(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년04월22일
(11) 등록번호 10-1971329
(24) 등록일자 2019년04월16일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01) *G06Q 20/02* (2012.01)
G06Q 20/36 (2012.01) *G06Q 20/38* (2012.01)
G06Q 40/02 (2012.01) *H04L 29/08* (2006.01)
(52) CPC특허분류
G06Q 20/401 (2013.01)
G06Q 20/02 (2013.01)
(21) 출원번호 10-2016-7011605
(22) 출원일자(국제) 2014년10월08일
심사청구일자 2016년05월02일
(85) 번역문제출일자 2016년05월02일
(65) 공개번호 10-2016-0068833
(43) 공개일자 2016년06월15일
(86) 국제출원번호 PCT/US2014/059621
(87) 국제공개번호 WO 2015/084486
국제공개일자 2015년06월11일
(30) 우선권주장
61/912,727 2013년12월06일 미국(US)
14/475,260 2014년09월02일 미국(US)
(56) 선행기술조사문헌
KR1020120105296 A*
KR1020130084646 A*
KR1020050013084 A
KR101113555 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
애플 인크.
미국 캘리포니아 (우편번호 95014) 쿠퍼티노 원 애플 파크 웨이
(72) 발명자
칸, 아머, 에이.
미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프 1
린데, 조아킴
미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프 1
(뒷면에 계속)
(74) 대리인
장덕순, 백만기

전체 청구항 수 : 총 20 항 심사관 : 박장환

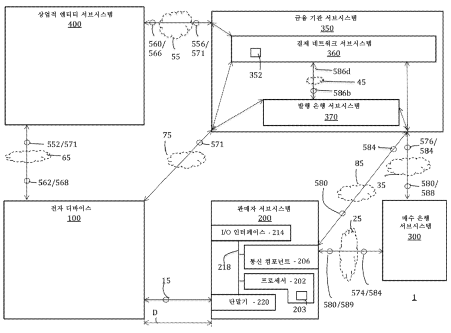
(54) 발명의 명칭 **전자 디바이스 상의 크리덴셜의 프로비저닝 및 인증**

(57) 요 약

크리덴셜들을 프로비저닝 및/또는 인증하기 위한 시스템들, 방법들, 및 컴퓨터 판독가능 매체들이 제공된다. 하나의 예시적인 실시예에서, 금융 기관 시스템은 전자 디바이스 및 판매자 서브시스템과 통신할 수 있다. 금융 기관 시스템은, 특히, 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 생성하고, 가상 상업 크리덴셜을

(뒷면에 계속)

대 표 도 - 도1



전자 디바이스 상에 프로비저닝하고, 가상 상업 크리덴셜이 전자 디바이스 상에 프로비저닝된 후, 판매자 서브시스템으로부터 거래 요청을 수신하고, 수신된 거래 요청으로부터 가상 상업 크리덴셜을 식별하고, 가상 상업 크리덴셜의 식별에 응답하여, 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크가 금융 거래에서 사용하기 위해 인증되는지 여부를 결정하도록 구성될 수 있다. 추가적인 실시예들이 또한 제공된다.

(52) CPC특허분류
G06Q 20/3223 (2013.01)
G06Q 20/36 (2013.01)
G06Q 20/3821 (2013.01)
G06Q 20/405 (2013.01)
G06Q 40/02 (2013.01)
H04L 67/10 (2013.01)
H04M 1/72522 (2013.01)
H04M 1/72561 (2013.01)

(72) 발명자
로젠, 자차리, 에이.
미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프 1
헐리, 티모시, 에스.
미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프 1

명 세 서

청구범위

청구항 1

전자 디바이스 및 판매자 서브시스템(merchant subsystem)과 통신하는 금융 기관 시스템으로서,

적어도 하나의 프로세서 컴포넌트;

적어도 하나의 메모리 컴포넌트; 및

적어도 하나의 통신 컴포넌트

를 포함하며, 상기 금융 기관 시스템은,

상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 메모리 컴포넌트에서, 실제 상업 크리덴셜(actual commerce credential)을 검증된 사용자 정보와 연관시키고;

상기 실제 상업 크리덴셜이 상기 검증된 사용자 정보와 연관된 후에, 상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 적어도 하나의 메모리 컴포넌트 내의 데이터베이스에서, 상기 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 생성하고 - 상기 링크는 초기에 인증되지 않은 것으로 설정된 링크 인증 상태를 포함함 -;

상기 링크가 생성된 후에, 상기 적어도 하나의 통신 컴포넌트에 의해, 상기 전자 디바이스의 보안 요소 상에 상기 가상 상업 크리덴셜을 프로비저닝(provisioning)하고;

상기 가상 상업 크리덴셜이 상기 전자 디바이스의 상기 보안 요소 상에 프로비저닝된 후에, 상기 적어도 하나의 통신 컴포넌트에 의해, 상기 전자 디바이스 및 상기 판매자 서브시스템을 포함하는 금융 거래에서의 시도 동안 상기 판매자 서브시스템으로부터 거래 요청을 수신하고;

상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 수신된 거래 요청으로부터 상기 가상 상업 크리덴셜을 식별하고;

상기 수신된 거래 요청으로부터의 상기 가상 상업 크리덴셜의 식별에 응답하여, 상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 실제 상업 크리덴셜과 상기 가상 상업 크리덴셜 사이의 상기 링크의 링크 인증 상태가 인증되었는지를 결정하고;

상기 실제 상업 크리덴셜과 상기 가상 상업 크리덴셜 사이의 상기 링크의 상기 링크 인증 상태가 인증되지 않은 것으로 결정되는 경우,

상기 금융 기관 시스템에 의해 상기 전자 디바이스의 사용자로부터 인증 정보를 요청하고;

상기 요청에 응답하여, 상기 금융 기관 시스템에 의해 인증 응답 데이터를 수신하고;

상기 금융 기관 시스템에 의해, 상기 수신된 인증 응답 데이터가 상기 검증된 사용자 정보의 적어도 일부를 나타내는지를 검출하고;

상기 검출이 상기 수신된 인증 응답 데이터가 상기 검증된 사용자 정보의 적어도 일부를 나타내는 것을 검출하는 것을 포함하는 경우, 상기 금융 기관 시스템에 의해 상기 링크의 상기 링크 인증 상태를 인증된 것으로 갱신하고;

상기 검출이 상기 수신된 인증 응답 데이터가 상기 검증된 사용자 정보의 적어도 일부를 나타내지 않는 것을 검출하는 것을 포함하는 경우, 상기 금융 기관 시스템에 의해 상기 링크의 상기 링크 인증 상태를 인증되지 않은 것으로 유지함으로써

상기 실제 상업 크리덴셜과 상기 가상 상업 크리덴셜 사이의 상기 링크를 인증하려고 시도하도록 구성되는, 금융 기관 시스템.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서, 상기 금융 기관 시스템은, 상기 실제 상업 크리덴셜과 상기 가상 상업 크리덴셜 사이의 상기 링크가 인증되는 것으로 결정되는 경우, 상기 실제 상업 크리덴셜을 이용하여 상기 수신된 거래 요청에 자금을 제공(fund)하도록 추가로 구성되는, 금융 기관 시스템.

청구항 5

제1항에 있어서, 상기 금융 기관 시스템은, 상기 가상 상업 크리덴셜에 링크되는 상기 실제 상업 크리덴셜과 연관된 어떠한 상기 검증된 사용자 정보도 상기 전자 디바이스로부터 먼저 수신하지 않고, 상기 전자 디바이스의 상기 보안 요소 상에 상기 가상 상업 크리덴셜을 프로비저닝하도록 구성되는, 금융 기관 시스템.

