서브시스템(200)에 송신되고, 트랜잭션의 상태가 디바이스(100)에 (예컨대, 판매자 서브시스템(200) 및/또는 상업적 개체 서브시스템(400)에 의해) 승인될 수 있는 것처럼 보일 수 있

다. 추가적으로 또는 대안적으로, 판매자 온라인 리소스의 확인은 디바이스(100)에 곧바로 일어날 수 있다(예컨대, 단계(612)가 없는 경우에도 단계들(614 내지 624)이 디바이스(100)와 임의의 사용자 상호작용 없이 일어날 수 있고, 단계(610) 후에 디바이스(100)의 사용자에게 즉시 보일 수 있음). 대안적으로, 일부 실시예들에서, 프로세스(600)는 전체가 디바이스(100)의 사용자에게 곧바로 일어날 수 있다(예컨대, 디바이스(100)는 보안 디바이스 트랜잭션이 언제 일어나야 하는지 자동으로 결정하고, 확인 응답 데이터를 자동으로 수신하고/하거나 디바이스 트랜잭션 데이터를 자동으로 송신하고/하거나 디바이스(100)와 임의의 능동적인 사용자 상호작용 없이 보안 디바이스 트랜잭션에 대한 안전한 트랜잭션 데이터를 자동으로 수신하고/하거나 송신하도록 구성될 수 있는 반면 판매자 온라인 리소스는 그 특정 보안 디바이스 트랜잭션에 대하여 개시되고 수행되는 확인 세션 동안 계속 확인될 수 있음). 예를 들어, 언급된 바와 같이, 모두 자동으로 디바이스(100)의 사용자에게 의한 임의의 능동적인 상호작용 없이, 디바이스(100)는 특정 제품이 구매되어야 한다고 결정하고 특정 제품에 대한 적어도 하나의 특정 판매자로부터 연관된 잠재적 트랜잭션 데이터를 획득하기 위하여 하나 이상의 판매자와 상호작용하도록 구성될 수 있다(예컨대, 디바이스(100)는 (예컨대, 더 많은 세탁 세제가 세탁기에 의해 필요함을 검출하거나 또는 사용자에게 의해 특정 날짜에 더 많은 세제를 사도록 사전설정된 캘린더 이벤트를 검출하는) 가전 제품이 구매되어야 한다고 결정하도록 구성될 수 있고, 자동으로 그 제품에 대하여 최고의 거래를 제공하는 특정 판매자를 식별할 수 있고, 자동으로 판매자와 상호작용하여 잠재적 트랜잭션 데이터를 획득하여 판매자로부터 그 제품을 구매할 수 있는 가전 제품일 수 있음). 그 후, 디바이스(100) 및/또는 특정 판매자는 단계(612)의 확인 세션을 자동으로 개시하도록 동작할 수 있다.

[0091]

일부 실시예들에서, 단계들(618 내지 622)은 챌린지 요청이 단계(616)에서 확인된 후에는 생략될 수 있고, 대신에, 단계(616)에서 챌린지 데이터 대신에 확인 데이터가 생성되고 저장될 수 있다. 따라서, 일부 실시예들에서, 단계들(614, 616)은 특정 확인 세션에 대한 판매자 온라인 리소스를 확인하는 데 적합할 수 있다. 일부 실시예들에서, 단계(616)에서 생성된 챌린지 데이터는 단계(622)에서 생성된 확인 데이터와 상이할 수 있다. 예를 들어, 챌린지 데이터의 길이는 챌린지 데이터(668)를 이용하여 판매자 서브시스템(200)에 대한 현저하게 견고한 챌린지를 인에이블하기에 충분한 무작위성을 제공하기에 충분할 수 있지만(예컨대, 적합한 길이의 데이터의 스트링, 예컨대, 10 자 이상), 확인 데이터는 세션 확인의 증명을 인에이블하기에 충분한 무작위성을 제공하고/하거나 확인 응답 데이터(674)를 이용하여 임의의 적합한 표준을 충족(예컨대, 유로페이 마스터 카드 비자("EMV") 표준의 데이터 길이 요구사항을 충족함)하기에 챌린지 데이터보다 짧을 수 있다(예컨대, 확인 데이터는 챌린지 데이터의 길이보다 짧은, 예컨대, 6 자 길이의 데이터의 스트링일 수 있음). 대안적으로, 챌린지 데이터와 확인 데이터는 동일하고 단계(616) 및 단계(622)에서 재사용될 수 있다. 확인 응답 데이터(674)의 확인 데이터(예컨대, 난스)는 상업적 개체 서브시스템(400)에 의해 생성되고 판매자 서브시스템(200)의 챌린지의 성공적인 확인에 기초하여 단계(624)에서 디바이스(100)로 제공될 수 있지만, 단지 결제 트랜잭션이 디바이스(100)와 판매자 사이에서 일어날 것이라는 결정에 기초하여 제공되지 않는다. 디바이스(100)는 디바이스(100) 상의 판매자에 특정할 수 있는 원시 애플리케이션을 통해 판매자 서브시스템(200)과 통신할 수 있고, 이어서 판매자 애플리케이션(113)은 이러한 애플리케이션에 의해 제공될 수 있다. 그러나, 디바이스(100)가 판매자에 특정할 수 있거나 또는 판매자에 특정할 수 없지만 판매자에 의해 관리되는 웹사이트(예컨대, 판매자의 제어 하의 서버상)에 지향될 수 있는 인터넷 브라우저 애플리케이션 또는 하이브리드 애플리케이션을 통해 판매자 서브시스템(200)과 통신할 수 있으면, 판매자 애플리케이션(113)은 통신을 판매자의 웹사이트로 (예컨대, 통신 컴포넌트(106)를 통해) 전달할 수 있는 레이아웃 엔진 소프트웨어 컴포넌트(예컨대, 웹킷)일 수 있다. 예를 들어, 디바이스(100)의 이러한 애플리케이션(113)은 판매자 서브시스템(200)에 제공될 임의의 디바이스 트랜잭션 데이터를 위한 도판일 수 있다.

[0092]

프로세스(600)의 소정 부분들의 대안적인 실시예들이 이제 상이한 판매자-구성들에 대하여 기재될 수 있다. 판매자 서브시스템(200)은 다양한 정도의 제어로 프로세스(600)의 보안 트랜잭션을 처리하도록 구비될 수 있다. 제1 판매자-구성에서, 판매자 서브시스템(200)은 전체 프로세스의 제어권을 보유할 수 있고, 판매자 서브시스템(200)은 판매자 온라인 리소스의 확인뿐만 아니라(예컨대, 단계들(614, 616) 및/또는 단계들(618, 620)에서, 판매자 서브시스템(200) 자체적으로 상업적 개체 서브시스템(400)과 통신하여 판매자 온라인 리소스를 확인할 수 있음) 상업적 개체 서브시스템(400)에 의해 암호화된 보안 데이터의 복호화(예컨대, 단계(636)에서, 판매자 서브시스템(200)은 판매자 키(157)를 이용하여 적어도 부분적으로 안전한 트랜잭션 데이터(684)의 판매자 크리덴셜 데이터(681)를 복호화할 수 있음)도 처리하도록 동작할 수 있다. 이러한 제1 판매자-구성에서, 판매자 서브시스템(200)은 자체 결제 서비스 제공자("PSP")의 역할을 할 수 있고, 프로세스(600)에서 온라인 리소스를 등록하고 확인하기 위해 상업적 개체 서브시스템(400)과 통신하는 유일한 서브시스템일 수 있으며, 이는 물량이 많은 대형 판매자(예컨대, 아마존닷컴(Amazon.com))에게는 통상적일 수 있다. 대안적으로, 제2 판매자-구성에서,

판매자 서브시스템(200)은 결제 복호화 책무를 임의의 적합한 판매자-파트너 서브시스템, 예컨대, PSP 서브시스템(310)에 넘겨줄 수 있는데, 이는 도 1a 및 도 6에서 매수 은행(300)의 일부인 것으로 도시될 수 있다. 이러한 제2 판매자-구성에서, 판매자 서브시스템(200)은 판매자 온라인 리소스의 확인을 처리하도록(예컨대, 단계(614) 및/또는 단계들(618, 620)에서, 판매자 서브시스템(200) 자체적으로 상업적 개체 서브시스템(400)과 통신하여 판매자 온라인 리소스를 확인함) 동작할 수 있고, PSP 서브시스템(310)은 상업적 개체 서브시스템(400)에 의해 암호화된 보안 데이터의 복호화를 처리하도록(예컨대, 단계(638)에서, PSP 서브시스템(310)은 판매자 키(157)를 이용하여 적어도 부분적으로 결제 데이터(686)의 판매자 크리덴셜 데이터(681)를 복호화할 수 있음) 동작할 수 있다. 이러한 제2 판매자-구성에서, 판매자 서브시스템(200)은 그것의 결제 복호화를 위해 별개의 제3자 백-엔드 PSP를 사용할 수 있으며, 판매자 서브시스템(200) 및 PSP 서브시스템(310) 둘 모두는 프로세스(600)에서 상업적 개체 서브시스템(400)과 통신하여 온라인 리소스를 등록할 수 있는데, 이는 결제 서비스 제공자(예컨대, 매수 은행(예컨대, 체이스 페이먼트테크(Chase Paymentech)))를 활용할 수 있는 소형 판매자 또는 다수의 매수 은행, 카드, 및 결제 네트워크들과 통신 및/또는 판매자 서브시스템(200)을 대신하여 외부 네트워크 및 은행 계좌와의 이러한 기술적 연결성 및 관계를 관리하도록 동작함으로써, 판매자 서브시스템(200)이 금융 기관에 덜 의존하게 하는 소형 PSP(예컨대, 스트라이프(Stripe), 브레인트리(Braintree), 퍼스트 데이터(First Data) 등))에게 통상적일 수 있다. 이러한 제2 판매자-구성의 PSP 서브시스템(310)은 디바이스(100)의 사용자로부터 숨겨질 수 있는데, 디바이스(100)의 사용자는 단지 판매자 서브시스템(200)의 온라인 리소스와(예컨대, 도 3a 내지 도 3d의 스크린들(190a 내지 190d)에서) 교류할 수 있다. 대안적으로, 제3 판매자-구성에서, 판매자 서브시스템(200)은 온라인 리소스 확인 책무 및 결제 복호화 책무를 임의의 적합한 판매자-파트너 서브시스템, 예컨대, PSP 서브시스템(310)에 넘겨줄 수 있다. 이러한 제3 판매자-구성에서, PSP 서브시스템(310)은 판매자 온라인 리소스의 확인뿐만 아니라(예컨대, 단계(614)에서, PSP 서브시스템(310) 자체적으로(예컨대, PSP 서브시스템(310)이 세션 개시 데이터(662)를 판매자 서브시스템(200)으로부터 수신하는 것에 응답하여) 챗봇지 요청 데이터(664)를 상업적 개체 서브시스템(400)과 교환하여 판매자 온라인 리소스를 확인하고) 상업적 개체 서브시스템(400)에 의해 암호화된 보안 데이터의 복호화(예컨대, 단계(638)에서, PSP 서브시스템(310)은 판매자 키(157)를 이용하여 적어도 부분적으로 결제 데이터(686)의 판매자 크리덴셜 데이터(681)를 복호화함)를 처리하도록 동작할 수 있다. 이러한 제3 판매자-구성에서, 판매자 서브시스템(200)은 확인 및 결제 복호화를 위하여 별개의 제3자 프론트-엔드 PSP를 사용할 수 있어서, 판매자 서브시스템(200) 및 PSP 서브시스템(310) 둘 모두는 프로세스(600)에서 상업적 개체 서브시스템(400)과 통신하여 온라인 리소스를 등록 및 확인할 수 있으며, 이는 제3자 결제 서비스 제공자에 의존하여 그들을 대신하여 전체 체크아웃 및 결제 프로세스를 수행할 수 있는 "롱테일(long tail)" 판매자(예컨대, 스프라이트 체크아웃(Stripe Checkout)이 스프라이트 인크(Stripe, Inc.)의 PSP에 제공될 수 있음)에 대하여 통상적일 수 있다. 별개의 제3자 프론트-엔드 PSP 서브시스템(310)은 판매자 서브시스템(200)의 웹 리소스 내에서 작동할 수 있는 데스크톱, 태블릿, 및 모바일 디바이스들을 위한 내장형 결제 형태(예컨대, 이는 PSP 서브시스템(310)의 서버 상에 호스팅될 수 있는, 예컨대, 판매자 서브시스템(200)의 판매자 리소스에 내장되는 PSP 서브시스템(310)의 자바 스크립트)를 제공하여, 고객(예컨대, 디바이스(100)의 사용자)이 판매자 서브시스템(200)의 웹 리소스로부터 넘어와서 트랜잭션을 완료하거나 또는 고객이 판매자 서브시스템(200)의 웹 리소스에서 PSP 서브시스템(310)의 웹 리소스로 넘어가서 프로세스(예컨대, 페이팔닷컴(PayPal.com))를 완료하지 않고 고객이 PSP 서브시스템(310)의 그 결제 형태를 통해 결제할 수 있게 한다. 이러한 제3 판매자-구성의 PSP 서브시스템(310)은 판매자 온라인 리소스와 유사할 수 있는 PSP 온라인 리소스를 관리 및 운영하도록 동작할 수 있지만, 결제를 자체적으로 프로세싱하도록 구비되지 않은 판매자 온라인 리소스에 의해 활용될 수 있는데, 예를 들어, 웹사이트 판매자 온라인 리소스(113)는 그 웹사이트 판매자 온라인 리소스(113)와 인터페이스하는 디바이스(100)의 사용자를, 웹사이트 판매자 온라인 리소스(113)의 임의의 부분 내에 내장될 수 있거나 또는 사용자가 웹사이트 판매자 온라인 리소스(113)의 임의의 적합한 부분으로부터 넘어올 수 있는 웹사이트 PSP 온라인 리소스(113)의 인터페이스로 인도할 수 있다(예컨대, 도 3a 내지 도 3d의 스크린들(190a 내지 190d)의 하나 이상의 임의의 적합한 부분들은 웹사이트 판매자 온라인 리소스 대신에 웹사이트 PSP 온라인 리소스에 의해 제공될 수 있음). 따라서, 판매자 서브시스템(200) 및 PSP 서브시스템(310)(예컨대, 매수자 서브시스템(300))은 함께 시스템(1)의 유일한 견고한 프로세싱 서브시스템(299)을 제공할 수 있거나 또는 시스템(1)의 구성 및 판매자 서브시스템(200)의 역량에 따라 시스템(1)의 별개의 개체들로서 사용될 수 있다.

[0093]

판매자 온라인 리소스를 상업적 개체 서브시스템(400)에 등록하는 것은 판매자 서브시스템(200)이, 단독으로 또는 PSP 서브시스템(310)과 조합하여(예컨대, 3개의 판매자-구성들 중 어느 것이 채용되는지에 따라), 상업적 개체 서브시스템(400)을 이용하여 온라인 리소스를 확인하고 또한 상업적 개체 서브시스템(400)에 의해 암호화된 것처럼 크리덴셜 데이터를 복호화하도록 동작하도록, 상업적 개체 서브시스템(400)을 이용하여 등록하는 것을

포함할 수 있다. 예를 들어, 단계(606)는 상업적 개체 서브시스템(400)과 판매자 서브시스템(200) 또는 PSP 서브시스템(310) 사이에 온라인 리소스와 연관된 하나 이상의 판매자 식별자(167)에 대한 판매자 키들(157)이 공유되는 것을 포함할 뿐만 아니라(이러한 키들(157)은 상업적 개체 서브시스템(400)에서(예컨대, 단계(631)에서) 데이터를 암호화하고 판매자 서브시스템(200) 또는 PSP 서브시스템(310)에서(예컨대, 단계(636)에서 또는 단계(638)에서) 그 데이터를 복호화하는 데 사용될 수 있음), 또한 상업적 개체 서브시스템(400)과 판매자 서브시스템(200) 또는 PSP 서브시스템(310) 사이에 온라인 리소스와 연관된 하나 이상의 판매자 식별자(167)에 대한 증명서(177)가 공유되는 것을 포함할 수 있으며, 증명서(177)는 (예컨대, 단계들(614, 616)에서) 온라인 리소스를 확인하는 데 사용될 수 있다.