청구항 6

방법으로서,

금융 기관 서브시스템에 의해, 실제 상업 크리덴셜을 검증된 사용자 정보와 연관시키는 단계;

상기 연관시키는 단계 후에, 상기 금융 기관 서브시스템에 의해, 상기 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 생성하는 단계 - 상기 링크를 생성하는 단계는 상기 링크의 링크 인증 상태를 인증되지 않은 것으로 초기에 설정하는 단계를 포함함 -;

상기 생성하는 단계 후에, 상기 금융 기관 서브시스템에 의해, 전자 디바이스 상의 상기 가상 상업 크리덴셜의 프로비저닝을 가능하게 하는 단계;

상기 전자 디바이스 상의 상기 가상 상업 크리덴셜의 상기 프로비저닝을 가능하게 하는 단계 후에, 상기 금융 기관 서브시스템에 의해, 상기 전자 디바이스 및 판매자 서브시스템을 포함하는 금융 거래에서의 시도 동안 상기 판매자 서브시스템으로부터 거래 요청을 수신하는 단계;

상기 금융 기관 서브시스템에 의해, 상기 수신된 거래 요청으로부터 상기 가상 상업 크리덴셜을 식별하는 단계;

상기 수신된 거래 요청으로부터의 상기 가상 상업 크리덴셜의 식별에 응답하여, 상기 금융 기관 서브시스템에 의해, 상기 실제 상업 크리덴셜과 상기 가상 상업 크리덴셜 사이의 상기 링크의 상기 링크 인증 상태가 인증되었는지를 결정하는 단계; 및

상기 결정하는 단계가 상기 실제 상업 크리덴셜과 상기 가상 상업 크리덴셜 사이의 상기 링크의 상기 링크 인증 상태가 인증되지 않은 것으로 결정하는 단계를 포함하는 경우, 상기 금융 기관 서브시스템에 의해, 상기 실제 상업 크리덴셜과 상기 가상 상업 크리덴셜 사이의 상기 링크를 인증하려고 시도하는 단계

를 포함하고, 상기 시도하는 단계는,

상기 금융 기관 서브시스템에 의해 상기 전자 디바이스의 사용자로부터 인증 정보를 요청하는 단계;

상기 요청하는 단계에 응답하여, 상기 금융 기관 서브시스템에 의해 인증 응답 데이터를 수신하는 단계;

상기 금융 기관 서브시스템에 의해, 상기 수신된 인증 응답 데이터가 상기 검증된 사용자 정보의 적어도 일부를 나타내는지를 검출하는 단계;

상기 검출하는 단계가 상기 수신된 인증 응답 데이터가 상기 검증된 사용자 정보의 적어도 일부를 나타내는 것을 검출하는 단계를 포함하는 경우, 상기 금융 기관 서브시스템에 의해 상기 링크의 상기 링크 인증 상태를 인증된 것으로 갱신하는 단계; 및

상기 검출하는 단계가 상기 수신된 인증 응답 데이터가 상기 검증된 사용자 정보의 적어도 일부를 나타내지 않는 것을 검출하는 단계를 포함하는 경우, 상기 금융 기관 서브시스템에 의해 상기 링크의 상기 링크 인

증 상태를 인증되지 않은 것으로 유지하는 단계

를 포함하는, 방법.

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

제6항에 있어서, 상기 실제 상업 크리덴셜과 상기 가상 상업 크리덴셜 사이의 상기 링크가 인증되는 것으로 결정되는 경우, 상기 방법은, 상기 금융 기관 서브시스템이 상기 실제 상업 크리덴셜을 이용하여 상기 수신된 거래 요청에 자금을 제공하는 단계를 추가로 포함하는, 방법.

청구항 11

제6항에 있어서, 상기 실제 상업 크리덴셜과 연관된 어떠한 인증 정보도 전달하도록 상기 전자 디바이스에 요구하지 않고, 상기 전자 디바이스로 하여금 상기 실제 상업 크리덴셜을 이용해 구매에 자금을 제공하기 위해 상기 프로비저닝된 가상 상업 크리덴셜을 사용할 수 있게 하는 단계를 추가로 포함하는, 방법.

청구항 12

제1항에 있어서, 상기 금융 기관 시스템은 상기 전자 디바이스 상에 상기 가상 상업 크리덴셜을 프로비저닝한 후에 상기 전자 디바이스 상에 데이터를 추가하지 않고 상기 링크를 인증하도록 구성되는, 금융 기관 시스템.

청구항 13

제6항에 있어서, 상기 인증하는 단계는 상기 전자 디바이스 상의 임의의 데이터 추가를 포함하지 않는, 방법.

청구항 14

제6항에 있어서, 상기 인증하는 단계는 임의의 데이터를 상기 전자 디바이스에 통신하는 단계를 포함하지 않는, 방법.

청구항 15

제6항에 있어서, 상기 인증하는 단계는 상기 전자 디바이스로부터 임의의 데이터를 통신하는 단계를 포함하지 않는, 방법.

청구항 16

판매자 서브시스템 및 전자 디바이스와 통신하는 금융 기관 시스템으로서,

적어도 하나의 프로세서 컴포넌트;

적어도 하나의 메모리 컴포넌트; 및

적어도 하나의 통신 컴포넌트

를 포함하며, 상기 금융 기관 시스템은,

상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 메모리 컴포넌트에서, 실제 상업 크리덴셜을 검증된 사용자 정보와 연관시키고;

상기 실제 상업 크리덴셜이 상기 검증된 사용자 정보와 연관된 후에, 상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 적어도 하나의 메모리 컴포넌트에서, 상기 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이

의 링크를 생성하고;

상기 링크가 생성된 후에, 상기 적어도 하나의 통신 컴포넌트에 의해, 상기 전자 디바이스 상에 상기 가상 상업 크리덴셜을 프로비저닝하고;

상기 가상 상업 크리덴셜이 상기 전자 디바이스 상에 프로비저닝된 후에, 상기 적어도 하나의 통신 컴포넌트에 의해, 상기 판매자 서브시스템으로부터, 상기 판매자 서브시스템 및 상기 전자 디바이스를 포함하는 거래에 대한 거래 허가 요청에서 상기 가상 상업 크리덴셜을 수신하도록 구성되며, 상기 금융 기관 시스템은, 상기 금융 기관 시스템에 의해 상기 전자 디바이스로부터 어떠한 상기 검증된 사용자 정보도 수신하지 않고, 다음의 각각:

상기 실제 상업 크리덴셜을 상기 검증된 사용자 정보와 연관시키는 것;

상기 실제 상업 크리덴셜과 상기 가상 상업 크리덴셜 사이의 상기 링크를 생성하는 것; 및

상기 전자 디바이스 상에 상기 가상 상업 크리덴셜을 프로비저닝하는 것

을 수행하도록 구성되는, 금융 기관 시스템.

청구항 17

제16항에 있어서, 상기 금융 기관 시스템은

상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 수신된 가상 상업 크리덴셜, 및 상기 적어도 하나의 메모리 컴포넌트에 저장된 데이터 구조를 이용함으로써 상기 수신된 가상 상업 크리덴셜과 상기 실제 상업 크리덴셜 사이의 상기 링크를 검출하고;

상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 검출된 링크가 인증되었는지를 결정하고;

상기 검출된 링크가 인증되지 않은 것으로 결정되는 경우, 상기 적어도 하나의 통신 컴포넌트에 의해, 상기 링크를 검출하기 위해 상기 전자 디바이스의 사용자로부터 인증 정보를 요청하도록 추가로 구성되는, 금융 기관 시스템.