[0094]

단지 하나의 예로서, 단계(606)에서, 온라인 리소스(예컨대, 웹사이트 판매자 온라인 리소스(113))에 대한 공유 키들에 대한 제1 증명서 서명 요청("CSR")이 생성되어 상업적 개체 서브시스템(400)에 전달될 수 있다. 공유 키들에 대한 이 제1 CSR은 온라인 리소스와 연관된 적어도 하나의 판매자 식별자(167), 예컨대, 온라인 리소스의 전체 주소 도메인 이름("FQDN")(예컨대, 그것의 정확한 위치, 예컨대, 루트 및 서브도메인들(예컨대, DNS 호스트명)을 명시할 수 있는 웹 도메인) 및/또는 온라인 리소스의 도메인에 링크될 수 있는 임의의 다른 적합한 판매자 식별자 및/또는 온라인 리소스와 연관될 수 있는 임의의 적합한 판매자-파트너의 임의의 다른 적합한 식별자(예컨대, 판매자 서브시스템(200)이 상업적 개체 서브시스템(400)에 의해 암호화된 크리덴셜 데이터를 복호화하기 위해 PSP를 사용할 수 있는 경우 PSP 식별자)를 포함할 수 있다. 상업적 개체 서브시스템(400)은 단계(606)에서 키 쌍(예컨대, 공개키 및 개인 판매자 키(157))이 제1 CSR의 판매자 식별자들(167) 중 하나 이상과 연관될 수 있는 상업적 개체 서브시스템(400)과 판매자 서브시스템(200) 또는 PSP 서브시스템(310) 간의 공유 비밀이 되도록 용이하게 함으로써 공유 키들에 대한 제1 CSR에 응답할 수 있다. 예를 들어, 키 쌍 중 제1 판매자 키(157)는 판매자 온라인 리소스에 대한 제1 CSR의 판매자 식별자들 중 하나, 일부, 또는 각각에 대하여 또는 다른 방식으로 그것들과 연관하여 상업적 개체 서브시스템(400)의 표(430)에 저장될 수 있는 반면, 키 쌍 중 제2 판매자 키(157)는 판매자 온라인 리소스에 대한 제1 CSR의 판매자 식별자들 중 하나, 일부, 또는 각각에 대하여 또는 다른 방식으로 그것들과 연관하여 판매자 서브시스템(200) 및/또는 PSP 서브시스템(310)에 저장될 수 있다. 하나 이상의 판매자 식별자는 특정 판매자 온라인 리소스(113)와 연관될 수 있는데, 예컨대, 제1 판매자 식별자(167)는 특정 판매자 온라인 리소스(113)와 고유하게 연관되고(예컨대, 웹 리소스 판매자 온라인 리소스(113)인 경우 FQDN) 및/또는 제2 판매자 식별자(167)는 특정 판매자 서브시스템(200)의 각각의 판매자 온라인 리소스(113)와 연관된다. 추가적으로 또는 대안적으로, 하나 이상의 판매자 키는 특정 판매자 식별자 또는 특정 판매자 온라인 리소스(113)와 연관될 수 있다. 단계(606)의 하나 이상의 인스턴스에서, 모든 그러한 판매자 키 및 판매자 식별자 연관성들이 상업적 개체 서브시스템(400)에 의해 저장되거나 또는 다른 방식으로 상업적 개체 서브시스템(400)에 (예컨대, 하나 이상의 표(430)) 액세스가능할 수 있다. 제1 판매자-구성에서, 판매자 서브시스템(200)은 이러한 제1 CSR을 생성하고 상업적 개체 서브시스템(400)에 제공할 수 있고, 판매자 서브시스템(200)은 판매자 키(157)를 온라인 리소스에 대한 제1 CSR의 판매자 식별자들(167)의 하나, 일부, 또는 각각에 대하여 또는 다른 방식으로 그것들과 연관하여 저장할 수 있다. 제2 및 제3 판매자-구성에서, PSP 서브시스템(310) 또는 판매자 서브시스템(200)은 이러한 제1 CSR을 생성할 수 있지만, PSP 서브시스템(310) 또는 판매자 서브시스템(200) 중 어느 하나가 이러한 제1 CSR을 상업적 개체 서브시스템(400)에 제공할 수 있고, PSP 서브시스템(310)은 상업적 개체 서브시스템(400)으로부터(예컨대, 직접 또는 판매자 서브시스템(200)을 통해) 판매자 키(157)를 수신하고 판매자 키(157)를 온라인 리소스에 대한 제1 CSR의 판매자 식별자들(167)의 하나, 일부, 또는 각각에 대하여 또는 다른 방식으로 그것들과 연관하여 저장할 수 있다.

[0095]

추가적으로, 단계(606)에서, 온라인 리소스(예컨대, 웹사이트 판매자 온라인 리소스(113))에 대한 증명서에 대한 제2 CSR이 생성되어 상업적 개체 서브시스템(400)에 전달될 수 있다. 증명서에 대한 이 제2 CSR은 온라인 리소스와 연관된 적어도 하나의 판매자 식별자(167), 예컨대, 제1 CSR의 적어도 하나의 판매자 식별자(167) 또는 다른 식별자(예컨대, 온라인 리소스의 FQDN 또는 온라인 리소스의 도메인에 링크될 수 있는 임의의 다른 적합한 판매자 식별자) 및/또는 온라인 리소스와 연관될 수 있는 임의의 적합한 판매자-파트너의 임의의 다른 적합한 식별자(예컨대, 판매자 서브시스템(200)이 온라인 리소스를 확인하기 위하여 PSP 서브시스템을 사용할 수 있는 경우 PSP 식별자)를 포함할 수 있다. 상업적 개체 서브시스템(400)은 증명서(177)가 생성되고 상업적 개체 서브시스템(400)과 판매자 서브시스템(200) 또는 PSP 서브시스템(310) 간에 공유되는 것을 용이하게 함으로써 단계(606)에서 증명서에 대한 제2 CSR에 응답할 수 있는데, 증명서(177)는 제2 CSR의 판매자 식별자들(167) 중 하나, 일부, 또는 전부를 포함할 수 있고 (예컨대, 상업적 개체 서브시스템(400)에 의해) 판매자 온라인 리소스에 대한 제1 CSR의 판매자 키를 이용하여 생성될 수 있다(예컨대, 이는 제2 CSR의 판매자 식별자들 중 하나 이상에 의해 식별될 수 있음). 예를 들어, 제2 CSR의 온라인 리소스에 대한 증명서(177)는 상업적 개체 서브시

시스템(400)의 표(430)에 온라인 리소스에 대한 제2 CSR의 판매자 식별자들 중 하나, 일부, 또는 각각에 대하여 또는 다른 방식으로 그것들과 연관하여 저장될 수 있는 반면, 증명서(177)는 또한 그것들의 판매자 서브시스템(200) 및/또는 PSP 서브시스템(310)에 온라인 리소스에 대한 제2 CSR의 판매자 식별자들 중 하나, 일부, 또는 각각에 대하여 또는 다른 방식으로 그것들과 연관하여 저장될 수 있다. 증명서(177)는 임의의 적합한 디지털 증명서, 예컨대, 전송 계층 보안("TLS") 증명서 또는 보안 소켓 계층("SSL") 증명서일 수 있다. 제1 판매자-구성 및 제2 판매자-구성 둘 모두에서, 판매자 서브시스템(200)은 이러한 제2 CSR을 생성하고 상업적 개체 서브시스템(400)에 제공할 수 있고, 판매자 서브시스템(200)은 증명서(177)를 온라인 리소스에 대한 제2 CSR의 판매자 식별자들(167) 중 하나, 일부, 또는 각각에 대하여 또는 다른 방식으로 그것들과 연관하여 저장할 수 있다. 제3 판매자-구성에서, PSP 서브시스템(310) 및/또는 판매자 서브시스템(200)은 이러한 제2 CSR을 생성하고, 이러한 제2 CSR을 상업적 개체 서브시스템(400)에 제공할 수 있고, PSP 서브시스템(310)은 증명서(177)를 온라인 리소스에 대한 제2 CSR의 판매자 식별자들(167) 중 하나, 일부, 또는 각각에 대하여 또는 다른 방식으로 그것들과 연관하여 저장할 수 있고, PSP 서브시스템(310)에 증명서(177)를 제공하기 위한 이 프로세스는 판매자 서브시스템(200)에 상관없이 수행될 수 있고 판매자 서브시스템(200)이 PSP 서브시스템(310)과 파트너십을 형성하기 이전에 수행될 수 있다 (예컨대, PSP 서브시스템(310)은 상업적 개체 서브시스템(400)의 신뢰하는 PSP일 수 있고, 판매자 서브시스템(200)이 PSP 서브시스템(310) 및 PSP 서브시스템(310)의 도메인을 통해 결제가 일어나는 프론트-엔드 PSP 모델을 제공하기 위하여 PSP 서브시스템(310)과 파트너를 맺기 전에 증명서(177)가 제공될 수 있음). 판매자 서브시스템(200)은 상업적 개체 서브시스템(400)에 PSP 제공된 도메인을 제공하고, 상업적 개체 서브시스템(400)으로부터 PSP 서브시스템(310)이 신뢰성있고 그 도메인에 대한 증명서(177)를 갖고 있다는 승인을 요청할 수 있다.

[0096]

추가적으로, 단계(606)에서, 제1 CSR 및 제2 CSR 중 어느 하나 또는 둘 모두의 핸들링 전, 중, 후에, 판매자 서브시스템(200)에 의한 또는 판매자-파트너 PSP 서브시스템(310)에 의한 웹사이트 온라인 리소스의 도메인(예컨대, FQDN)의 소유권은 검증되거나 또는 다른 방식으로 상업적 개체 서브시스템(400)에 증명될 수 있다(예컨대, 이는 단계(501)에 대하여 기재된 바와 같음). 키들에 대한 제1 CSR, 증명서에 대한 제2 CSR, 및 도메인 검증 중 어느 하나는 온라인 리소스를 등록하면 키들에 대한 제1 CSR, 증명서에 대한 제2 CSR, 및 도메인 검증 중 임의의 다른 하나 전 또는 후에 일어날 수 있다. 그러나, 일부 실시예들에서, 증명서에 대한 제2 CSR을 프로세싱하기 전에 도메인을 검증하는 것은 등록 프로세스를 더 용이하고/하거나 더 효율적으로 인에이블할 수 있다. 제1 판매자-구성 및 제2 판매자-구성 둘 모두에서, 판매자 서브시스템(200)은 등록되어 있는 웹사이트 판매자 온라인 리소스의 FQDN을 상업적 개체 서브시스템(400)과 공유할 수 있는데, 상업적 개체 서브시스템(400)은 임의의 적합한 파일(예컨대, JSON 파일 같은 것)을 판매자 서브시스템(200)에 제공할 수 있고, 판매자 서브시스템(200)은 그 파일에(예컨대, 공유된 판매자 키(157)를 이용하여) 서명하고 그 파일을 FQDN 상에 호스팅할 수 있고, 이어서 상업적 개체 서브시스템(400)은 FQDN으로부터 그 서명된 파일에 액세스하고 파일을(예컨대, 공유된 판매자 키(157)를 이용하여) 서명해제하여 액세스된 파일이 판매자 서브시스템(200)과 공유된 파일과 매칭되며 임의의 연관된 임계치가 충족되었음을(예컨대, 기간 등)을 승인할 수 있다. 제3 판매자-구성에서, PSP 서브시스템(310)은 등록되어 있는 웹사이트 온라인 리소스(예컨대, PSP의 웹사이트 온라인 리소스)의 FQDN을 상업적 개체 서브시스템(400)과 공유할 수 있고, 상업적 개체 서브시스템(400)은 임의의 적합한 파일(예컨대, JSON 파일 같은 것)을 PSP 서브시스템(310)에 제공할 수 있고, PSP 서브시스템(310)은 그 파일에(예컨대, 공유된 판매자 키(157)를 이용하여) 서명하고 그 파일을 FQDN 상에 호스팅할 수 있고, 이어서 상업적 개체 서브시스템(400)은 FQDN으로부터 그 서명된 파일에 액세스하고 파일을(예컨대, 공유된 판매자 키(157)를 이용하여) 서명해제하여 액세스된 파일이 PSP 서브시스템(310)과 공유된 파일과 매칭되며 임의의 연관된 임계치가 충족되었음을(예컨대, 기간 등)을 승인할 수 있다. 제3 판매자-구성에서, 판매자 서브시스템(200)은 판매자 서브시스템(200)과 PSP 서브시스템(310) 간의 파트너십을 나타내는 데이터를 상업적 개체 서브시스템(400)에 전달하도록 동작할 수 있으며, 상업적 개체 서브시스템(400)은 판매자 서브시스템(200)에 대한 PSP 서브시스템(310)의 유효성을 승인하고, 프로세스(600)의 다른 부분들 동안 임의의 적합한 사용을 위해 판매자 서브시스템(200)의 판매자 식별자(167)와 PSP 서브시스템(310)의 FQDN 및/또는 증명서(177) 간의 연관성을 (예컨대, 표(430) 내에) 저장하도록 동작할 수 있다. 일부 실시예들에서, 제2 판매자-구성 및 제3 판매자-구성에서 PSP 서브시스템(310)에 제공된 판매자 키(들)(157)는 PSP 서브시스템(310)에 의해 임의의 파트너 판매자 서브시스템(200)에 대하여 데이터를 복호화하는 데 널리 사용될 수 있다. 대안적으로, 제2 판매자-구성 및 제3 판매자-구성에서 PSP 서브시스템(310)에 제공된 판매자 키(들)(157)는 특정 파트너 판매자 서브시스템(200)에 특정할 수 있어서, 판매자 서브시스템(200)은 상업적 개체 서브시스템(400)과(예컨대, 키들에 대한 제1 CSR을 이용하여) 통신할 수 있고 이어서 PSP 서브시스템(310)이 그 판매자 서브시스템(200)에 특정한 이러한 판매자 키(들)(157)를(예컨대, 상업적 개

체 서브시스템(400)으로부터 또는 판매자 서브시스템(200)으로부터 직접) 수신하도록 인에이블할 수 있고, 이러한 판매자 키(들)(157)는 상업적 개체 서브시스템(400)에서(예컨대, 표(430) 내에) 및/또는 PSP 서브시스템(310)에서 임의의 적합한 판매자 서브시스템(200)의 판매자 식별자(167)에 대하여 저장되거나 또는 다른 방식으로 그것과 연관될 수 있다. 이는 특정 판매자 서브시스템이 더 이상 상업적 개체 서브시스템(400)에 의해 신뢰받지 않으면 판매자 특정 판매자 키(157)가 상업적 개체 서브시스템(400)에서 유효하지 않도록 인에이블할 수 있는 반면, PSP 서브시스템(310)의 다른 판매자 특정 키들이 다른 판매자 서브시스템에 대하여 계속 사용되도록 인에이블할 수 있다. 일부 실시예들에서, PSP 서브시스템(310)이 상업적 개체 서브시스템(400)과 직접 인터페이스하도록 인에이블하는 하나 이상의 API가 제공될 수 있는데, 이는 판매자 서브시스템(200)으로 하여금 그 프로세스에 직접 관여하도록 요구하지 않으면서 PSP 서브시스템(310)이 상업적 개체 서브시스템(400)과 임의의 판매자 키들(157) 및/또는 PSP 서브시스템(310)의 특정 파트너 판매자 서브시스템(200)에 특정할 수 있는 증명서(177)를 공유하도록 할 수 있다(예컨대, PSP 서브시스템(310)은 그 판매자에 대한 대체물로서 상업적 개체 서브시스템(400)에 대하여 판매자 역할을 할 수 있음). 증명서(177)는 또한 PSP 서브시스템(310)에 범용될 수 있거나 또는 특정 파트너 판매자 서브시스템(200)에 특정할 수 있다.

[0097]

따라서, 단계(606) 및/또는 단계(501)는 온라인 리소스의 도메인이 상업적 개체 서브시스템(400)에 의해 검증되는 것뿐만 아니라, 그 온라인 리소스의 도메인과 연관되거나 또는 동일한 판매자 식별자(167)가 판매자 키(157) 및 증명서(177) 둘 모두에 대하여 상업적 개체 서브시스템(400) 및 판매자 서브시스템(200)에서 저장되는 것 및/또는 상업적 개체 서브시스템(400)에서 온라인 리소스를 등록하기 위하여 판매자-파트너 PSP 서브시스템(310)에서 저장되는 것을 포함할 수 있다. 검증된 FQDN 및/또는 온라인 리소스의 임의의 다른 적합한 판매자 식별자(167)는 따라서 판매자 키(157) 및 증명서(177)에 대하여 상업적 개체 서브시스템(400) 및 판매자 서브시스템(200) 및/또는 PSP 서브시스템(310)에서 저장되어(예컨대, 프로세스(600)의 단계(606)에서 및/또는 프로세스(500)의 단계(501)에서) 확인 세션 동안 온라인 리소스의 FQDN의 확인을 인에이블할 뿐만 아니라(예컨대, 프로세스(600)의 단계들(614, 616) 및/또는 프로세스(500)의 단계(506)에서), 상업적 개체 서브시스템(400)에 의한 보안 데이터의 암호화(예컨대, 프로세스(600)의 단계(631) 및/또는 프로세스(500)의 단계(518)에서) 및 판매자 서브시스템(200) 또는 PSP 서브시스템(310)에 의한 그 암호화된 보안 데이터의 대응 복호화(예컨대, 프로세스(600)의 단계(636) 또는 단계(638)에서 및/또는 프로세스(500)의 단계(522) 이후)를 인에이블할 수 있다. 예를 들어, 제1 판매자-구성 및 제2 판매자-구성 둘 모두에서, 판매자 서브시스템(200)이 판매자 온라인 리소스(113)의 확인 세션을 개시하기 위하여 단계(612)에서 디바이스(100)로부터 임의의 적합한 판매자 온라인 리소스 확인 세션 개시 데이터(662)를 수신하는 것에 응답하여(이러한 확인 세션 개시 데이터(662)는 온라인 리소스의 식별자(예컨대, 디바이스(100)에 의해 액세스되고 있는 판매자 온라인 리소스의 FQDN)를 포함할 수 있음), 판매자 서브시스템(200)은 수행될 특정 보안 데이터 트랜잭션(예컨대, 단계(610) 및/또는 단계(612)에서 식별되는 것과 같은 금융 결제 트랜잭션)에 대한 판매자 온라인 리소스를 확인하기 위하여 단계(614)에서 임의의 적합한 챌린지 요청 데이터(664), 예컨대, 단계(606)에서 판매자 서브시스템(200)에 의해 수신되고 확인 세션 개시 데이터(662)의 FQDN에 대하여 저장된 증명서(177)를 상업적 개체 서브시스템(400)으로 전달하도록 동작할 수 있다. 대안적으로, 제3 판매자-구성에서, PSP 서브시스템(310)이 PSP 온라인 리소스(113)의 확인 세션을 개시하기 위하여 단계(612)에서 디바이스(100)로부터 임의의 적합한 온라인 리소스 확인 세션 개시 데이터(662)를 수신하는 것에 응답하여(이러한 확인 세션 개시 데이터(662)는 온라인 리소스의 식별자(예컨대, 디바이스(100)에 의해 액세스되고 있는 PSP 온라인 리소스의 FQDN)를 포함할 수 있음), PSP 서브시스템(310)은 수행될 특정 보안 데이터 트랜잭션(예컨대, 단계(610) 및/또는 단계(612)에서 식별되는 것과 같은 금융 결제 트랜잭션)에 대한 PSP 온라인 리소스를 확인하기 위하여 단계(614)에서 임의의 적합한 챌린지 요청 데이터(664), 예컨대, 단계(606)에서 PSP 서브시스템(310)에 의해 수신되고 확인 세션 개시 데이터(662)의 FQDN에 대하여 저장된 증명서(177)를 상업적 개체 서브시스템(400)으로 전달하도록 동작할 수 있다. 단계(614)에서 판매자 서브시스템(200) 또는 PSP 서브시스템(310)으로부터 상업적 개체 서브시스템(400)으로 전달된 이러한 챌린지 요청 데이터(664)는 상업적 개체 서브시스템(400)에 대한 온라인 리소스의 유효성을 증명하도록 시도하기 위한 임의의 적합한 데이터를 포함할 수 있으며, 임의의 적합한 데이터는 단계(606)에서 상업적 개체 서브시스템(400)에 의해 생성된, FQDN 및/또는 온라인 리소스와 연관된 임의의 다른 적합한 식별자를 포함할 수 있는 증명서(177), 및 임의의 다른 적합한 데이터(예컨대, 디바이스(100)를 식별하는 데이터 및/또는 수행될 특정 보안 데이터 트랜잭션을 식별하는 데이터(예컨대, 단계(610) 및/또는 단계(612)에서 식별되는 금융 결제 트랜잭션, 이는 본 명세서에서 잠재적 트랜잭션 식별 정보로 지칭될 수 있고, 임의의 추가적인 보안 계층(들)을 현재 데이터 트랜잭션 프로세스에 제공 및/또는 향후 데이터 트랜잭션들에 대한 임의의 추가적인 보안(예컨대, 사기 검출) 서비스를 제공하기 위한 프로세스(600)의 임의의 적합한 부분들 동안 사용될 수 있음)를 포함하지만, 이에 한정되지 않는다.

[0098]

프로세스(600)의 단계(616)에서, 상업적 개체 서브시스템(400)이 단계(614)에서 판매자 서브시스템(200) 또는 PSP 서브시스템(310)으로부터 증명서(177)를 구비한 임의의 적합한 챌린지 요청 데이터(664)를 수신하는 것에 응답하여, 상업적 개체 서브시스템(400)은 챌린지 요청의 판매자 식별자(167)에 의해 식별된 온라인 리소스(113)를 확인하도록 동작할 수 있다. 예를 들어, 제1 판매자-구성 및 제2 판매자-구성 둘 모두에서, 상업적 개체 서브시스템(400)이 단계(614)에서 판매자 서브시스템(200)으로부터 증명서(177)를 구비한 임의의 적합한 챌린지 요청 데이터(664)를 수신하는 것에 응답하여, 상업적 개체 서브시스템(400)은 수신된 챌린지 요청 데이터(664)의 증명서(177)를 검증하고 체크하여 임의의 적합한 프로세스(들)를 통해 그것의 신뢰성이 아직 유효하고 만료되지 않았음을 보장하도록 동작할 수 있다(예컨대, 증명서(177)는 상업적 개체 서브시스템(400)에 의해 데이터(664)에서 수신될 수 있고 이어서 상업적 개체 서브시스템(400)은 그 증명서(177)가 상업적 개체 서브시스템(400)에 알려졌는지(예컨대, 표(430)에 저장되어 있는지) 그리고 그 증명서(177)가 아직 신뢰할 수 있는지 및/또는 그 증명서(177)가 만료되지 않았는지 결정하도록 동작할 수 있음). 그 다음, 수신된 증명서(177)가 검증되면, FQDN 및/또는 기타 판매자 식별자(167)가 수신된 증명서(177)로부터 추출되고, 상업적 개체 서브시스템(400)의 표(430)에 저장된 임의의 FQDN 및 증명서(177) 연관성과 교차 체크되어 수신된 증명서(177)의 FQDN이 등록되도록 보장할 수 있다. 예를 들어, 단계(616)에서, 상업적 개체 서브시스템(400)은 수신된 챌린지 요청 데이터(664)의 판매자 식별자(167)에 의해 식별된 온라인 리소스(113)가 유효하고 상업적 개체 서브시스템(400)에 등록된 온라인 리소스임을 승인하도록 시도하도록 동작할 수 있는데, 이는 그 판매자 식별자(167)를 표(430) 내에서 식별함으로써(예컨대, 판매자 식별자(167)가 상업적 개체 서브시스템(400)에 (예컨대, 단계(606)에서) 등록되어 있고 이러한 등록이 아직 유효하다고 (예컨대, 상업적 개체 서브시스템(400)이 판매자 식별자(167)를 표(430)에서 제거하거나 또는 의심스럽거나 또는 다른 방식으로 더 이상 신뢰하지 않아서 표(430)에서 플래그 표시된 판매자 식별자(167)를 제거하지 않았음) 결정함) 승인될 수 있다. 유사하게, 제3 판매자-구성에서, 상업적 개체 서브시스템(400)이 단계(614)에서 PSP 서브시스템(310)으로부터 증명서(177)를 구비한 임의의 적합한 챌린지 요청 데이터(664)를 수신하는 것에 응답하여, 상업적 개체 서브시스템(400)은 수신된 챌린지 요청 데이터(664)의 증명서(177)를 검증하고 체크하여 그것의 신뢰성이 여전히 유효하고 만료되지 않았음을 보장하도록 동작할 수 있으며, 수신된 증명서(177)가 검증된 경우, FQDN 및 기타 판매자 식별자(167) 및 PSP 식별자가 수신된 증명서(177)로부터 추출되어 이어서 식별된 PSP가 식별된 판매자 대신에 트랜잭트하도록 인가되었는지 그리고 추출된 FQDN이 상업적 개체 서브시스템(400)의 다른 추출된 판매자 식별자에 등록되었는지 결정되어 단계(614)의 요청을 완전히 확인할 수 있다. 판매자 식별자(167)는 특정 판매자 서브시스템(200)에 대하여 광역 판매자 식별자일 수 있다(예컨대, 단독 판매자 식별자(167)는 원시 앱 판매자 온라인 리소스 및 판매자 서브시스템(200)의 웹사이트 판매자 온라인 리소스를 식별하는 데 사용될 수 있고/있거나 단독 FQDN은 다중 판매자 서브시스템과 연관될 수 있음(예컨대, PSP의 FQDN은 다중 판매자 서브시스템에 의해 사용될 수 있음)). FQDN 및 적어도 하나의 기타 식별자, 예컨대, 특정 판매자 서브시스템(200)의 고유 식별자 및/또는 특정 PSP 서브시스템(310)의 고유 식별자는 둘 모두 증명서(177)에서 추출되고 이 둘은 이미 상업적 개체 서브시스템(400)에서 (예컨대, 표(430) 내에) 서로 연관되어 있음을 승인될 수 있는데, 이는 단계(606)에서 수행되었을 수 있다. 상업적 개체 서브시스템(400)에 의한 수신된 챌린지 요청 데이터(664)의 임의의 적합한 확인 후(예컨대, 수신된 증명서(177)의 검증 및/또는 수신된 증명서(177)의 FQDN의 확인 및/또는 식별된 PSP와 수신된 증명서(177)의 식별된 판매자 간의 인가된 관계의 승인 후), 상업적 개체 서브시스템(400)은 또한, 단계(616)에서, 임의의 적합한 확인 데이터를 생성하고 그 확인 데이터를 수신된 챌린지 요청 데이터(664)의 임의의 적합한 식별자 데이터에 대하여 저장하도록 동작할 수 있다. 예를 들어, 단계(616)에서 수신된 챌린지 요청 데이터(664)의 임의의 적합한 확인 후, 상업적 개체 서브시스템(400)은 또한 단계(616)에서 임의의 적합한 확인 데이터(예컨대, 엔트로피 및/또는 임의의 적합한 암호화 난수를 통한 임의의 적합한 무작위 데이터(예컨대, 위에서 기재한 단계(622)의 확인 데이터와 유사함)) 및 확인 세션 식별자(예컨대, 임의의 적합한 영숫자 스트링 또는 현재 온라인 리소스 확인 세션을 상업적 개체 서브시스템(400)에 대하여 고유하게 식별할 수 있는 임의의 다른 적합한 식별자(예컨대, 이는 디바이스(100)에 의해 단계(612)에서 또는 판매자 서브시스템(200) 또는 PSP 서브시스템(310)에 의해 단계(614)에서 또는 상업적 개체 서브시스템(400)에 의해 단계(616)에서 생성될 수 있음))를 생성하도록 동작할 수 있고, 이어서 상업적 개체 서브시스템(400)은 단계(616)에서 그 확인 데이터를 챌린지 요청 데이터(664)의 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두에 대하여 상업적 개체 서브시스템(400)에 액세스가능한 임의의 적합한 데이터 구조에(예컨대, 표(430)에 또는 다른 방식으로) 저장할 수 있다. 따라서, 소정 실시예들에서, 확인 세션 식별자는 상업적 개체 서브시스템(400)에 의해 생성되어, 상업적 개체 서브시스템(400)이 확인 세션 식별자가 적어도 특정 판매자 식별자에 대하여 상업적 개체 서브시스템(400)에 의해 수행되고 있는 특정 확인 프로세스에 고유함을 보장할 수 있다. 그러나, 판매자 서브시스템(200) 또는 PSP 서브시스템(310)에 의해 확인 세션 식별자가 생성되는 경우, 상업적 개체 서브시스템(400)은 그 확인 세션 식별자가

그 특정 확인 세션에 사용되도록 인에이블하기 전에 이러한 확인 세션 식별자가 확인 세션의 판매자 식별자에 고유한지 승인할 수 있다. 다른 방식으로, 상업적 개체 서브시스템(400)은 확인 세션 식별자를 거부하고 새로운 식별자가 판매자 서브시스템(200) 또는 PSP 서브시스템(310)에 의해 생성되도록 요청할 수 있다. 이러한 저장된 링크 또는 이러한 확인 데이터와 확인 세션의 식별자 데이터(예컨대, 확인 세션 식별자 및/또는 챌린지 요청 데이터(664)의 판매자 식별자) 간의 연관성은 나중에 상업적 개체 서브시스템(400)에 의해 사용되어(예컨대, 단계(630)에서) 수행될 보안 데이터 트랜잭션을 추가로 보호할 수 있다. 또한, 일부 실시예들에서, 챌린지 요청 데이터(664)의 임의의 또는 모든 잠재적 트랜잭션 식별 정보는 단계(616)에서 또한 확인 데이터 및 식별자 데이터에 대하여 저장되거나 또는 다른 방식으로 그것들과 연관될 수 있다.

[0099]

제1, 제2, 및 제3 판매자-구성 중 임의의 구성에서, 이러한 단계(616) 후, 단계들(618, 620, 622)은 생략될 수 있는데, 그 이유는 온라인 리소스가 단계들(614, 616)의 단일 세트에서 확인될 수 있고, 이어서 프로세스(600)가 단계(624)를 포함할 수 있기 때문이며, 이때 상업적 개체 서브시스템(400)은 임의의 적합한 확인 응답 데이터(674)를 생성 및 전달하도록 동작할 수 있다. 예를 들어, 확인 응답 데이터(674)는 단계(616)의 확인 데이터를 임의의 다른 적합한 데이터와 함께 포함할 수 있는 세션 객체일 수 있는데, 임의의 다른 적합한 데이터는, 확인 세션 식별자(예컨대, 단계(616)에서 생성된 확인 세션 식별자), 하나 이상의 판매자 식별자(예컨대, 챌린지 요청 데이터(664)의 임의의 또는 각각의 판매자 식별자(예컨대, FQDN, 기타 판매자 식별자, PSP 식별자 등) 및/또는 상업적 개체 서브시스템(400)에서(예컨대, 표(430) 내에) 확인 세션 동안 확인되어 있는 온라인 리소스와 다른 방식으로 연관될 수 있는 것), 챌린지 요청 데이터(664)의 증명서(177) 등을 포함하지만, 이에 한정되지 않는다. 일부 실시예들에서, 도 6에 도시된 바와 같이, 이러한 확인 응답 데이터(674)는 상업적 개체 서브시스템(400)으로부터 직접 전자 디바이스(100)로(예컨대, 임의의 적합한 통신 프로토콜을 이용하는 통신 경로(65)를 통해) 전달될 수 있는데, 전자 디바이스(100)를 식별하는 데이터(예컨대, 디바이스 식별자(119))는 확인 세션 개시 데이터(662) 및/또는 챌린지 요청 데이터(664) 또는 다른 것과 연관되거나 또는 다른 방식으로 포함되어 상업적 개체 서브시스템(400)이 확인 응답 데이터(674)를 적절한 전자 디바이스(100)에 전달할 수 있도록 할 수 있다. 대안적으로, 일부 실시예들에서(미도시), 확인 응답 데이터(674)는 상업적 개체 서브시스템(400)으로부터 전자 디바이스(100)로 판매자 서브시스템(200)을 통해(예컨대, 제1 또는 제2 판매자-구성에서) 및/또는 PSP 서브시스템(310)을 통해(예컨대, 제3 판매자-구성에서) 전달될 수 있으며, 이로써 판매자 서브시스템(200) 및/또는 PSP 서브시스템(310)은 상업적 개체 서브시스템(400)으로부터 확인 응답 데이터(674)를 수신하고 이어서 확인 응답 데이터(674)의 적어도 일부분을 전자 디바이스(100) 상으로 전달할 수 있다. 확인 응답 데이터(674)의 세션 객체는 상업적 개체 서브시스템(400)에 의해(예컨대, HTTP 헤더에서 또는 다른 방식으로) 또한 전자 디바이스(100)에 액세스가능할 수 있는 상업적 개체 서브시스템(400)과 연관된 액세스 키(예컨대, 보안 요소(145)의 액세스 키(155a), 액세스 키(155b), CRS(151k), 및/또는 ISD 키(156k) 또는 디바이스 애플리케이션(예컨대, 카드 관리 애플리케이션(103b))에 알려질 수 있는 임의의 키)로 서명될 수 있어서, 디바이스(100)는 서명된 확인 데이터를 수신하게 되면 서명을 확인하여 전자 디바이스(100)에 의해 신뢰받을 수 없는 다른 개체 서브시스템이 아닌 상업적 개체 서브시스템(400)이 확인 응답 데이터(674)를 생성했음을 승인하고/하거나 이러한 액세스 키에 대한 액세스가 없는 다른 개체(예컨대, 판매자 서브시스템(200) 및/또는 PSP 서브시스템(310))가 서명된 확인 데이터를 사용하는 것을 방지하면서 그 다른 개체가 이러한 서명된 확인 데이터를 수신하고 디바이스(100)에 전달하도록 인에이블할 수 있다.