청구항 18

제17항에 있어서, 상기 금융 기관 시스템은 상기 데이터 구조를 이용함으로써 상기 검출된 링크가 인증되는지 여부를 결정하도록 구성되는, 금융 기관 시스템.

청구항 19

제16항에 있어서, 상기 금융 기관 시스템은,

상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 수신된 가상 상업 크리덴셜과 상기 실제 상업 크리덴셜 사이의 상기 링크를 검출하고;

상기 적어도 하나의 프로세서 컴포넌트에 의해, 상기 검출된 링크가 인증되었는지를 결정하고;

상기 검출된 링크가 인증되지 않은 것으로 결정되는 경우, 상기 적어도 하나의 통신 컴포넌트에 의해, 상기 전자 디바이스의 사용자로부터 인증 정보를 요청하고;

상기 적어도 하나의 통신 컴포넌트에 의해, 상기 사용자로부터 상기 인증 정보를 요청하도록 상기 판매자 서브시스템에게 명령함으로써, 상기 전자 디바이스의 사용자로부터 상기 인증 정보를 요청하도록 추가로 구성되는, 금융 기관 시스템.

청구항 20

제19항에 있어서, 상기 금융 기관 시스템은 상기 전자 디바이스 상에 데이터를 추가하지 않고 상기 링크를 인증하도록 구성되는, 금융 기관 시스템.

청구항 21

제16항에 있어서, 상기 금융 기관 시스템은 상기 요청된 인증 정보를 상기 판매자 서브시스템으로부터 수신하도

록 추가로 구성되는, 금융 기관 시스템.

청구항 22

비일시적 컴퓨터 판독가능 매체로서, 그 위에 기록되는 컴퓨터 판독가능 명령어들을 포함하며, 상기 컴퓨터 판독가능 명령어들은,

실제 상업 크리덴셜을 검증된 사용자 정보와 연관시키고;

가상 상업 크리덴셜과 상기 실제 상업 크리덴셜 사이의 링크를 검출하고;

상기 검출된 링크가 인증되는지 여부를 결정하고;

상기 검출된 링크가 인증되지 않는 것으로 결정되는 경우에, 상기 실제 상업 크리덴셜과 연관된 임의의 상기 검증된 사용자 정보를 통신하도록 사용자의 전자 디바이스에 요구하지 않고, 상기 사용자로부터 상기 실제 상업 크리덴셜과 연관된 상기 검증된 사용자 정보를 포함하는 인증 정보를 요청하기 위한, 비일시적 컴퓨터 판독가능 매체.

청구항 23

제22항에 있어서, 상기 실제 상업 크리덴셜과 연관된 상기 요청된 인증 정보를 이용하여 상기 검출된 링크를 인증하기 위해 그 위에 기록되는 추가적인 컴퓨터 판독가능 명령어들을 추가로 포함하는, 비일시적 컴퓨터 판독가능 매체.

청구항 24

전자 디바이스 및 판매자 서브시스템 중 적어도 하나와 통신하는 금융 기관 시스템으로서,

적어도 하나의 프로세서 컴포넌트;

적어도 하나의 메모리 컴포넌트; 및

적어도 하나의 통신 컴포넌트

를 포함하며, 상기 금융 기관 시스템은,

상기 금융 기관 시스템에 의해 상기 전자 디바이스로부터 어떠한 검증된 사용자 정보도 수신하지 않고, 실제 상업 크리덴셜을 상기 검증된 사용자 정보와 연관시키고;

상기 금융 기관 시스템에 의해 상기 전자 디바이스로부터 어떠한 상기 검증된 사용자 정보도 수신하지 않고, 상기 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 생성하고;

상기 금융 기관 시스템에 의해 상기 전자 디바이스로부터 어떠한 상기 검증된 사용자 정보도 수신하지 않고, 상기 전자 디바이스 상의 상기 가상 상업 크리덴셜의 프로비저닝을 가능하게 하도록 구성되는, 금융 기관 시스템.

청구항 25

제24항에 있어서, 상기 금융 기관 시스템은, 상기 판매자 서브시스템으로부터, 상기 전자 디바이스 및 상기 판매자 서브시스템을 포함하는 거래에 대한 거래 허가 요청에서 상기 가상 상업 크리덴셜을 수신하도록 추가로 구성되는, 금융 기관 시스템.

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

발명의 설명

기 술 분 야

[0001] 본 개시내용은 전자 디바이스 상의 크리덴셜들의 프로비저닝(provisioning) 및 인증에 관한 것이며, 보다 구체적으로는, 전자 디바이스 상의 가상 상업 크리덴셜(virtual commerce credential)들의 프로비저닝 및 인증에 관한 것이다.

배 경 기 술

[0002] 휴대용 전자 디바이스들(예컨대, 셀룰러 전화기들)에는, 다른 엔티티와의 비접촉식 근접-기반 통신을 가능하게 하기 위한 근거리 통신(near field communication, "NFC") 컴포넌트들이 제공될 수 있다. 종종, 이들 통신은, 전자 디바이스로 하여금 신용 카드 크리덴셜 또는 대중 교통 티켓 크리덴셜과 같은 상업 크리덴셜에 액세스하고 그것을 공유할 것을 요구하는, 금융 거래들 또는 다른 보안 데이터 거래들과 연관된다. 그러나, 그러한 비접촉식 근접-기반 통신들은 흔히 그러한 상업 크리덴셜들을 악성 엔티티들에 의한 차단(interception)에 노출시킨다.

발명의 내용

[0003] 본 문헌은, 근거리 통신 및/또는 다른 무선 통신이 가능한 전자 디바이스 상에서 크리덴셜들을 프로비저닝하고 인증하기 위한 시스템들, 방법들, 및 컴퓨터 판독가능 매체들을 기술한다.

[0004] 예를 들어, 금융 기관 시스템은 전자 디바이스 및 판매자 서브시스템(merchant subsystem)과 통신할 수 있다. 금융 기관 시스템은 적어도 하나의 프로세서 컴포넌트, 적어도 하나의 메모리 컴포넌트, 및 적어도 하나의 통신 컴포넌트를 포함할 수 있으며, 여기서 금융 기관 시스템은, 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 생성하고, 전자 디바이스 상에 가상 상업 크리덴셜을 프로비저닝하고, 가상 상업 크리덴셜이 전자 디바이스 상에 프로비저닝된 후, 판매자 서브시스템으로부터 거래 요청을 수신하고, 수신된 거래 요청으로부터 가상 상업 크리덴셜을 식별하고, 가상 상업 크리덴셜의 식별에 응답하여, 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크가 금융 거래에서 사용하기 위해 인증되는지 여부를 결정하도록 구성될 수 있다.

[0005] 다른 예로서, 방법은, 금융 기관 서브시스템을 이용해, 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 생성하는 단계를 포함할 수 있다. 생성하는 단계 후에, 방법은 또한 금융 기관 서브시스템을 이용하여 전자 디바이스 상의 가상 상업 크리덴셜의 프로비저닝을 가능하게 하는 단계를 포함할 수 있다. 전자 디바이스 상의 가상 상업 크리덴셜의 프로비저닝 단계 후에, 방법은 또한 금융 기관 서브시스템을 이용하여 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 인증하는 단계를 포함할 수 있다.