[0100]

제1, 제2, 및 제3 판매자-구성 중 임의의 구성에서, 디바이스(100)의 사용자가 단계(610)에서 수신된 잠재적 트랜잭션 데이터(660)(예컨대, 결제 요청 데이터)에 응답하여 잠재적 트랜잭션에 자금을 공급하는 데 사용하기 위한 특정 결제 크리덴셜을 선택 또는 승인을 하려고 하고 또한 할 수 있으며, 확인 응답 데이터(674)(예컨대, 단계들(612 내지 616)의 판매자 온라인 리소스 확인 세션의 성공을 나타낼 수 있는 데이터)가 단계(624)에서 전자 디바이스(100)에 의해 수신된 경우, 프로세스(600)는 단계(625)로 진행할 수 있는데, 단계(625)에서 프로세스(600)는, (예컨대, 단계(625)에서, 위에 언급된) 임의의 세션 식별자 일관성이 식별된 후에, 디바이스(100)의 사용자에게 의해 잠재적 트랜잭션 데이터(660)에 기초하여 (예컨대, 도 3c의 인증 프롬프트(315)의 사용자 선택을 통해) 특정 판매자, 제품, 가격, 및 배송 목적지에 대한 잠재적 트랜잭션을 수행하기 위하여 특정 크리덴셜을 활용하는 의도 및 인증을 수신하는 것을 포함할 수 있다. 일부 실시예들에서, 이러한 의도 및 인증 전에 세션 식별자 일관성이 검증되는 것을 포함하는 단계(625)에 추가적으로 또는 대안적으로, 단계(625)는 이러한 의도 및 인증 전에 도메인 일관성이 검증되는 것을 포함할 수 있다. 예를 들어, 디바이스(100)가 단계(624)에서 확인 응답 데이터(674)를 수신하는 것에 응답하여, 디바이스(100)는 이러한 확인 응답 데이터(674)의 도메인 식별자(예컨대, 확인 응답 데이터(674)의 FQDN)를 현재 디바이스(100)의 온라인 리소스의 주소 막대창에 있는 도메인 식별자와 비교하도록 동작할 수 있다. 예를 들어, 디바이스(100)의 웹 키트(예컨대, 온라인 리소스 애플리

케이션(113))는 확인 응답 데이터(674)를 수신하고 그 확인 응답 데이터(674)를 디바이스(100)의 패스 키트(예컨대, 카드 관리 애플리케이션(103b))에 현재 웹 키트에 의해 타겟팅되고 있는 도메인 식별자(예컨대, FQDN)와 함께 전달할 수 있다. 이어서, 패스 키트는 수신된 확인 응답 데이터(674)의 서명(존재하는 경우)을 (예컨대, 디바이스(100)의 액세스 키를 이용하여) 확인하고, 도메인 식별자(예컨대, FQDN)를 확인 응답 데이터(674)로부터 추출하고, 이어서 그 추출된 도메인 식별자를 웹 키트에 의해 식별되고 그로부터 제공된 도메인 식별자(예컨대, 현재 디바이스(100)의 웹 키트에 의해 호스팅된 자바 스크립트의 FQDN(예컨대, 제1 및 제2 판매자-구성의 판매자 온라인 리소스의 FQDN 및 제3 판매자-구성의 PSP 온라인 리소스의 FQDN))와 비교할 수 있는데, 이는 응답 데이터(674)가 현재 디바이스(100)에 의해 액세스되고 있는 동일한 온라인 리소스와 연관되어 있음을 승인하도록 디바이스(100)를 인에이블할 수 있다(예컨대, 리플레이 공격(replay attack)을 방지하기 위함). 임의의 적합한 세션 식별자 일관성 및/또는 임의의 적합한 도메인 식별자 일관성이 단계(625)에서 검증된 후, 단계(625)에서 특정 결제 크리덴셜에 대한 의도 및 인증이 수신될 수 있다. 이어서, 제1, 제2, 및 제3 판매자-구성의 각각의 구성에 대하여, 단계들(626 내지 629)이 위에 기재한 바와 같이 일어날 수 있는데, 확인 응답 데이터(674)의 임의의 또는 모든 적합한 부분들(예컨대, 세션 식별자, 확인 데이터(예컨대, 난스), FQDN, 및/또는 임의의 다른 적합한 판매자 식별자 또는 PSP 식별자, 및/또는 임의의 기타 데이터(예컨대, 증명서(177)의 적어도 일부분))은 보안 디바이스 데이터(677) 및 트랜잭션 데이터(660)와 함께 디바이스 트랜잭션 데이터(678)로서 포함될 수 있다.

[0101] 제1, 제2, 및 제3 판매자-구성 중 임의의 구성에서, 상업적 개체 서브시스템(400)은 단계(630)에서 디바이스(100)가 디바이스 트랜잭션 데이터(678)에 포함했을 수 있는 확인 응답 데이터(674)의 확인 데이터를 확인하도록 동작할 수 있다. 예를 들어, 이러한 디바이스 트랜잭션 데이터(678)를 수신하는 것에 응답하여, 상업적 개체 서브시스템(400)은 확인 응답 데이터(674)의 적어도 일부분 또는 전부를 그 디바이스 트랜잭션 데이터(678)로부터 식별하고, 단계(630)에서 (예컨대, 프로세스(500)의 단계(516)에 유사하게) 그 수신된 디바이스 트랜잭션 데이터(678)의 확인 데이터가 현재 상업적 개체 서브시스템(400)에 저장되어 있음을 승인하거나, 또는, 더 구체적으로, 일부 실시예들에서, 그 수신된 디바이스 트랜잭션 데이터(678)의 확인 데이터가 현재 상업적 개체 서브시스템(400)에서 수신된 디바이스 트랜잭션 데이터(678)의 확인 세션 식별자 및/또는 수신된 디바이스 트랜잭션 데이터(678)의 판매자 식별자(예컨대, FQDN)에 대하여 (예컨대, 표(430) 내에) 저장되어 있음을 승인하도록 동작할 수 있다. 확인 데이터와 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두 간의 이러한 저장된 링크는 링크가 자동으로 소거되기 전에 제한된 길이의 시간 동안만 유지될 수 있어서, 전자 디바이스(100)는, 그것이 단계(624)에서 확인 응답 데이터(674)를 수신한 뒤, 확인된 판매자 온라인 리소스를 이용하여 특정 보안 데이터 트랜잭션을 수행하기 위하여 상업적 개체 서브시스템(400)에 의해 보호되는 디바이스 트랜잭션 데이터(678)의 보안 디바이스 데이터(677)를 인에이블하기 위하여 단계(628)에서 상업적 개체 서브시스템(400)에 디바이스 트랜잭션 데이터(678)를 송신해야 하는 소정 지속 시간에 제한될 수 있다(예컨대, 상업적 개체 서브시스템(400)은 소정 기간 후에 확인 데이터와 상업적 개체 서브시스템(400)의 확인 세션 식별자 및/또는 판매자 식별자 간의 이러한 연관성을 제거하도록(예컨대, 링크가 생성되고 10 분 이내에 표(430)로부터의 링크를 제거) 동작할 수 있으며, 이는 트랜잭션의 보안을 증가시킬 수 있음). 추가적으로 또는 대안적으로, 확인 데이터와 확인 세션 식별자와 판매자 식별자 중 하나 또는 둘 모두 간의 저장된 링크는 또한, 단계(614)에서 (예컨대, 쉘런지 요청 데이터(664)의 일부로서) 판매자 서브시스템(200) 또는 PSP 서브시스템(310)에 의해 상업적 개체 서브시스템(400)에 이용가능하게 될 수 있는 임의의 적합한 특정 잠재적 트랜잭션 식별 정보, 예컨대, 디바이스(100)와 판매자 서브시스템(200) 또는 PSP 서브시스템(310) 간에 공유될 특정 유형의 보안 데이터의 식별(예컨대, 금융 거래에 대한 통화 및 금액 및 결제 유형, 및 유사한 특정 잠재적 트랜잭션 식별 정보는 또한 단계(628)의 디바이스 트랜잭션 데이터(678)의 일부분으로서 전자 디바이스(100)에 의해 상업적 개체 서브시스템(400)에 이용가능하게 될 수 있음)과 단계(622)에서 연관될 수 있어서, 단계(630)는 또한 상업적 개체 서브시스템(400)이 (예컨대, 단계(616)에서 표(430)에 저장된 것처럼) 단계(614)에서 수신된 확인 데이터에 대하여 현재 저장된 특정 잠재적 트랜잭션 식별 정보가 단계(628)에서 수신된 특정 잠재적 트랜잭션 식별 정보와 적어도 유사하다고 승인하는 것을 포함할 수 있다.

[0102] 그 다음, 단계(631)에서, 프로세스(600)는 상업적 개체 서브시스템(400)이 판매자 서브시스템(200) 또는 PSP 서브시스템(310)(예컨대, 단계(606)에서 확인 세션의 온라인 리소스에 대하여 키들에 대한 제1 CSR을 생성했을 수 있는 서브시스템)과 연관된 판매자 키(예컨대, 판매자 키(157))를 식별하는 것을 포함할 수 있다. 즉, 단계(629)에서 적합한 액세스 정보를 이용하여 디바이스 트랜잭션 데이터(678)의 적어도 일부분을 복호화한 후(예컨대, 보안 디바이스 데이터(677)를 복호화하여 디바이스 결제 크리덴셜 데이터(676) 및 보안 디바이스 데이터(677)에 암호화되었을 수 있는 임의의 기타 정보를 인식한 후), 상업적 개체 서브시스템(400)은 이어서, 단계

(631)에서, 디바이스 트랜잭션 데이터(678)의 적어도 일부분(예컨대, 디바이스 결제 크리덴셜 데이터(676)의 토큰 데이터 및/또는 암호 데이터)을 판매자 서브시스템(200)의 적절한 판매자 키(157)(예컨대, 제1 판매자-구성) 또는 PSP 서브시스템(310)의 적절한 판매자 키(157)(예컨대, 제2 판매자-구성 및 제3 판매자-구성)로 암호화된 판매자 크리덴셜 데이터(681)로서 재암호화할 수 있으며, 그 적절한 판매자 키(157)는 상업적 개체 서브시스템(400)에서 데이터(678)에 포함될 수 있는 확인 데이터의 임의의 적합한 식별자 데이터를 이용하여 그리고 그 식별자 데이터와 연관된 임의의 사전 저장된 연관성(예컨대, 표(430)에, 이는 단계(606) 동안 정의될 수 있음)을 이용하여 식별될 수 있다. 예를 들어, 암호화된 판매자 크리덴셜 데이터(681)는 적어도 디바이스 트랜잭션 데이터(678)로부터의 암호화된 디바이스 결제 크리덴셜 데이터(676)뿐만 아니라 임의의 적합한 트랜잭션 데이터, 예컨대 구매량 데이터 또는 디바이스 트랜잭션 데이터(678) 및/또는 잠재적 트랜잭션 데이터(660)로부터의 또는 이에 기초하는 기타 적합한 트랜잭션 데이터를 포함할 수 있다. 암호화된 판매자 크리덴셜 데이터(681)는, 판매자 서브시스템(200) 또는 PSP 서브시스템(310)에 의해 수신되면, 판매자 서브시스템(200)이 상업적 개체 서브시스템(400)을 이러한 암호화된 판매자 크리덴셜 데이터(681)의 생성자로서 설정할 수 있도록 상업적 개체 서브시스템(400)에 의해 서명될 수 있고/있거나 이러한 암호화된 판매자 크리덴셜 데이터(681)가 서명된 이후에 변경되지 않았음을 보장하도록 그 서브시스템을 인에이블할 수 있다. 이러한 암호화된 판매자 크리덴셜 데이터(681)는 단계(631)에서 생성되고, 단계(632)에서 (예컨대, 상업적 개체 서브시스템(400)의 서버(410)로부터 디바이스(100)의 통신 컴포넌트(106)로 도 1a의 경로(65)를 통해) 안전한 트랜잭션 데이터(682)처럼 임의의 다른 적합한 데이터와 함께 디바이스(100)로 전송될 수 있다.

[0103] 단계들(631, 632)은 상업적 개체 서브시스템(400)으로부터 전송된 크리덴셜 데이터가 도 1a의 안전한 트랜잭션 데이터(682)의 일부(예컨대, 암호화된 판매자 크리덴셜 데이터(681)의 토큰 데이터 및/또는 암호 데이터)로서 보안 요소(145) 이외의 디바이스(100)의 일부분에 의해 복호화될 수 없는 방법으로 암호화될 수 있도록 보장하도록 동작할 수 있다. 즉, 안전한 트랜잭션 데이터(682)의 크리덴셜 데이터(예컨대, 암호화된 판매자 크리덴셜 데이터(681)의 토큰 데이터 및/또는 암호 데이터)는 디바이스(100)의 어떠한 부분에도, 예컨대, 일부 실시예들에서, 보안 요소(145)에도 노출되거나 또는 다른 방식으로 액세스 불가능한 판매자 키(예컨대, 판매자 키(157))를 이용하여 암호화될 수 있다. 또한, 안전한 트랜잭션 데이터(682)의 크리덴셜 데이터(예컨대, 암호화된 판매자 크리덴셜 데이터(681)의 토큰 데이터 및/또는 암호 데이터)는 보안 요소(145) 밖에 있는 디바이스(100)의 어떠한 부분에도 노출되거나 또는 다른 방식으로 액세스 불가능한 크리덴셜 키(155a')를 이용하여 암호화될 수 있다.

[0104] 제1 및 제2 판매자-구성에서, 안전한 트랜잭션 데이터(682)는 이어서 단계(634)에서 디바이스(100)에 의해 판매자 서브시스템(200)으로 안전한 트랜잭션 데이터(684)로서 (예컨대, 통신 경로(15)를 통해 또는 비접촉식 근접성 기반 통신(5)으로서) 전달될 수 있거나, 또는, 대안적으로, 판매자 크리덴셜 데이터(681)는 디바이스(100)(미도시)를 통해 전달되지 않고 상업적 개체 서브시스템(400)으로부터 판매자 서브시스템(200)으로 전달될 수 있다. 잠재적 트랜잭션 데이터(660)의 하나, 일부, 또는 모든 부분들은 디바이스(100) 및/또는 상업적 개체 서브시스템(400)을 통해 안전한 트랜잭션 데이터(682) 및/또는 안전한 트랜잭션 데이터(684)로 전달될 수 있어서, 잠재적 트랜잭션의 소정의 식별자들은 프로세스(600) 동안 개체들의 각각에 의해 식별될 수 있다.

[0105] 결제 크리덴셜 데이터(675/676)를 포함하는 판매자 크리덴셜 데이터(681)가 판매자 서브시스템(200)에 의해 (예컨대, 안전한 트랜잭션 데이터(684)로서 단계(634)에서) 수신되면, 프로세스(600)는 또한 판매자 서브시스템(200)이 결제 데이터(686)를 생성 및 전송하도록 구성될 수 있는 단계(636)를 포함할 수 있다. 제1 판매자-구성에서, 예를 들어, 단계(636)에서, 판매자 서브시스템(200)은 그것의 알려진 판매자 키(157)를 이용하여 적어도 부분적으로 안전한 트랜잭션 데이터(684)의 판매자 크리덴셜 데이터(681)를 복호화할 수 있으며, 결제 데이터(686)는 크리덴셜 SSD(154a)의 안전한 결제 크리덴셜 데이터를 포함할 수 있는데, 결제 크리덴셜 데이터는 그것의 크리덴셜 키(155a')(예컨대, 데이터(676))로 암호화되지만 금융 기관 서브시스템(350)에 이용불가능한 키로 암호화되지 않고, 이어서 이러한 데이터(686)는 판매자 서브시스템(200)에 의해 임의의 적합한 서브시스템(예컨대, 매수 은행 서브시스템(300) 및/또는 PSP 서브시스템(310))으로 전달될 수 있다. 대안적으로, 제2 판매자-구성에서, 예를 들어, 단계(636)에서, 판매자 서브시스템(200)은 안전한 트랜잭션 데이터(684)의 재암호화된 판매자 크리덴셜 데이터(681)를 PSP 서브시스템(310)으로 결제 데이터(686)로서 전달할 수 있고, 이어서 PSP 서브시스템(310)은 그것의 알려진 판매자 키(157)를 이용하여 적어도 부분적으로 결제 데이터(686)의 그 재암호화된 판매자 크리덴셜 데이터(681)를 복호화할 수 있다. 대안적으로, 제3 판매자-구성에서, 안전한 트랜잭션 데이터(682)는 디바이스(100)에 의해 PSP 서브시스템(310)으로 (예컨대, 현재 디바이스(100)에 의해 액세스될 수 있는 PSP 온라인 리소스를 이용하여) 전달될 수 있고, 이어서 PSP 서브시스템(310)은 그것의 알려진 판매자 키(157)를 이용하여 적어도 부분적으로 그 전달된 안전한 트랜잭션 데이터의 재암호화된 판매자 크리덴셜 데이

터(681)를 복호화할 수 있다. 프로세스(600)의 남은 과정은 위에 기재한 바와 같이 단계들(638 내지 644)에 대하여 진행할 수 있으며, 판매자 서브시스템(200) 및 PSP 서브시스템(310) 중 적절한 것(들)이 데이터를 디바이스(100)와 응용가능한 판매자-구성에 따라 교환한다.

[0106] 도 7의 설명

[0107] 도 7은 관리 개체 서브시스템을 이용하여 프로세싱 서브시스템과 전자 디바이스 상에서 실행되는 온라인 리소스를 통해 프로세싱 서브시스템에 통신가능하게 결합된 전자 디바이스 간의 보안 트랜잭션을 수행하기 위한 프로세스(700)를 도시하는 흐름도이다. 프로세스(700)의 단계(702)에서, 관리 개체 서브시스템은 온라인 리소스에 대한 확인 요청을 수신할 수 있으며, 확인 요청은 확인 요청 데이터를 포함할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(614)에서 챌린지 요청 데이터(664)를 수신할 수 있고/있거나 단계(620)에서 챌린지 응답 데이터(670)를 수신할 수 있음). 프로세스(700)의 단계(704)에서, 관리 개체 서브시스템은 확인 요청 데이터 및 등록 데이터를 이용하여 온라인 리소스를 확인할 수 있고, 등록 데이터는 확인 요청을 수신하기 전에 초기에 관리 개체 서브시스템에 이용가능하게 될 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(616)에서 챌린지 요청 데이터(664) 및 단계(606)로부터의 등록 데이터를 이용하여 및/또는 프로세스(600)의 단계(622)에서 챌린지 응답 데이터(670) 및 단계(606)로부터의 등록 데이터를 이용하여 온라인 리소스(113)를 확인할 수 있음). 프로세스(700)의 단계(706)에서, 관리 개체 서브시스템은 확인 응답 데이터를 확인 요청 데이터의 적어도 일부분과 연관시킬 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(616)에서 및/또는 단계(622)에서 확인 데이터를 식별자 데이터에 대하여 연관시킬 수 있음). 프로세스(700)의 단계(708)에서, 관리 개체 서브시스템은 확인 응답 데이터를 전자 디바이스에 전달할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(624)에서 확인 데이터를 확인 응답 데이터(674)의 일부분으로서 전자 디바이스(100)에 전달할 수 있음). 프로세스(700)의 단계(710)에서, 관리 개체 서브시스템은 전자 디바이스로부터 디바이스 트랜잭션 데이터를 수신할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(628)에서 전자 디바이스(100)로부터 디바이스 트랜잭션 데이터(678)를 수신할 수 있음). 프로세스(700)의 단계(712)에서, 관리 개체 서브시스템은 확인 응답 데이터를 이용하여 디바이스 트랜잭션 데이터를 확인할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(630)에서 확인 응답 데이터(674)를 이용하여 디바이스 트랜잭션 데이터(678)의 확인 데이터를 확인할 수 있음). 프로세스(700)의 단계(714)에서, 디바이스 트랜잭션 데이터가 확인된 후, 관리 개체 서브시스템은 프로세싱 서브시스템에 의한 사용을 위하여 디바이스 트랜잭션 데이터 상에 기초하여 보안 트랜잭션 데이터를 생성할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(631)에서 디바이스 트랜잭션 데이터(678)에 기초하여 판매자 크리덴셜 데이터(681)를 생성할 수 있음).

[0108] 도 7의 프로세스(700)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 추가적인 단계들이 추가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다.

[0109] 도 8의 설명

[0110] 도 8은 관리 개체 서브시스템을 이용하여 프로세싱 서브시스템과 전자 디바이스 상에서 실행되는 온라인 리소스를 통해 프로세싱 서브시스템에 통신가능하게 결합된 전자 디바이스 간의 보안 트랜잭션을 인에이블하기 위한 도시화된 프로세스(800)의 흐름도이다. 프로세스(800)의 단계(802)에서, 관리 개체 서브시스템과 프로세싱 서브시스템 간의 프로세싱 공유 비밀을 설정함으로써 온라인 리소스를 등록할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(606)에서 판매자 서브시스템(200)과 공유 비밀을 설정함으로써 온라인 리소스(113)를 등록할 수 있음). 프로세스(800)의 단계(804)에서, 관리 개체 서브시스템은 온라인 리소스에 대한 확인 요청을 수신할 수 있는데, 확인 요청은 온라인 리소스를 나타내는 프로세싱 식별자를 포함할 수 있고, 확인 요청은 온라인 리소스를 통하여 전자 디바이스와 프로세싱 서브시스템 간의 잠재적 트랜잭션에 고유한 확인 세션 식별자를 추가로 포함할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 단계(614)에서 챌린지 요청 데이터(664)를 판매자 식별자 및 세션 식별자와 함께 수신하고/하거나 프로세스(600)의 단계(620)에서 챌린지 응답 데이터(670)를 판매자 식별자 및 세션 식별자와 함께 수신할 수 있음). 프로세스(800)의 단계(806)에서, 관리 개체 서브시스템은 프로세싱 식별자에 의해 표시된 온라인 리소스를 확인 세션 식별자 및 프로세싱 공유 비밀을 이용하여 확인할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(616)에서 챌린지 요청 데이터(664) 및 단계(606)로부터의 등록 데이터를 이용하여 온라인 리소스(113)를 확인할 수 있고/있거나 프로세스(600)의 단계(622)에서 챌린지 응답 데이터(670) 및 단계(606)로부터의 등록 데이터를 이용하여 온라인 리소스(113)를 확인할 수 있음).

[0111] 도 8의 프로세스(800)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 추가적인 단계들이 추가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다.

[0112] 도 9의 설명

[0113] 도 9는 관리 개체 서브시스템을 이용하여 프로세싱 서브시스템과 전자 디바이스 상에서 실행되는 온라인 리소스를 통해 프로세싱 서브시스템에 통신가능하게 결합된 전자 디바이스 간의 보안 트랜잭션을 수행하기 위한 도시화된 프로세스(900)의 흐름도이다. 프로세스(900)의 단계(902)에서, 관리 개체 서브시스템은 온라인 리소스에 대한 확인 요청을 수신할 수 있고, 확인 요청은 확인 요청 데이터를 포함할 수 있고, 확인 요청 데이터는 온라인 리소스를 통하여 전자 디바이스와 프로세싱 서브시스템 간의 잠재적 트랜잭션을 나타내는 잠재적 트랜잭션 식별 정보를 포함할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(614)에서 챌린지 요청 데이터(664)를 수신하고/하거나 단계(620)에서 챌린지 응답 데이터(670)를 수신할 수 있음). 프로세스(900)의 단계(904)에서, 관리 개체 서브시스템은 확인 요청 데이터의 적어도 일부분을 이용하여 온라인 리소스를 확인할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(616)에서 챌린지 요청 데이터(664)를 이용하여 온라인 리소스(113)를 확인하고/하거나 프로세스(600)의 단계(622)에서 챌린지 응답 데이터(670)를 이용하여 온라인 리소스(113)를 확인할 수 있음). 프로세스(900)의 단계(906)에서, 관리 개체 서브시스템은 확인 응답 데이터를 적어도 잠재적 트랜잭션 식별 정보와 연관시킬 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(616)에서 및/또는 단계(622)에서 확인 데이터를 잠재적 트랜잭션 식별 정보와 연관시킬 수 있음). 프로세스(900)의 단계(908)에서, 관리 개체 서브시스템은 확인 응답 데이터를 전자 디바이스에 전달할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(624)에서 확인 데이터를 확인 응답 데이터(674)의 일부분으로서 전자 디바이스(100)에 전달할 수 있음). 프로세스(900)의 단계(910)에서, 관리 개체 서브시스템은 전자 디바이스로부터 디바이스 트랜잭션 데이터를 수신할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(628)에서 전자 디바이스(100)로부터 디바이스 트랜잭션 데이터(678)를 수신할 수 있음). 프로세스(900)의 단계(912)에서, 관리 개체 서브시스템은 확인 응답 데이터 및 잠재적 트랜잭션 식별 정보를 이용하여 디바이스 트랜잭션 데이터를 확인할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(630)에서 확인 응답 데이터(674) 및 잠재적 트랜잭션 식별 정보를 이용하여 디바이스 트랜잭션 데이터(678)의 확인 데이터를 확인할 수 있음). 프로세스(900)의 단계(914)에서, 디바이스 트랜잭션 데이터가 확인된 후, 관리 개체 서브시스템은 프로세싱 서브시스템에 의한 사용을 위하여 디바이스 트랜잭션 데이터 상에 기초하여 보안 트랜잭션 데이터를 생성할 수 있다(예컨대, 상업적 개체 서브시스템(400)은 프로세스(600)의 단계(631)에서 디바이스 트랜잭션 데이터(678)에 기초하여 판매자 크리덴셜 데이터(681)를 생성할 수 있음).

[0114] 도 9의 프로세스(900)에 나타난 단계들은 단지 예시적인 것이고, 기존의 단계들은 수정되거나 또는 생략될 수 있고, 추가적인 단계들이 추가될 수 있으며, 소정 단계들의 순서가 변경될 수 있다는 것이 이해된다.

[0115] 실시예의 추가 설명

[0116] 디바이스(100)의 보안 요소의 크리덴셜이 트랜잭션 데이터의 결제 크리덴셜 데이터로서(예컨대, 판매자 단말기(220)에 대한 비접촉식 근접성 기반 통신으로서 및/또는 판매자 서버(210)에 대한 온라인-기반 통신으로서) 제공될 있도록 적절하게 인에이블되면(예컨대, 크리덴셜 SSD(154a)의 인에이블된 애플릿(153a)과 연관된 상거래 크리덴셜 데이터), 매수 은행 서브시스템(300)은 금융 기관 서브시스템(350)과의 금융 거래를 완료하기 위하여 이러한 결제 크리덴셜 데이터를 활용할 수 있다. 예를 들어, 디바이스(100)의 사용자가 구매할 제품을 선택하고 적절하게 디바이스(100)의 특정 크리덴셜이 결제에 사용되도록 인에이블한 후, 판매자 서브시스템(200)은 특정 크리덴셜에 대한 결제 크리덴셜 데이터를 나타내는 결제 크리덴셜 데이터를 수신할 수 있다. 판매자 서버(210) 및/또는 판매자 단말기(220)는 디바이스(100)가 결제 크리덴셜 데이터를 제공하는 것에 응답하여 제품 또는 서비스를 최종 사용자 전자 디바이스의 사용자에게 제공할 수 있는 임의의 적합한 판매자 또는 판매자 서브시스템(200)의 판매자 에이전트에 의해 제공될 수 있다. 이러한 수신된 결제 크리덴셜 데이터(예컨대, 데이터(684)와 같음)에 기초하여, 판매자 서브시스템(200)은 데이터(686)를 생성하여(예컨대, 판매자 서브시스템(200)과 매수 은행 서브시스템(300) 간 통신 경로(25)를 통해) 매수 은행 서브시스템(300)으로 전송하도록 구성될 수 있고, 데이터(686)는 디바이스 결제 크리덴셜을 나타낼 수 있는 결제 크리덴셜 데이터 및 인가 요청 및 제품 또는 서비스에 대한 판매자의 구매 가격을 포함할 수 있다. 또한 결제 프로세서 또는 매수자로 알려진, 매수 은행 서브시스템(300)은 판매자 서브시스템(200)과 연관된 판매자의 बैंकिंग 파트너일 수 있고, 매수 은행 서브시스템(300)은 금융 기관 서브시스템(350)과 협력하여 결제 디바이스(100)에 의해 자금이 공급되도록 시도되는 크리덴셜 트랜잭션들을 결제 크리덴셜 데이터를 이용하여 승인 및 해결하도록 구성될 수 있다. 매수 은행

서브시스템(300)은 이어서 인가 요청을 결제 데이터(686)로부터 금융 기관 서브시스템(350)으로 인가 요청 데이터(688)로서 (예컨대, 매수 은행 서브시스템(300)과 금융 기관 서브시스템(350) 간 통신 경로(35)를 통해) 전달할 수 있다.

[0117] 결제 네트워크 서브시스템(360) 및 발행 은행 서브시스템(370)은 단일 개체 또는 별개의 개체들일 수 있다. 예를 들어, 아메리칸 익스프레스(American Express)는 결제 네트워크 서브시스템(360) 및 발행 은행 서브시스템(370) 둘 다일 수 있다. 그에 반해, 비자(Visa) 및 마스터카드(MasterCard)는 결제 네트워크(360)일 수 있고, 체이스(Chase), 웰스 파고(Wells Fargo), بانک 오브 아메리카(Bank of America) 등과 같은 발행 은행(370)과 협력하여 동작할 수 있다. 금융 기관 서브시스템(350)은 또한 매수 은행 서브시스템(300)과 같은 하나 이상의 매수 은행을 포함할 수 있다. 예를 들어, 매수 은행 서브시스템(300)은 발행 은행 서브시스템(370)과 동일한 개체일 수 있다. 매수 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 별개의 개체들인 경우에, 결제 네트워크 서브시스템(360)은 데이터(690)를 매수 은행 서브시스템(300)으로부터 수신할 수 있고, 이어서 요청을 발행 은행 서브시스템(370)에 데이터(405)로서 (예컨대, 결제 네트워크 서브시스템(360)과 발행 은행 서브시스템(370) 간 통신 경로(45)를 통해) 전달할 수 있다. 결제 네트워크 서브시스템(360)과 발행 은행 서브시스템(370)이 동일한 개체인 경우에, 매수 은행 서브시스템(300)은 데이터(690)를 직접 발행 은행 서브시스템(370)에 제출할 수 있다. 또한, 결제 네트워크 서브시스템(360)은 발행 은행 서브시스템(370) 대신에 매수 은행 서브시스템(300)에 (예컨대, 결제 네트워크 서브시스템(360)과 발행 은행 서브시스템(370) 간에 합의된 조건에 따라) 응답할 수 있다. 매수 은행 서브시스템(300)과 발행 은행 서브시스템(370) 간에 교류함으로써, 결제 네트워크 서브시스템(360)은 각각의 매수 은행 서브시스템(300) 및 각각의 발행 은행 서브시스템(370)이 직접 상호작용해야만 하는 개체들의 수를 줄일 수 있다. 즉, 금융 기관 서브시스템(350)의 직접 통합 지점들을 최소화하기 위하여, 결제 네트워크 서브시스템(360)은 다양한 발행 은행들(370) 및/또는 다양한 매수 은행들(300)에 대하여 집합자의 역할을 할 수 있다. 금융 기관 서브시스템(350)은 또한 매수 은행 서브시스템(300)과 같은 하나 이상의 매수 은행을 포함할 수 있다. 예를 들어, 매수 은행 서브시스템(300)은 발행 은행 서브시스템(370)과 동일한 개체일 수 있다.