[0006] 또 다른 예로서, 판매자 시스템은 전자 디바이스 및 금융 기관 서브시스템과 통신할 수 있다. 판매자 시스템은 프로세서 컴포넌트, 메모리 컴포넌트, 및 통신 컴포넌트를 포함할 수 있으며, 여기서 판매자 시스템은, 전자 디바이스로부터 비접촉식 근접-기반 통신을 수신하고, 수신된 통신 중에서 디바이스 상업 크리덴셜을 나타내는 정보를 금융 기관 서브시스템으로 전송하고, 전송된 정보에 기초하여 금융 기관 서브시스템으로부터 인가 요청을 수신하고, 수신된 인가 요청에 기초하여 실제 상업 크리덴셜에 대한 인증 정보를 제공하도록 전자 디바이스의 사용자에게 프롬프트(prompt)하도록 구성될 수 있다.

[0007] 또 다른 예로서, 금융 기관 시스템은 판매자 서브시스템과 통신할 수 있다. 금융 기관 시스템은 적어도 하나의 프로세서 컴포넌트, 적어도 하나의 메모리 컴포넌트, 및 적어도 하나의 통신 컴포넌트를 포함할 수 있으며, 여기서 금융 기관 시스템은 판매자 서브시스템으로부터 가상 상업 크리덴셜을 수신하고, 수신된 가상 상업 크리덴

셜과 실제 상업 크리덴셜 사이의 링크를 검출하고, 검출된 링크가 인증되는지 여부를 결정하도록 구성될 수 있다.

[0008] 또 다른 예로서, 비일시적 컴퓨터 판독가능 매체는 가상 상업 크리덴셜과 실제 상업 크리덴셜 사이의 링크를 검출하고, 검출된 링크가 인증되는지 여부를 결정하기 위한, 그 위에 기록되는 컴퓨터 판독가능 명령어들을 포함할 수 있다.

[0009] 또 다른 예로서, 금융 기관 시스템은 전자 디바이스 및 판매자 서브시스템 중 적어도 하나와 통신할 수 있다. 금융 기관 시스템은 적어도 하나의 프로세서 컴포넌트, 적어도 하나의 메모리 컴포넌트, 및 적어도 하나의 통신 컴포넌트를 포함할 수 있으며, 여기서 금융 기관 시스템은 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 생성하고, 전자 디바이스 상의 가상 상업 크리덴셜의 프로비저닝을 가능하게 하고, 전자 디바이스 상의 가상 상업 크리덴셜의 프로비저닝 후에 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 인증하도록 구성될 수 있다.

[0010] 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. 본 명세서에 기술된 주제의 다른 특징들, 양태들 및 이점들은 하기의 상세한 설명, 도면 및 청구범위로부터 명백해질 것이다.

도면의 간단한 설명

[0011] 이하의 논의는 하기 도면들을 참조하며, 도면들에서 유사한 참조 부호들은 전체에 걸쳐 유사한 부분들을 지칭할 수 있다.

도 1은 전자 디바이스 상에서 크리덴셜들을 프로비저닝하고 인증하기 위한 예시적인 시스템의 개략도이다;

도 2는 도 1의 시스템의 전자 디바이스의 더욱 상세한 개략도이다;

도 3은 도 1 및 도 2의 전자 디바이스의 정면도이다;

도 4는 도 1의 시스템의 상업적 엔티티 서브시스템(commercial entity subsystem)의 더욱 상세한 개략도이다;

도 5 내지 도 6은 전자 디바이스 상에서 크리덴셜들을 프로비저닝하고 인증하기 위한 예시적인 프로세스들의 흐름도이다;

도 7은 전자 디바이스 상에서 크리덴셜들을 프로비저닝하고 인증하기 위해 사용될 수 있는 도 1의 시스템의 예시적인 데이터 구조를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0012] 보안 데이터 거래에서 나중에 사용하기 위한 전자 디바이스 상의 상업 크리덴셜의 프로비저닝은, 금융 기관이, 실제 상업 크리덴셜을 식별하는 것, 그 실제 상업 크리덴셜을 가상 상업 크리덴셜과 링크시키는 것, 및 실제 상업 크리덴셜보다는 그 가상 상업 크리덴셜을 전자 디바이스 상에 프로비저닝하는 것을 포함할 수 있다. 나중에, 판매자가 전자 디바이스로부터 가상 상업 크리덴셜을 포함하는 금융 거래 요청을 (예컨대, 비접촉식 근접-기반 통신으로서) 수신하는 경우, 판매자는 가상 상업 크리덴셜을 갖는 금융 거래 요청을 금융 기관에 포워드할 수 있고, 이어서 금융 기관은 그 가상 상업 크리덴셜에 이전에 링크되었던 실제 상업 크리덴셜을 식별할 수 있고 그 실제 상업 크리덴셜을 이용하여 금융 거래 요청에 자금을 제공(fund)하려고 시도할 수 있다. 가상 상업 크리덴셜과 실제 상업 크리덴셜 사이의 링크는 가상 상업 크리덴셜이 전자 디바이스 상에 프로비저닝될 때 생성될 수 있지만 인증되지 않을 수 있어서, 프로비저닝된 가상 상업 크리덴셜을 전자 디바이스가 금융 거래 요청에서 처음으로 사용할 때에, 금융 기관은 그 가상 상업 크리덴셜에 링크된 실제 상업 크리덴셜을 검출할 수는 있지만 링크가 아직 인증되지 않았다고 결정할 수 있다. 그러한 경우들에서, 링크되었지만 비-인증된 그 실제 상업 크리덴셜을 이용하여 금융 거래 요청에 자금을 제공하려고 시도하기 전에, 금융 기관은 링크를 제대로 인증하기 위해 필요한 정보를 전자 디바이스의 사용자로부터 획득하기 위해 판매자를 레버리지(leverage)할 수 있다.

[0013] 도 1은, (예를 들어, 상업적 엔티티 서브시스템(400)과 연계하여) 금융 기관 서브시스템(350)으로부터 하나 이상의 크리덴셜이 전자 디바이스(100) 상에 프로비저닝될 수 있는 시스템(1)을 도시하며, 여기서 그러한 크리덴

셜들은 판매자 서브시스템(200) 및 연관된 매수 은행 서브시스템(acquiring bank subsystem)(300)과 상거래를 이행하기 위해 전자 디바이스(100)에 의해 사용될 수 있다. 도 2 및 도 3은 시스템(1)의 전자 디바이스(100)의 특정 실시예들에 관한 추가적인 상세 사항들을 도시하는 한편, 도 4는 시스템(1)의 상업적 엔티티 서브시스템(400)의 특정 실시예들에 관한 추가적인 상세 사항들을 도시한다. 도 5 내지 도 6은 시스템(1)의 맥락에서, 전자 디바이스(100) 상에서 크리덴셜들을 프로비저닝하고 인증하기 위한 예시적인 프로세스들의 흐름도이고, 도 7은 전자 디바이스(100) 상에서 크리덴셜들을 프로비저닝하고 인증하기 위해 사용될 수 있는 도 1의 시스템의 예시적인 데이터 구조(352)를 도시한다.

[0014] 도 1, 도 2, 도 3 및 도 4의 설명

[0015] 도 1은, 전자 디바이스 상의 크리덴셜들의 안전한 프로비저닝 및/또는, 상업적 또는 금융 거래에서 그러한 크리덴셜들을 사용할 수 있게 하도록 그러한 크리덴셜들의 인증을 허용할 수 있는 예시적인 시스템(1)의 개략도이다. 예를 들어, 도 1에 도시된 바와 같이, 시스템(1)은 최종-사용자 전자 디바이스(100)뿐만 아니라 전자 디바이스(100) 상에 크리덴셜들을 안전하게 프로비저닝하기 위한 상업적 엔티티 서브시스템(400) 및 금융 기관 서브시스템(350)을 포함할 수 있다. 게다가, 도 1에 도시된 바와 같이, 시스템(1)은 또한, 그러한 프로비저닝된 크리덴셜들에 기초하여 전자 디바이스(100)로부터 비접촉식 근접-기반 통신들(15)(예컨대, 근거리 통신들)을 수신하기 위한 판매자 서브시스템(200)뿐만 아니라, 금융 기관 서브시스템(350)과의 거래를 완료하기 위해 그러한 비접촉식 근접-기반 통신들(15)을 이용할 수 있는 매수 은행 서브시스템(300)을 포함할 수 있다. 판매자 서브시스템(200)은 또한 거래 동안에 프로비저닝된 크리덴셜의 사용자 인증을 가능하게 하도록 구성될 수 있다.

[0016] 도 2에 도시된 바와 같이, 그리고 이하에서 더 상세히 기술되는 바와 같이, 전자 디바이스(100)는 프로세서(102), 메모리(104), 통신 컴포넌트(106), 전력 공급장치(108), 입력 컴포넌트(110), 출력 컴포넌트(112), 안테나(116), 및 근거리 통신("NFC") 컴포넌트(120)를 포함할 수 있으며, 여기서 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 또는 I/O 인터페이스(114)일 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. 프로세서(102)는 애플리케이션(103) 및/또는 애플리케이션(113)과 같은 하나 이상의 애플리케이션을 실행하는 데 사용될 수 있다. 애플리케이션들(103, 113) 각각은 하나 이상의 운영 체제 애플리케이션, 펌웨어 애플리케이션, 미디어 재생 애플리케이션, 미디어 편집 애플리케이션, 통신 애플리케이션(예컨대, 단문자 메시지 서비스(short message service, "SMS") 또는 텍스트 메시지 애플리케이션, 전화 통신 애플리케이션, 이메일 애플리케이션, 인터넷 애플리케이션 등), NFC 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)을 로딩할 수 있다. 하나의 예로서, 애플리케이션(103)은 운영 체제 애플리케이션일 수 있는 한편 애플리케이션(113)은 제3자 애플리케이션(예를 들어, 판매자 서브시스템(200)의 판매자와 연관된 애플리케이션 및/또는 금융 기관 서브시스템(350)의 금융 기관과 연관된 애플리케이션 및/또는 상업적 엔티티 서브시스템(400)에 의해 생성되고/되거나 유지되는 애플리케이션)일 수 있다. NFC 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200)(예컨대, 판매자 서브시스템(200)의 판매자 결제 단말기(220)) 사이에서 임의의 적합한 비접촉식 근접-기반 거래들 또는 통신들(15)을 가능하게 할 수 있는 임의의 적합한 근접-기반 통신 메커니즘일 수 있다. NFC 컴포넌트(120)는 전자 디바이스(100)와 서브시스템(200) 사이에서 비접촉식 근접-기반 통신(15)을 가능하게 하기 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 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 제어기 모듈(140)은, NFC 컴포넌트(120)의 기능을 지시하는 데 도움을 줄 수 있는 NFC 저전력 모드 또는 wallet 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) 사이의 NFC 통신(15)을 허용할 수 있다. NFC 메모리 모듈(150)은 변조 금지(tamper resistant)일 수 있고 보안 요소(secure element)의 적어도 일부분을 제공할 수 있다. 예를 들어, 그러한 보안 요소는, 잘-식별된 신뢰 기관(well-identified trusted authority)들의 세트에 의해 제시될 수 있는 규칙들 및 보안 요건들(예컨대, 금융 기관 서브시스템의 권한 및/또는 글로벌플랫폼(GlobalPlatform)과 같은 산업 표준)에 따라 애플리케이션들 및 그것들의 기밀의 암호화 데이터(예컨대, 애플릿(153) 및 키(155))를 안전하게 호스팅할 수 있는 변조-금지 플랫폼을 (예컨대, 단일의 또는 다중 칩 보안 마이크로컨트롤러로서) 제공하도록 구성될 수 있다. NFC 메모리 모듈(150)은 발행자 보안 도메인(issuer security domain, "ISD")(152) 및 보충적 보안 도메인(supplemental security domain, "SSD")(154)(예컨대, 서비스 제공자 보안 도메인(service provider security domain, "SPSD"), 신뢰 서비스 관리자 보안 도메인(trusted service manager security domain, "TSMSD") 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(trusted service manager, "TSM") 또는 발행 금융 기관(issuing financial institution)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 프로비저닝하기 위한 키들 및/또는 다른 적합한 정보를 저장할 수 있는 NFC 메모리 모듈(150)의 일부분일 수 있다. 특정한 보충적 보안 도메인("SSD")(154)(예컨대, SSD들(154a, 154b) 중 하나)은, 전자 디바이스(100)에 특정 특권들 또는 결제 권리들을 제공할 수 있는 특정 크리덴셜(예컨대, 특정 신용 카드 크리덴셜 또는 특정 대중 교통 카드 크리덴셜)과 연관될 수 있다. 각각의 SSD(154)는 자신의 애플리케이션 또는 애플릿(153)(예컨대, 애플릿들(153a, 153b) 중 각각의 애플릿)에 대한 자신의 관리자 키(155)(예컨대, 키들(155a, 155b) 중 각각의 키)를 가질 수 있으며, 이는 전자 디바이스(100)와 판매자 서브시스템(200) 사이의 NFC 통신(15)으로서 NFC 디바이스 모듈(130)에 의한 사용을 위해 그 SSD(154)의 특정 크리덴셜을 인에이블하도록 활성화될 필요가 있을 수 있다.

[0017] 도 1의 판매자 서브시스템(200)는, (예를 들어, 전자 디바이스(100)가 단말기(220)의 소정 거리 또는 근접성 D 내에 올 때) 전자 디바이스(100)로부터 NFC 통신(15)을 검출, 판독, 또는 달리 수신하기 위한 단말기(220)의 판독기를 포함할 수 있다. 따라서, 판매자 단말기(220)와 전자 디바이스(100) 사이의 NFC 통신(15)이 무선으로 일어날 수 있으며, 그와 같이, 각각의 디바이스들 사이에 분명한(clear) "가시선(line of sight)"을 요구하지 않을 수 있다는 것에 주의한다. NFC 디바이스 모듈(130)은 수동 또는 능동일 수 있다. 수동인 경우, NFC 디바이스 모듈(130)은 판매자 서브시스템(200)의 적합한 단말기(220)의 응답 범위 D 내에 있을 때에만 활성화될 수 있다. 예를 들어, 판매자 서브시스템(200)의 단말기(220)는 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, 판매자 서브시스템(200)의 단말기(220)로 NFC 통신(15)으로서 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 서브시스템(200)의 단말기(220)로 NFC 통신(15)으로서 능동적으로 전송하게 할 수 있다. 도 1에 또한 도시된 바와 같이, 그리고 이하에서 더욱 상세히 기술되는 바와 같이, 판매자 서브시스템(200)은 또한 전자 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 판매자 프로세서 컴포넌트(202), 전자 디바이스(100)의 애플리케이션(103/113)과 동일하거나 유사할 수 있는 판매자 애플리케이션(203), 전자 디바이스(100)의 통신 컴포넌트(106)와 동일하거나 유사할 수 있는 판매자 통신 컴포넌트(206), 전자 디바이스(100)의 I/O 인터페이스(114)와 동일하거나 유사할 수 있는 판매자 I/O 인터페이스(214), 전자 디바이스(100)의 버스(118)와 동일하거나 유사할 수 있는 판매자 버스(218), 전자 디바이스(100)의 메모리 컴포넌트(104)와 동일하거나 유사할 수 있는 판매자 메모리 컴포넌트(도시되지 않음), 및/또는 전자 디바이스(100)의 전력 공급장치 컴포넌트(108)와 동일하거나 유사할 수 있는 판매자 전력 공급장치 컴포넌트(도시되지 않음)를 포함할 수 있다.