[0118] 발행 은행 서브시스템(370)이 인가 요청을 (예컨대, 매수 은행 서브시스템(300)으로부터 데이터(688)로서 직접 또는 결제 네트워크 서브시스템(360)을 통해 데이터(405)로서 간접적으로) 수신하면, 결제 정보(예컨대, 디바이스(100)의 상거래 크리덴셜 정보) 및 인가 요청에 포함된 구매량이 분석되어 상거래 크리덴셜과 연관된 계좌에 구매량을 커버할 만큼 충분한 크레딧이 있는지 결정할 수 있다. 충분한 자금이 없는 경우, 발행 은행 서브시스템(370)은 부정적인 인가 응답을 매수 은행 서브시스템(300)에 전송함으로써 요청된 트랜잭션을 거절할 수 있다. 그러나, 충분한 자금이 존재하는 경우, 발행 은행 서브시스템(370)은 긍정적인 인가 응답을 매수 은행 서브시스템(300)에 전송함으로써 요청된 트랜잭션을 승인할 수 있고, 금융 거래는 완료될 수 있다. 두 유형의 인가 응답이 사용자 금융 서브시스템(350)에 의해 매수 은행 서브시스템(300)으로 인가 응답 데이터 또는 트랜잭션 상태 데이터(690)로서 제공될 수 있다(예컨대, 트랜잭션 상태 데이터(690)는 발행 은행 서브시스템(370)으로부터 매수 은행 서브시스템(300)으로 통신 경로(35)를 통해 직접 제공될 수 있거나, 또는 트랜잭션 상태 데이터(690)는 발행 은행 서브시스템(370)으로부터 통신 경로(45)를 통해 결제 네트워크 서브시스템(360)에 제공될 수 있는 인가 응답 데이터 또는 트랜잭션 상태 데이터(415)에 기초하여 결제 네트워크 서브시스템(360)으로부터 매수 은행 서브시스템(300)으로 제공될 수 있음).

[0119] 언급한 바와 같이, 그리고 도 2에 도시된 바와 같이, 전자 디바이스(100)는, 음악 재생기(예컨대, 미국 캘리포니아주 쿠퍼티노 소재의 애플 사에 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 레코

터, 라디오, 의료 장비, 상업용 제품, 운송 차량 기구, 악기, 계산기, 셀룰러 전화기(예컨대, 애플 사에 의해 입수가능한 아이폰™), 기타 무선 통신 디바이스, 개인 휴대 단말기, 리모콘, 무선 호출기, 컴퓨터(예컨대, 데스크톱, 랩톱, 태블릿(예컨대, 애플 사에 의해 입수가능한 아이패드™), 서버 등), 모니터, 텔레비전, 스테레오 장치, 셋업 박스(set up box), 셋톱 박스(set-top box), 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, 보안 데이터 트랜잭션을 수행하는 것에 전용되는 디바이스), 다른 실시예들에서, 전자 디바이스(100)는 다수의 기능을 수행할 수 있다(예컨대, 보안 데이터 트랜잭션을 수행하고, 음악을 재생하고, 전화 통화를 수신 및 전송하는 디바이스). 전자 디바이스(100)는 사용자가 어디로 이동하든지 금융 거래를 수행하도록 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 인크의 애플 워치(Apple Watch™)), 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, 전자 디바이스(100)는 전혀 휴대용이 아닐 수 있고, 대신에 대체로 고정형일 수 있다.

[0120] 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. 게다가, 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.

[0121] 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 저장하기 위해 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 식별 모듈("SIM") 카드 또는 시큐어 디지털("SD") 메모리 카드) 상에 통합될 수 있다. 메모리(104)는 미디어 데이터(예컨대, 음악 및 이미지 파일), (예를 들어, 디바이스(100) 상에서 기능들을 구현하기 위한) 소프트웨어, 펌웨어, 신호도 정보(예컨대, 미디어 재생 신호도), 생활방식 정보(예컨대, 음식 신호도), 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.

[0122] 통신 컴포넌트(106)는, 디바이스(100)가 임의의 적합한 통신 프로토콜을 이용하여 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 전화기 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 액세스리 디바이스)에 통신가능하게 연결되고 무선으로 또는 유선 접속을 통해(예를 들어, 커넥터 포트를 이용하여) 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 기타 적합한 개체에(예컨대, 임의의 적합한 인터넷 접속에) 전달하도록 동작할 때 온라인 통신 컴포넌트라고 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 이용할 수 있다.

[0123] 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(예를 들어, 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(예를 들어, 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, 리튬이온 배터리, 또는 납축전지), 무정전 또는 연속적 전원 공급장치(uninterruptible 또는 continuous power supply, "UPS" 또는 "CPS"), 및 전력 생성원으로부터 수신된 전력(예컨대, 전력 발전소에서 생성되고, 전기 소켓을 통해 또는 다른 식으로 사용자에게 전달되는 전력)을 처리하기 위한 회로 중 하나 이상을 포함할 수 있다. 전력은 전원 공급장치(108)에 의해 교류 또는 직류로서 제공될 수 있으며, 전력을 변환하거나 수신된 전력을 특정한 특성들로 제한하도록 처리될 수 있다. 예를 들어, 전력은 직류로 또는 직류로부터 변환되고, 평균 전력, 유효 전력, 피크 전력, 펄스당 에너지, 전압, (예를 들어, 암페어로 측정되는) 전류, 또는 수신된 전력의 임의의 다른 특성 중 하나 이상의 값으로 제한될 수 있다. 전원 공급장치(108)는, (예를 들어, 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.

[0124] 하나 이상의 입력 컴포넌트(110)는, 사용자가 디바이스(100)와 상호작용하거나 그와 인터페이스하는 것을 허용하기 위해 제공될 수 있다. 예를 들어, 입력 컴포넌트(110)는 터치 패드, 다이얼, 클릭 휠, 스크롤 휠, 터치 스크린, 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-처리 애플리케이션과 연계하여 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.

[0125] 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.

[0126] 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, 콤팩트 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 관한 정보, 디바이스 동작 스크린들 등)를 디스플레이하도록 동작할 수 있다.

[0127] 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.

[0128] 전자 디바이스(100)의 프로세서(102)는 전자 디바이스(100)의 하나 이상의 컴포넌트의 동작들 및 성능을 제어하도록 동작할 수 있는 임의의 처리 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-처리 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 방법을 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(예를 들어, 버스(118)를 통해) 또는 다른 디바이스 또는 서버로부터(예를 들어, 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.

[0129] 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) 사이에서 비접촉식 근접성 기반 거래들 또는 통신들(15)을 가능하게 할 수 있는 임의의 적합한 근접성 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 추가적으로, 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)와 판매자 서브시스템(200) 사이의 통신은 NFC 컴포넌트와 판매자 서브시스템(200) 사이의 임의의 적합한 가까운 범위의 거리(예컨대, 도 1 및 도 1a의 NFC 컴포넌트(120)와 판매자 결제 단말기(220) 간의 거리(D)를 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. 이러한 NFC 컴포넌트는 상품 정보를 획득하고, 결제 정보를 전송하고, 외부 디바이스(예컨대, NFC 컴포넌트(120)와 판매자 단말기(220) 간의 통신)와 다른 식으로 통신하는 방식을 제공할 수 있다.

[0130] NFC 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200) 사이에서 비접촉식 근접성 기반 통신을 가능하게 하기 위한 임의의 적합한 모듈들을 포함할 수 있다. 도 2에 도시된 바와 같이, 예를 들어, NFC 컴포넌

트(120)는 NFC 디바이스 모듈(130), NFC 제어기 모듈(140), 및 NFC 메모리 모듈(150)을 포함할 수 있다.

[0131] 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 근접성 기반 또는 NFC 통신(5)의 일부로서 전송될 수 있는 임의의 적합한 데이터를 포함하거나, 라우팅하거나, 또는 달리 제공하도록 구성될 수 있다. 추가적으로 또는 대안적으로, NFC 데이터 모듈(132)은, 비접촉식 근접성 기반 통신(예컨대, NFC 컴포넌트(120)와 판매자 단말기(220) 간의 통신(5))의 일부로서 판매자 서브시스템(200)으로부터 NFC 컴포넌트(120)에 의해 수신될 수 있는 임의의 적합한 데이터를 포함하거나, 라우팅하거나, 또는 달리 수신하도록 구성될 수 있다.

[0132] 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 근접성 기반 통신 기능들을 가능하게 하기 위해 제공될 수 있다.

[0133] 대안적으로 또는 추가적으로, NFC 컴포넌트(120)는, 전자 디바이스(100)의 다른 통신 컴포넌트(예컨대, 통신 컴포넌트(106))가 이용할 수 있는 동일한 송수신기 회로 또는 안테나(예컨대, 안테나(116))를 이용할 수 있다. 예를 들어, 통신 컴포넌트(106)가 안테나(116)를 이용하여 전자 디바이스(100)와 다른 원격 개체 사이의 Wi-Fi, 블루투스™, 셀룰러, 또는 GPS 통신을 가능하게 할 수 있는 한편, NFC 컴포넌트(120)는 안테나(116)를 이용하여 NFC 디바이스 모듈(130)의 NFC 데이터 모듈(132)과 다른 개체(예컨대, 판매자 서브시스템(200)) 사이의 비접촉식 근접성 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 전송되도록 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 근접성 기반 또는 NFC 통신을 전달하기 위해 적절히 인에이블될 수 있기 전에, 부스터(136)로부터의 증폭을 요구할 수 있다(예를 들어, 안테나(116)를 이용해 다른 유형들의 데이터를 전송하기 위해 필요할 수 있는 것보다, 안테나(116)를 이용해 NFC 데이터를 전송하기 위해 필요할 수 있는 전력이 더 클 수 있음).

[0134] NFC 제어기 모듈(140)은 적어도 하나의 NFC 프로세서 모듈(142)을 포함할 수 있다. NFC 프로세서 모듈(142)은 NFC 디바이스 모듈(130)과 연계하여 동작하여, 전자 디바이스(100)와 판매자 서브시스템(200) 사이에서 NFC 통신을 전달하기 위한 NFC 컴포넌트(120)를 인에이블하고, 활성화하고, 허용하고, 그리고/또는 달리 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 제어기 모듈(140)의 NFC 프로세서 모듈(142)은, NFC 컴포넌트(120)의 기능을 지시하는 데 도움을 줄 수 있는, NFC 저전력 모드 또는 지갑 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 제어기 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 디바이스(initiator device)로서 지정하는 데 사용될 수 있다.

[0135] NFC 제어기 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 인에이블된 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 제어기 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 연계하여) 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) 상에서 실행중인 애플리케이션(예컨대, 애플리케이션(103) 및/또는 애플리케이션(143))에 의해 정의되거나 달리 지시될 수 있다.

[0136] NFC 메모리 모듈(150)은 NFC 디바이스 모듈(130) 및/또는 NFC 제어기 모듈(140)과 연계하여 동작하여, 전자 디바이스(100)와 판매자 서브시스템(200) 간의 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 부정조작 방지일 수 있고 보안 요소의 적어도 일부분을 제공할 수 있다. 예를 들어, NFC 메모리 모듈(150)은 NFC 제어기 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 제어기 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 제어기 모듈(140) 및 NFC 메모리 모듈(150)은 독립적으로 또는 조합하여, 부정조작 방지일 수 있는 보안 요소(145)의 적어도 일부분을 제공할 수 있다. 예를 들어, 이러한 보안 요소(145)는 잘 식별된 신뢰 기관들(예컨대, 글로벌플랫폼과 같은 금융 기관 서브시스템 및/또는 산업 표준의 기관)의 세트에 의해 제시될 수 있는 규칙 및 보안 요구조건에 따라 애플리케이션들 및 그것들의 비밀 및 암호 데이터(예컨대, 애플릿(153) 및 키(155))를 안전하게 호스팅할 수 있는(예컨대, 싱글칩 또는 멀티칩 보안 마이크로제어기와 같은) 부정조작 방지 플랫폼을 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 제어기 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 칩 내의 매우 안전한, 부정조작 방지 하드웨어 컴포넌트일 수 있으며, 민감한 데이터 또는 애플리케이션들을 전자 디바이스(100) 상에 저장하는 데 사용될 수 있다. 보안 요소(145)의 적어도 일부분은 착탈식 회로 카드, 예컨대, UICC(universal integrated circuit card) 또는 SIM(subscriber identity module) 카드에 제공되어, GSM(global system for mobile communications) 네트워크들, UMTS(universal mobile telecommunications systems) 및/또는 LTE(long-term evolution) 표준 네트워크들과 호환되는 전자 디바이스들(100)에 사용될 수 있다. 대안적으로 또는 추가적으로, 보안 요소(145)의 적어도 일부분 디바이스(100)의 제조시 전자 디바이스(100)에 내장될 수 있는 집적 회로에 제공될 수 있다. 대안적으로 또는 추가적으로, 보안 요소(145)의 적어도 일부분은 전자 디바이스(100)에 꽂거나, 삽입되거나, 또는 다른 방식으로 연결될 수 있는 주변 기기, 예컨대, 마이크로 SD(micro secure digital) 메모리 카드에 제공될 수 있다.

[0137] 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 개체 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 통화(예컨대, 비트코인 및 연관된 결제 네트워크) 등과 연관된 상업적 크리덴셜들)을 생성하거나 다른 식으로 전자 디바이스(100) 상에 발급하기 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 특정 특권 또는 결제 권한을 전자 디바이스(100)에 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 대하여 TSM일 수 있고, 제1 SSD(154a)의 애플릿(153a)은 제1 결제 네트워크 서브시스템(360)에 의해 관리되는 상거래 크리덴셜과 연관될 수 있는 반면, 제2 결제 네트워크 서브시스템(360)(예컨대, 마스터카드)은 다른 SSD(154)에 대한 TSM일 수 있다.

[0138] NFC 컴포넌트(120)의 사용을 인에이블하기 위한(예컨대, 디바이스(100) 상에 발급된 상거래 크리덴셜들의 활성화 인에이블하기 위한) 보안 특징들이 제공될 수 있으며, 이는 크리덴셜의 신용 카드 정보 또는 은행 계좌 정보와 같은 기밀 결제 정보를 전자 디바이스(100)로부터 판매자 서브시스템(200)으로 전송할 때 특히 유용할 수

있다. 그러한 보안 특징들은 또한 제한된 액세스를 가질 수 있는 보안 저장 영역을 포함할 수 있다. 예를 들어, 개인 식별 번호("PIN") 입력을 통한, 또는 생체인식 센서와의 사용자 상호작용을 통한 사용자 인증이, (예컨대, 사용자가 보안 요소의 보안 도메인 요소의 수명 주기 상태를 변경하기 위하여) 보안 저장 영역에 액세스하기 위해 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 마이크로제어기를 포함할 수 있다.