[0018] 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 애플리케이션과 연관된 GUI(180)의 대응하는 스크린을 디스플레이하도록 구성될 수 있다. 예를 들어, "설정 어시스턴트(Setup Assistant)" 텍스트 표시자(181)로 라벨링된 특정 아이콘(182)(즉, 특정 아이콘(183))이 선택되면, 디바이스(100)는 특정 설정 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.

[0019] 도 1의 시스템(1)을 다시 참조하면, NFC 컴포넌트(120)가 디바이스(100)의 인에이블된 크리덴셜과 연관된 상업 크리덴셜 데이터(예컨대, NFC 컴포넌트(120)의 SSD(154)의 인에이블된 애플릿(153)과 연관된 상업 크리덴셜 데이터)를 갖는 NFC 통신(15)을 판매자 서브시스템(200)으로 전달하도록 적절하게 인에이블되는 경우, 매수 은행 서브시스템(300)은 (예컨대, 이하에서 더욱 상세히 기술되는 바와 같이) 금융 기관 서브시스템(350)과의 상업적 또는 금융 거래를 완료하기 위해 NFC 통신(15) 중에서 그러한 상업 크리덴셜 데이터를 이용할 수 있다. 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 발생되는 대금을 지불할 소비자의 능력에 대한 1차 책임(primary liability)을 맡는 금융 기관일 수 있다. 각각의 특정 크리덴셜은 특정 사용자의 계정 또는 계정들에 전자적으로 링크될 수 있는 특정 결제 카드와 연관될 수 있다. 신용 카드, 직불 카드, 차지 카드(charge card), 선불 카드, 플릿 카드(fleet card), 선물 카드 등을 포함한, 다양한 유형들의 결제 카드가 적합하다. 특정 결제 카드의 상업 크리덴셜이, 판매자 서브시스템(200)과의 NFC 통신(15)에서 사용하기 위해 발행 은행 서브시스템(370)에 의해 전자 디바이스(100) 상에 프로비저닝될 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, 상업 크리덴셜들)의 사용을 처리할 수 있는 다양한 매수 은행 및/또는 다양한 발행 은행(370)의 네트워크일 수 있다. 대안적으로 또는 추가적으로, 상업적 또는 금융 거래에서 사용하기 위해 디바이스(100) 상에 프로비저닝될 수 있는 소정 크리덴셜들은 특정 사용자의 계정 또는 계정들에 전자적으로 링크되거나 달리 연관될 수 있지만, 어떠한 결제 카드와도 연관되지 않을 수 있다. 예를 들어, 사용자의 은행 계좌 또는 다른 금융 계정은 디바이스(100) 상에 프로비저닝된 크리덴셜과 연관될 수 있지만 어떠한 결제 카드와도 연관되지 않을 수 있다.

[0020] 결제 네트워크 서브시스템(360) 및 발행 은행 서브시스템(370)은 단일 엔티티 또는 별개의 엔티티들일 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 서브시스템들(360)일 수 있고, 체이스(Chase), 웰스 파고(Wells Fargo), 뱅크 오브 아메리카(Bank of America) 등과 같은 발행 은행 서브시스템들(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 엔티티일 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.

[0021] 시스템(1) 내에서 거래들을 가능하게 하기 위하여, 하나 이상의 상업 크리덴셜이 전자 디바이스(100) 상에 프로비저닝될 수 있다. 그러나, 디바이스(100) 상에 크리덴셜을 프로비저닝하기 전에, 디바이스(100)의 사용자는 사용자가 크리덴셜의 인가된 사용자이고 크리덴셜이 양호한 상태임(good standing)을 입증하려고 시도할 수 있다. 도 1에 도시된 바와 같이, 상업적 엔티티 서브시스템(400)이 시스템(1) 내에 제공될 수 있으며, 여기서 상업적 엔티티 서브시스템(400)은, 디바이스(100) 상에 금융 기관 서브시스템(350)으로부터의 크리덴셜을 프로비

저닝할지 여부가 결정되고 있을 때 새로운 보안 계층(layer of security)을 제공하고 그리고/또는 더욱 중단없는(seamless) 사용자 경험을 제공하도록 구성될 수 있다. 상업적 엔티티 서브시스템(400)은 디바이스(100)의 사용자에게 다양한 서비스들을 제공할 수 있는 특정 상업적 엔티티에 의해 제공될 수 있다. 단지 하나의 예로서, 상업적 엔티티 서브시스템(400)은 미국 캘리포니아주 쿠퍼티노 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)™ 스토어, 디바이스(100) 상에서 사용할 애플리케이션들을 판매/대여하기 위한 애플 앱 스토어(Apple App Store)™, 디바이스(100)로부터의 데이터를 저장하기 위한 애플 아이클라우드(Apple iCloud)™ 서비스, 다양한 애플 제품을 온라인에서 구입하기 위한 애플 온라인 스토어(Apple Online Store) 등), 애플 사는 또한 디바이스(100) 자체의 제공자, 제조자, 및/또는 개발자일 수 있다(예컨대, 디바이스(100)가 아이팟(iPod)™, 아이패드(iPad)™, 아이폰(iPhone)™ 등인 경우). 추가적으로 또는 대안적으로, 상업적 엔티티 서브시스템(400)은 네트워크 운용자에 의해 제공될 수 있다(예를 들어, 디바이스(100)의 사용자와 관계를 가질 수 있는, 버라이즌(Verizon) 또는 AT&T와 같은, 모바일 네트워크 운용자(예컨대, 소정의 통신 경로를 통해 그리고/또는 소정의 통신 프로토콜을 이용하여 디바이스(100)와 데이터의 통신을 가능하게 하기 위한 데이터 계획)).