[0139] 도 1a의 판매자 서브시스템(200)의 판매자 단말기(220)는 전자 디바이스(100)로부터 NFC 통신(예컨대, 디바이스(100)가 판매자 단말기(220)의 소정 거리 또는 근접성 내에 들게 될 때의 통신(5))을 검출, 판독, 또는 다른 방식으로 수신하기 위한 판독기를 포함할 수 있다. 따라서, 이러한 판매자 단말기와 전자 디바이스(100) 간의 NFC 통신이 무선으로 일어날 수 있으며, 그와 같이, 각각의 디바이스들 사이에 분명한(clear) "가시선(line of sight)"을 요구하지 않을 수 있다는 것에 주의한다. 언급된 바와 같이, NFC 디바이스 모듈(130)은 수동 또는 능동일 수 있다. 수동인 경우, NFC 디바이스 모듈(130)은 이러한 판매자 단말기의 적합한 판독기의 응답 범위 내에 있을 때에만 활성화될 수 있다. 예를 들어, 이러한 판매자 단말기의 판독기는 비교적 저전력의 전파장(radio wave field)을 방출할 수 있으며, 이는 NFC 디바이스 모듈(130)에 의해 이용되는 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, 이러한 판매자 단말기로 NFC 통신으로서 전송하게 할 수 있다. 능동인 경우, NFC 디바이스 모듈(130)은 전자 디바이스(100)에 로컬인 전원(예컨대, 전원 공급장치(108))을 포함하거나 다른 식으로 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 전송하게 할 수 있다. 판매자 단말기(220)는 판매자 서브시스템(200)의 판매자에 의해(예컨대, 제품 또는 서비스를 직접 디바이스(100)의 사용자에게 매장에서 판매하기 위한 판매자의 매장에서) 제공될 수 있다. NFC 컴포넌트(120)는 근거리 통신에 관하여 기술되었지만, 컴포넌트(120)는 임의의 적합한 비접촉식 근접성 기반 모바일 결제 또는 전자 디바이스(100)와 이러한 판매자 단말기 간의 임의의 다른 적합한 유형의 비접촉식 근접성 기반 통신을 제공하도록 구성될 수 있음이 이해될 것이다. 예를 들어, NFC 컴포넌트(120)는 전자기/정전기 커플링 기술들을 수반하는 것들과 같은 임의의 적합한 단거리 통신을 제공하도록 구성될 수 있다.

[0140] NFC 컴포넌트(120)가 근거리 통신에 관하여 기술되었지만, 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200) 사이의 임의의 적합한 비접촉식 근접성 기반 모바일 결제 또는 임의의 다른 적합한 유형의 비접촉식 근접성 기반 통신을 제공하도록 구성될 수 있다는 것이 이해될 것이다. 예를 들어, NFC 컴포넌트(120)는 전자기/정전기 커플링 기술들을 수반하는 것들과 같은 임의의 적합한 단거리 통신을 제공하도록 구성될 수 있다. 대안적으로, 일부 실시예들에서, 디바이스(100)의 NFC 컴포넌트(120)는 프로세서(102) 또는 디바이스(100)의 임의의 기타 부분에 이용가능한 데이터가 디바이스(100)의 NFC 컴포넌트(120)와 판매자 서브시스템(200)의 판매자 단말기(220) 간의 임의의 적합한 비접촉식 근접성 기반 통신으로서 교환되도록 인에이블하기 위한 임의의 적합한 컴포넌트들을 포함하도록 구성될 수 있지만, NFC 컴포넌트(120)는 프로세서(600)의 크리덴셜 데이터와 같은 금융 거래에 안전하게 자금을 공급하기 위하여 보안 크리덴셜 데이터를 생성하기 위한 크리덴셜 애플릿들을 디바이스(100)에 안전하게 저장하도록 동작가능한 보안 요소를 포함하거나 포함하지 않을 수 있다.

[0141] 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(예를 들어, 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 디바이스(100)는 다른 것들과 함께 동작하는 둘 이상의 디바이스의 조합으로서 제공될 수 있음이 이해될 것이다(예컨대, 임의의 적합한 근접 통신 프로토콜(예컨대, 블루투스™)을 통해 통신가능하게 결합된 셀룰러 전화기와 스마트 워치).

[0142] 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 있는 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 디스플레이할 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.

[0143] 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 탄성파, 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.

[0144] 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 각 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 달리 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, 스크린들이 디스플레이 출력 컴포넌트(112a) 상에 디스플레이될 수 있으며 다양한 사용자 인터페이스 요소들(예컨대, 도 3a 내지 도 3d의 스크린들(190a 내지 190d))을 포함할 수 있다. 추가적으로 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.

[0145] 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 전송하고 수신하도록 구성될 수 있는 접속 포트일 수 있다. 예를 들어, I/O 컴포넌트(114b)는 미국 캘리포니아주 쿠파티노 소재의 애플사의 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.

[0146] 전자 디바이스(100)는 또한, 적어도 하나의 햅틱 또는 촉각적 출력 컴포넌트(112c)(예컨대, 림블러), 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-처리 애플리케이션과 연계하여 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 달리 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. 게다가, 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 하우징(101) 내에 위치될 수 있고, 마크 또는 심볼(121)이 하우징(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.

[0147] 도 1 내지 도 9에 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 이용하여 한 전자 디바이스로부터 다른 전자 디바이스로 전달될 수 있다(예를 들어, 컴퓨터 판독가능 매체는 통신 컴포넌트(106)를 통해 전자 디바이스(100)로 (예를 들어, 애플리케이션(103)의 적어도 일부분으로서 그리고/또는 애플리케이션(113)의 적어도 일부분으로서 그리고/또는 애플리케이션(143)의 적어도 일부분으로서) 전달될 수 있음). 그러한 일시적 컴퓨터 판독가능 매체는 컴퓨터 판독가능 코드, 명령어들, 데이터 구조들, 프로그램 모듈들, 또는 다른 데이터를 반송파 또는 다른 전송 메커니즘과 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.

[0148] 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 이해될 것이다. 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 모듈들은 하나 이상의 특정한 태스크를 수행할 수 있거나 하나 이상의 특정한 추상 데이터 형(abstrack data type)을 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.

[0149] 시스템(1)의 모듈들 또는 컴포넌트들 또는 서브시스템들 중 하나 이상의 적어도 일부는, 임의의 적합한 방식으로 (예를 들어, 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 개체에 저장되거나 달리 그에 액세스가능할 수 있다. 예를 들어, NFC 컴포넌트(120)의 임의의 또는 각각의 모듈은 임의의 적합한 기술들을 이용하여(예를 들어, 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.

[0150] 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 이용하여 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 인터페이스할 수 있다. 대안적으로, NFC 컴포넌트(120)는 탈착가능할 필요는 없으며, 모듈의 이용에 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 이용할 수 있다. 시스템(1)의 임의의 또는 각각의 모듈 또는 컴포넌트(예컨대, NFC 컴포넌트(120)의 임의의 또는 각각의 모듈)는 자신의 처리 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, 처리 회로 및/또는 메모리를 공유할 수 있다.

[0151] 본 개시내용은 본 기술에서의 그러한 개인 정보 데이터의 이용이 사용자들에게 이득을 주기 위해 사용될 수 있음을 인식한다. 예를 들어, 개인 정보 데이터는 더 큰 관심이 있는 타겟 콘텐츠를 사용자에게 전달하는 데 이용될 수 있다. 따라서, 그러한 개인 정보 데이터의 이용은 전달된 콘텐츠의 계산된 제어를 가능하게 한다. 게다가, 사용자에게 이득을 주는 개인 정보 데이터에 대한 다른 이용들이 또한 본 개시내용에 의해 고려된다.

[0152] 본 개시내용은 그러한 개인 정보 데이터의 수집, 분석, 공개, 전달, 저장, 또는 다른 이용을 책임지고 있는 개체들이 잘 확립된 프라이버시 정책들 및/또는 프라이버시 관례들을 준수할 것이라는 것을 추가로 고려한다. 특히, 그러한 개체들은, 대체로 개인 정보 데이터를 사적이고 안전하게 유지시키기 위한 산업적 또는 행정적 요건들을 충족시키거나 넘어서는 것으로 인식되는 프라이버시 정책들 및 관례들을 구현하고 지속적으로 이용해야 한다. 예를 들어, 사용자들로부터의 개인 정보는 개체의 적법하며 적절한 사용들을 위해 수집되어야 하고, 이들 적법한 사용들을 벗어나서 공유되거나 판매되지 않아야 한다. 또한, 그러한 수집은 단지 사용자들의 고지에 입각한 동의를 수신한 후에만 발생해야 한다. 부가적으로, 그러한 개체들은 그러한 개인 정보 데이터에 대한 액세스를 보호하고 안전하게 하며 개인 정보 데이터에 대한 액세스를 갖는 다른 사람들이 그들의 프라이버시 정책들 및 절차들을 고수한다는 것을 보장하기 위한 임의의 필요한 단계들을 취할 것이다. 게다가, 그러한 개체들은 널리 인정된 프라이버시 정책들 및 관례들에 대한 그들의 고수를 증명하기 위해 제3자들에 의해 그들 자신들이 평가를 받을 수 있다.

[0153] 전술한 것에도 불구하고, 본 개시내용은 또한 사용자가 개인 정보 데이터의 사용, 또는 그에 대한 액세스를 선택적으로 차단하는 실시예들을 고려한다. 즉, 본 개시내용은 그러한 개인 정보 데이터에 대한 액세스를 방지하거나 차단하기 위해 하드웨어 및/또는 소프트웨어 요소들이 제공될 수 있다는 것을 고려한다. 예를 들어, 광고 전달 서비스들의 경우에, 본 기술은 사용자들이 서비스들에 대한 등록 동안에 개인 정보 데이터의 수집에의 참여에 "동의(opt in)" 또는 "동의하지 않음(opt out)"을 선택하게 하도록 구성될 수 있다. 다른 예에서, 사용자들은 타겟 콘텐츠 전달 서비스들을 위한 위치 정보를 제공하지 않도록 선택할 수 있다. 또 다른 예에서, 사용자들은 정확한 위치 정보를 제공하지 않지만 위치 구역 정보의 전달을 허용하도록 선택할 수 있다.

[0154] 설명된 개념들의 추가 애플리케이션들

[0155] 보안 디바이스 기능에 대한 온라인 액세스를 확인하기 위한 시스템, 방법, 및 컴퓨터 판독가능 매체가 기술되어 있지만, 어떤 식으로든 본 명세서에 기술된 주제의 기술적 사상 및 범주로부터 벗어나지 않으면서 본 명세서에서 많은 변경들이 행해질 수 있다는 것이 이해될 것이다. 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 알려지

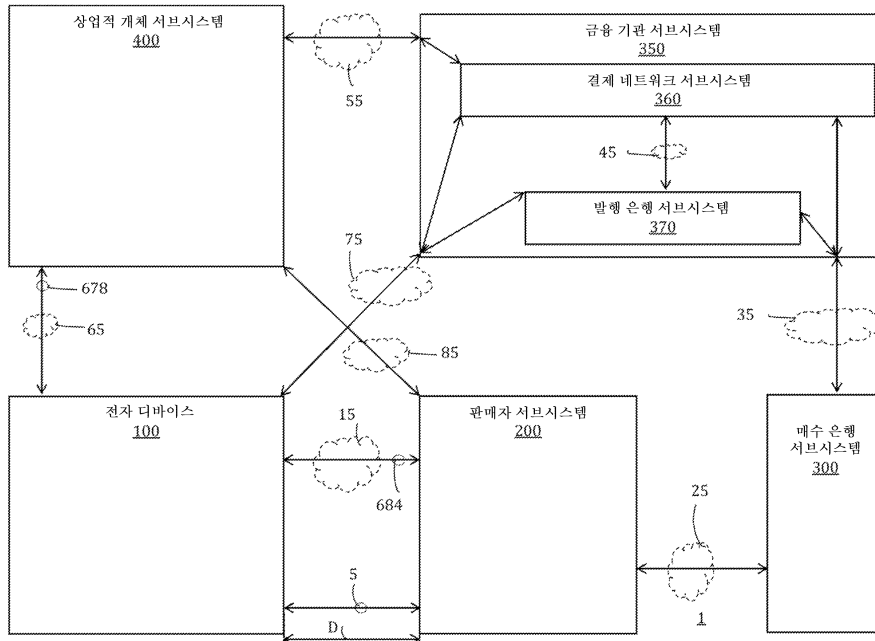
는 명확한 대안물들이, 정의된 요소들의 범주 내에 있는 것으로 규정된다.

[0156]

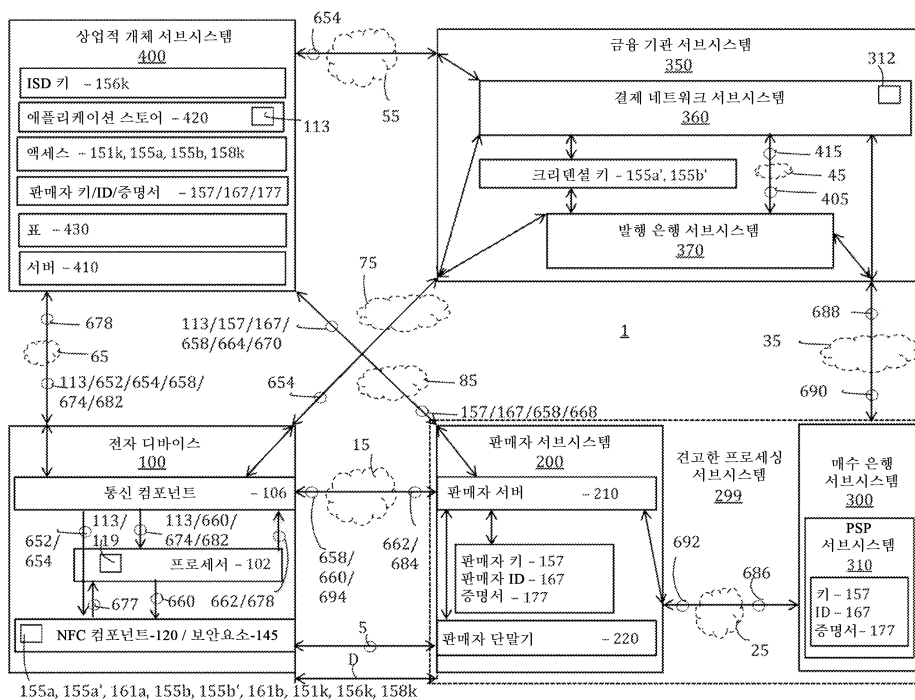
따라서, 이들 통상의 기술자는, 본 발명이, 제한이라기보다는 예시의 목적으로 제시되는, 기술된 실시예들 이외의 것에 의해 실시될 수 있다는 것을 이해할 것이다.