[0022] 상업적 엔티티 서브시스템(400)을 제공, 관리, 또는 적어도 부분적으로 제어할 수 있는 상업적 엔티티는 또한, 그 상업적 엔티티에 의해 제공되는 서비스들을 이용하기 위해 상이한 사용자들에게 그들 자신의 개인화된 계정들을 제공할 수 있다. 상업적 엔티티와의 각 사용자 계정은, 사용자가 상업적 엔티티와의 그들의 계정에 로그인하는 데 사용할 수 있는 특정한 개인화된 사용자 ID 및 패스워드와 연관될 수 있다. 상업적 엔티티와의 각 사용자 계정은 또한, 적어도 하나의 상업 크리덴셜과 연관되거나 그에 대한 액세스를 가질 수 있으며, 이어서 상업 크리덴셜은, 상업적 엔티티에 의해 공급되는 서비스들 또는 제품들을 구매하기 위해 사용자에 의해 사용될 수 있다. 예를 들어, 각각의 애플 ID 사용자 계정은 그 애플 ID와 연관된 사용자의 적어도 하나의 신용 카드와 연관될 수 있어서, 신용 카드는 이어서, 애플의 아이튠즈™ 스토어, 애플 앱 스토어™, 애플 아이클라우드™ 서비스 등으로부터 서비스들을 입수하기 위해 그 애플 ID 계정의 사용자에 의해 사용될 수 있다. 상업적 엔티티 서브시스템(400)을 제공, 관리, 또는 적어도 부분적으로 제어할 수 있는 상업적 엔티티(예컨대, 애플 사)는 금융 기관 서브시스템(350)의 임의의 금융 엔티티와 별개이고 그에 독립적일 수 있다. 예를 들어, 상업적 엔티티 서브시스템(400)을 제공, 관리, 또는 적어도 부분적으로 제어할 수 있는 상업적 엔티티는, 상업적 엔티티의 사용자 계정과 연관된 임의의 신용 카드 또는 다른 상업 크리덴셜을 제공 및 관리할 수 있는 임의의 결제 네트워크 서브시스템(360) 또는 발행 은행 서브시스템(370)과 별개이고 그에 독립적일 수 있다. 유사하게, 상업적 엔티티 서브시스템(400)을 제공, 관리, 또는 적어도 부분적으로 제어할 수 있는 상업적 엔티티는, 사용자 디바이스(100) 상에 프로비저닝될 임의의 상업 크리덴셜을 제공 및 관리할 수 있는 임의의 결제 네트워크 서브시스템(360) 또는 발행 은행 서브시스템(370)과 별개이고 그에 독립적일 수 있다. 그러한 상업적 엔티티는, 금융 기관 서브시스템(350)에 의해 제공된 특정 크리덴셜이 사용자 디바이스(100) 상에 프로비저닝되어야 하는지 여부를 상업적 엔티티 서브시스템(400)를 이용해 더욱 안전하게 결정하기 위하여, 그것의 사용자 계정들 각각과 연관된 알려진 상업 크리덴셜 정보, 및/또는 상업적 엔티티 서브시스템(400)이 디바이스(100)에 대하여 결정할 수 있는 임의의 적합한 정보(예컨대, 디바이스(100)에 의해 인에이블된 다양한 통신 메커니즘들)를 레버리지할 수 있다. 추가적으로 또는 대안적으로, 그러한 상업적 엔티티는, 사용자가 사용자 디바이스(100) 상에 금융 기관 서브시스템(350)에 의해 제공된 크리덴셜을 프로비저닝하기를 원할 때에 디바이스(100)의 사용자에게 더욱 중단없는 사용자 경험을 제공하기 위하여, 디바이스(100)의 다양한 컴포넌트(예를 들어, 그 상업적 엔티티가 디바이스(100)를 적어도 부분적으로 생성 또는 관리할 때의 디바이스(100)의 소프트웨어 및/또는 하드웨어 컴포넌트들)를 구성 또는 제어하는 자신의 능력을 레버리지할 수 있다. 상업적 엔티티 서브시스템(400)이 어떻게 구현될 수 있는지의 예에 관한 세부 사항들이 도 4를 참조하여 아래에 제공된다.

[0023] 도 4에 도시된 바와 같이, 상업적 엔티티 서브시스템(400)은 보안 플랫폼 시스템(secure platform system)일 수 있고, 보안 모바일 플랫폼(secure mobile platform, "SMP") 브로커 컴포넌트(410), SMP 신뢰 서비스 관리자(SMP trusted services manager, "TSM") 컴포넌트(420), SMP 암호 서비스 컴포넌트(SMP crypto services component)(430), 식별 관리 시스템(identity management system, "IDMS") 컴포넌트(440), 사기 시스템 컴포넌트(fraud system component)(450), 하드웨어 보안 모듈(hardware security module, "HSM") 컴포넌트(460) 및/또는 저장 컴포넌트(470)를 포함할 수 있다. 상업적 엔티티 서브시스템(400)의 하나의, 일부의, 또는 모든 컴포넌트는, 디바이스(100)의 프로세서 컴포넌트(102)와 동일하거나 유사할 수 있는 하나 이상의 프로세서 컴포넌트, 디바이스(100)의 메모리 컴포넌트(104)와 동일하거나 유사할 수 있는 하나 이상의 메모리 컴포넌트, 및/또는 디바이스(100)의 통신 컴포넌트(106)와 동일하거나 유사할 수 있는 하나 이상의 통신 컴포넌트를 사용하여

구현될 수 있다. 상업적 엔티티 서브시스템(400)의 하나의, 일부의, 또는 모든 컴포넌트는, 금융 기관 서브시스템(350)과 별개이고 그에 독립적일 수 있는 단일 상업적 엔티티(예컨대, 애플 사)에 의해 관리되고, 소유되고, 적어도 부분적으로 제어되고 그리고/또는 달리 제공될 수 있다. 상업적 엔티티 서브시스템(400)의 컴포넌트들은, 디바이스(100) 상에 금융 기관 서브시스템(350)으로부터의 크리덴셜을 프로비저닝할지 여부가 결정되고 있을 때 새로운 보안 계층을 제공하고 그리고/또는 더욱 중단없는 사용자 경험을 제공하기 위해, 서로 그리고 금융 기관 서브시스템(350) 및 전자 디바이스(100) 둘 모두와 집합적으로 상호작용할 수 있다.

[0024] 상업적 엔티티 서브시스템(400)의 SMP 브로커 컴포넌트(410)는 상업적 엔티티 사용자 계정으로 사용자 인증을 관리하도록 구성될 수 있다. SMP 브로커 컴포넌트(410)는 또한, 디바이스(100) 상의 크리덴셜들의 수명 주기 및 프로비저닝을 관리하도록 구성될 수 있다. SMP 브로커 컴포넌트(410)는 디바이스(100) 상에서 사용자 인터페이스 요소들(예컨대, GUI(180)의 요소들)을 제어할 수 있는 1차 종점(primary end point)일 수 있다. 디바이스(100)의 운영 체제 또는 다른 애플리케이션(예컨대, 애플리케이션(103), 애플리케이션(113), 및/또는 애플리케이션(143))은 특정 애플리케이션 프로그래밍 인터페이스(application programming interface, "API")들을 호출하도록 구성될 수 있고, SMP 브로커(410)는 그 API들의 요청들을 처리하고 데이터로 응답하도록 구성될 수 있으며, 이는 디바이스(100)의 사용자 인터페이스를 도출하고 그리고/또는 (예컨대, 상업적 엔티티 서브시스템(400)과 전자 디바이스(100) 사이의 통신 경로(65)를 통해) NFC 컴포넌트(120)의 보안 요소와 통신할 수 있는 애플리케이션 프로토콜 데이터 단위(application protocol data unit, "APDU")들로 응답할 수 있다. 그러한 APDU들은 시스템(1)의 신뢰 서비스 관리자("TSM")(예컨대, 상업적 엔티티 서브시스템(400)과 금융 기관 서브시스템(350) 사이의 통신 경로(55)의 TSM)를 통해 금융 기관 서브시스템(350)으로부터 상업적 엔티티 서브시스템(400)에 의해 수신될 수 있다. 상업적 엔티티 서브시스템(400)의 SMP TSM 컴포넌트(420)는, 금융 기관 서브시스템(350)으로부터 디바이스(100) 상의 크리덴셜 프로비저닝 동작들을 이행하는 데 사용될 수 있는 글로벌플랫폼-기반 서비스들을 제공하도록 구성될 수 있다. 글로벌플랫폼, 또는 임의의 다른 적합한 보안 채널 프로토콜은, SMP TSM 컴포넌트(420)로 하여금, 상업적 엔티티 서브시스템(400)과 금융 기관 서브시스템(350) 사이의 안전한 데이터 통신을 위해 TSM과 디바이스(100)의 보안 요소 사이에서 민감한 계정 데이터를 제대로 통신 및/또는 프로비저닝하게 할 수 있다.