도면

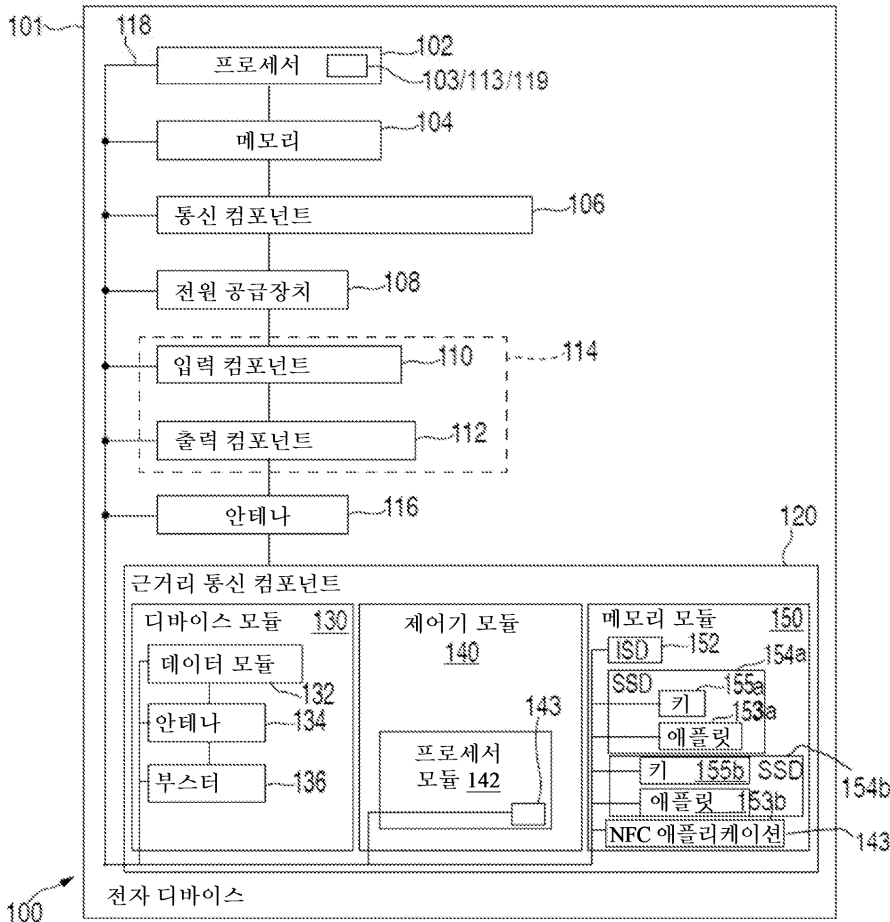
도면1



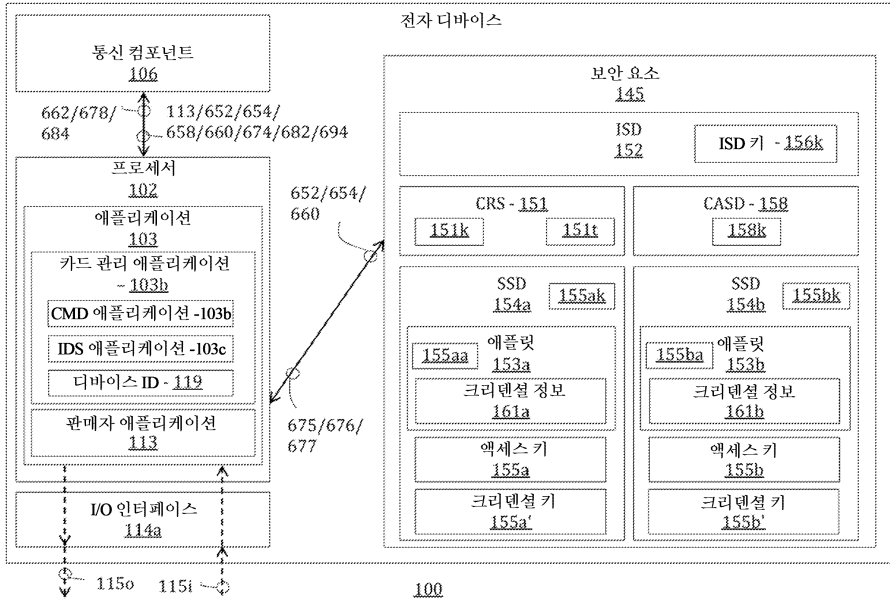
도면1a



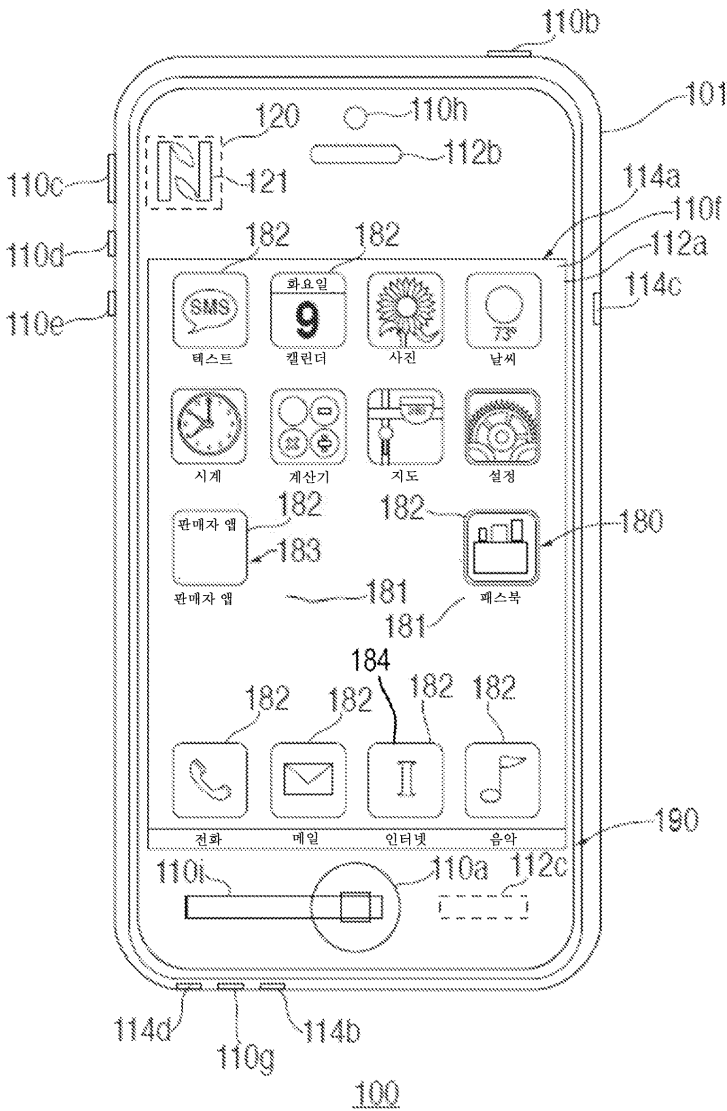
도면2



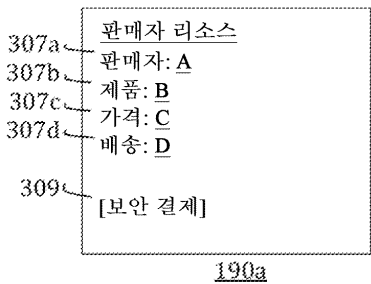
도면2a



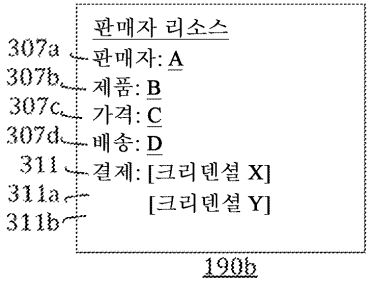
도면3



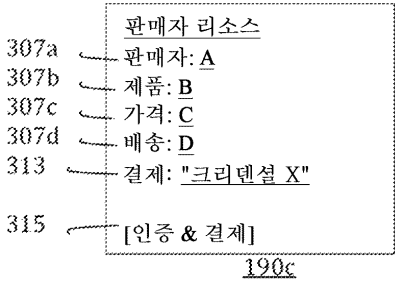
도면3a



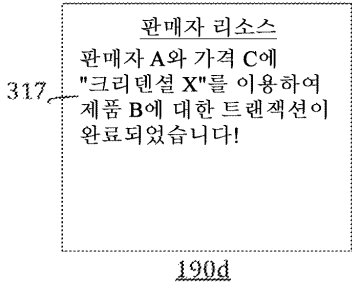
도면3b



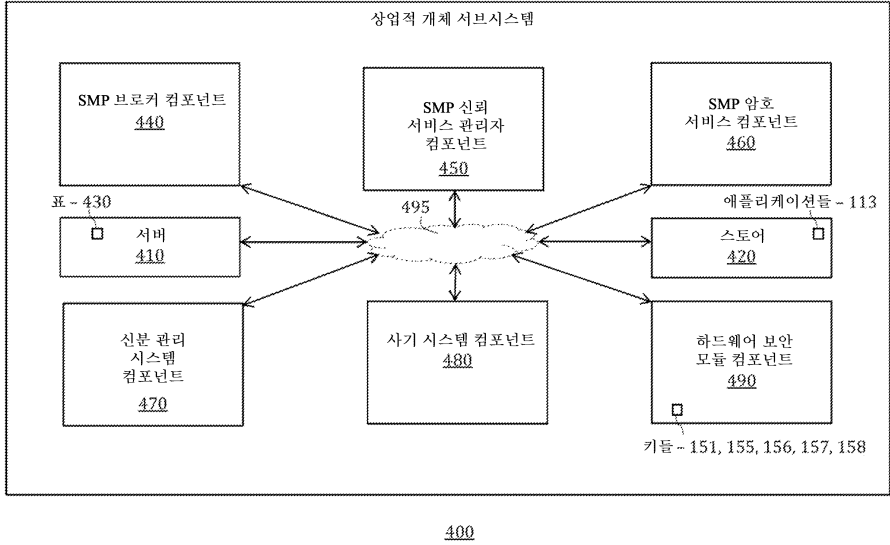
도면3c



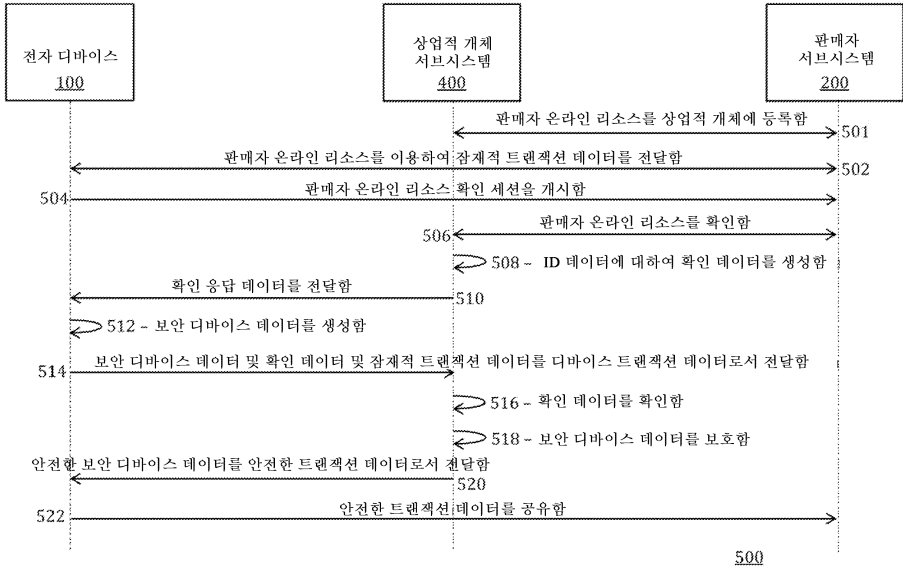
도면3d



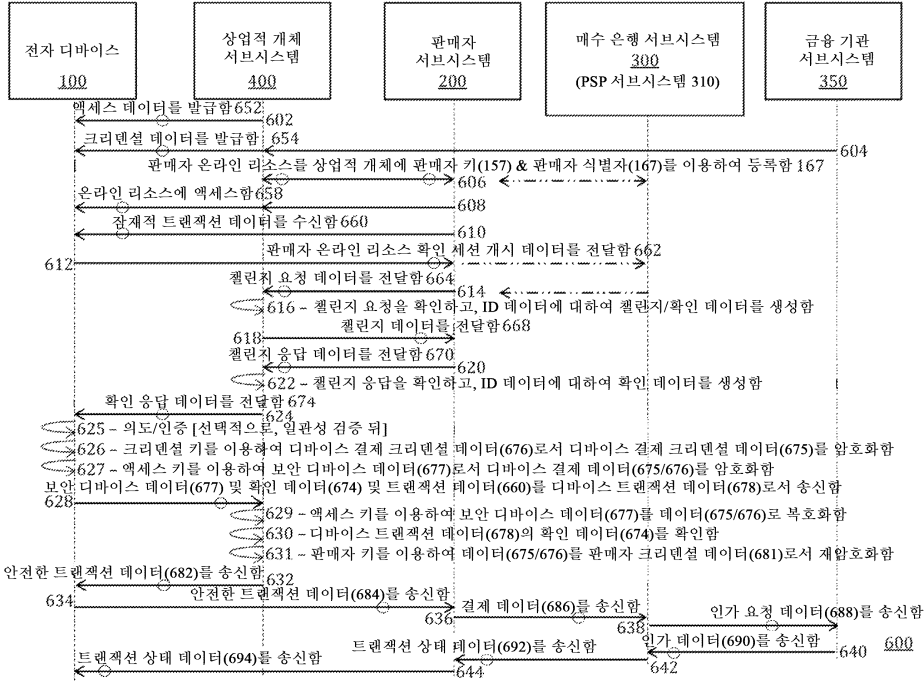
도면4



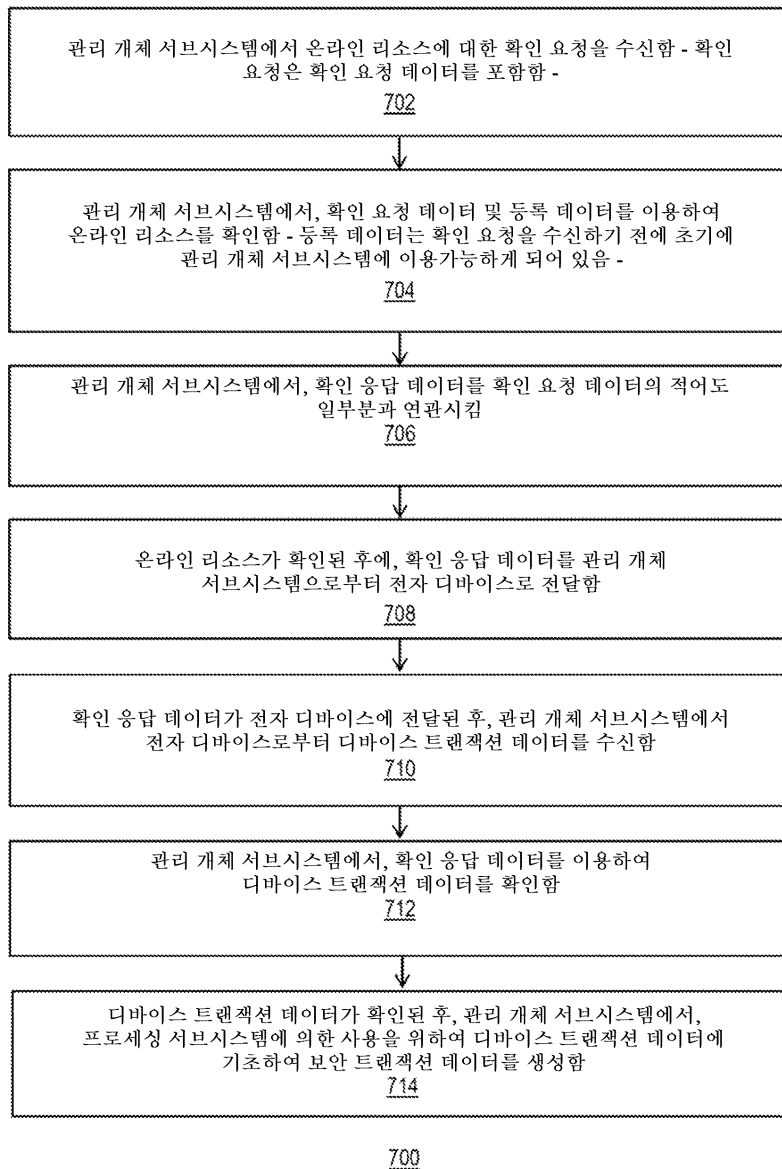
도면5



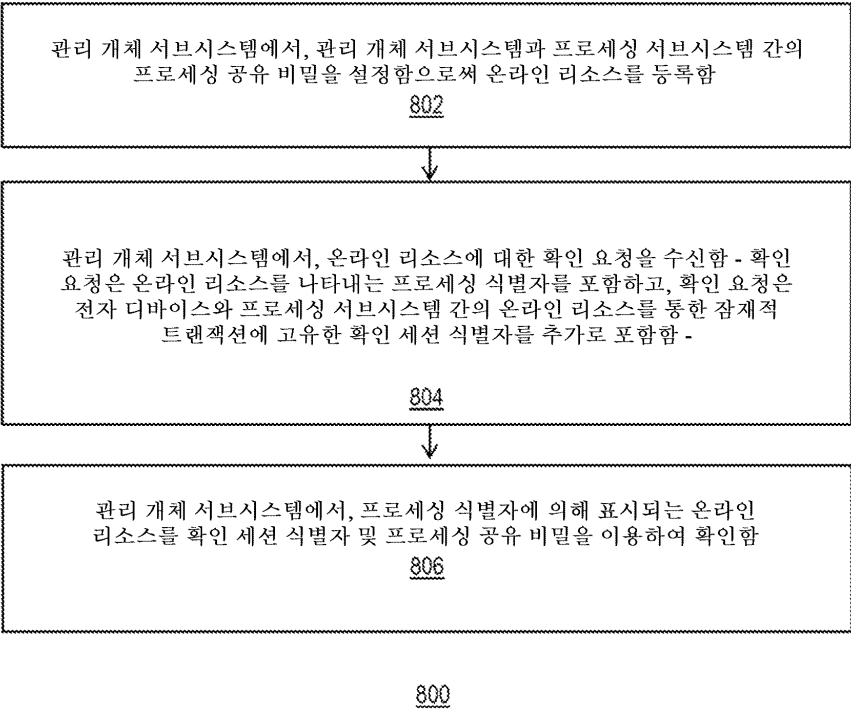
도면6



도면7



도면8



도면9