[0025] SMP TSM 컴포넌트(420)는 HSM 컴포넌트(460)를 사용하여 그것의 키들을 보호하고 새로운 키들을 생성하도록 구성될 수 있다. 상업적 엔티티 서브시스템(400)의 SMP 암호 서비스 컴포넌트(430)는, 사용자 인증 및/또는 시스템(1)의 다양한 컴포넌트들 사이의 기밀 데이터 전송에 요구될 수 있는 키 관리 및 암호화 동작들을 제공하도록 구성될 수 있다. SMP 암호 서비스 컴포넌트(430)는 안전한 키 저장 및/또는 불분명한(opaque) 암호화 동작들을 위해 HSM 컴포넌트(460)를 이용할 수 있다. SMP 암호 서비스 컴포넌트(430)의 결제 암호 서비스는 IDMS 컴포넌트(440)와 상호작용하여, 파일-상(on-file) 신용 카드들 또는 상업적 엔티티의 사용자 계정들과 연관된 다른 유형들의 상업 크리덴셜들을 검색하도록 구성될 수 있다. 그러한 결제 암호 서비스는, 그것의 사용자 계정들의 상업 크리덴셜들(예컨대, 신용 카드 번호들)을 설명하는 암호화되지 않은(clear) 텍스트(즉, 비-해싱된(non-hashed)) 정보를 메모리 내에 가질 수 있는 상업적 엔티티 서브시스템(400)의 유일한 컴포넌트이도록 구성될 수 있다. 상업적 엔티티 서브시스템(400)의 상업적 엔티티 사기 시스템 컴포넌트(450)는, 상업 크리덴셜 및/또는 사용자에 관하여 상업적 엔티티에 알려진 데이터에 기초하여(예를 들어, 상업적 엔티티와의 사용자 계정과 연관된 데이터(예컨대, 상업 크리덴셜 정보) 및/또는 상업적 엔티티의 제어 하에 있을 수 있는 임의의 다른 적합한 데이터 및/또는 금융 기관 서브시스템(350)의 제어 하에 있지 않을 수 있는 임의의 다른 적합한 데이터에 기초하여), 상업 크리덴셜에 대해 상업적 엔티티 사기 체크를 실행하도록 구성될 수 있다. 상업적 엔티티 사기 시스템 컴포넌트(450)는 다양한 인자 또는 임계치에 기초하여 크리덴셜에 대한 상업적 엔티티 사기 점수를 결정하도록 구성될 수 있다. 추가적으로 또는 대안적으로, 상업적 엔티티 서브시스템(400)은 저장소(470)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 저장하기 위한 애플 아이클라우드™ 서비스, 다양한 애플 제품을 온라인에서 구입하기 위한 애플 온라인 스토어 등). 단지 하나의 예로서, 저장소(470)는 애플리케이션(113)을 관리하고 이를 디바이스(100)에 (예컨대, 통신 경로(65)를 통해) 제공하도록 구성될 수 있으며, 여기서 애플리케이션(113)은 뱅킹 애플리케이션, 이메일 애플리케이션, 텍스트 메시징 애플리케이션, 인터넷 애플리케이션, 또는 임의의 다른 적합한 애플리케이션과 같은 임의의 적합한 애플리케이션일 수 있다. 임의의 적합한 통신 프로토콜 또는 통신 프로토콜들의 조합이, 상업적 엔티티 서브시스템(400)의 다양한 컴포넌트들 사이에서 (예컨대, 도 4의 적어도 하나의 통신 경로(495)를 통해) 데이터를 전달하고/하거나 상업적 엔티티 서브시스템(400)과 시스템(1)의 다른 컴포넌트들 사이에서(예컨대, 도 1의 통신 경로

(55)를 통한 금융 기관 서브시스템(350) 그리고/또는 도 1의 통신 경로(65)를 통한 전자 디바이스(100)) 데이터를 전달하기 위해 상업적 엔티티 서브시스템(400)에 의해 사용될 수 있다.

[0026] 도 5의 설명

[0027] 도 5는 전자 디바이스 상에서 크리덴셜을 프로비저닝하고 인증하기 위한 예시적인 프로세스(500)의 흐름도이다. 프로세스(500)는 시스템(1)의 다양한 요소들(예를 들어, 전자 디바이스(100), 판매자 서브시스템(200), 매수 은행 서브시스템(300), 금융 기관 서브시스템(350), 및 상업적 엔티티 서브시스템(400))에 의해 구현되는 것으로 도시된다. 그러나, 프로세스(500)는 임의의 다른 적합한 컴포넌트들 또는 서브시스템들을 이용하여 구현될 수 있다는 것이 이해되어야 한다. 프로세스(500)는, 디바이스(100) 또는 임의의 원격 엔티티와 최소의 사용자 상호작용을 가지면서 디바이스(100) 상에서 크리덴셜을 프로비저닝하고/하거나 인증하기 위한 중단없는 사용자 경험을 제공할 수 있다. 프로세스(500)는 단계(502)에서 시작될 수 있으며, 여기서 디바이스(100)는 크리덴셜 프로비저닝 요청 데이터(552)를 상업적 엔티티 서브시스템(400)과 통신할 수 있으며, 크리덴셜 프로비저닝 요청 데이터(552)는 디바이스(100) 상에 프로비저닝될 특정 상업 크리덴셜의 선택뿐만 아니라 디바이스(100)와 연관된 임의의 다른 적합한 정보를 포함할 수 있다. 예를 들어, 사용자가 (예를 들어, 디바이스(100)의 I/O 인터페이스(114a) 상의 GUI(180)와의 사용자 상호작용을 통해, 예컨대 "설정 어시스턴트" 아이콘(183)과 연관된 설정 어시스턴트 애플리케이션의 사용 동안에 그리고/또는 도 3의 "Passbook" 아이콘(184)과 연관된 "Passbook" 또는 "Wallet" 애플리케이션의 사용 동안에) 디바이스(100) 상에 프로비저닝하기 위한 특정 상업 크리덴셜을 선택하면, 그 선택은 디바이스(100)에 의해 상업적 엔티티 서브시스템(400)으로 크리덴셜 프로비저닝 요청 데이터(552)의 적어도 일부분으로서 전송될 수 있다. 그러한 사용자 선택 카드 요청(user selected card request)은 선택된 크리덴셜을 나타내는 임의의 적합한 정보(예컨대, 선택된 상업 크리덴셜과 연관된 주 계좌 번호(primary account number, "PAN")의 참인(true) 버전 또는 해싱된 버전)를 포함할 수 있다. 추가적으로, 크리덴셜 프로비저닝 요청 데이터(552)의 그러한 사용자 선택 카드 요청은 선택된 크리덴셜을 디바이스(100) 상에 프로비저닝하기 위해 금융 기관 서브시스템(350)에 의해 사용될 수 있는, 그 크리덴셜과 연관된 임의의 적합한 보안 정보(예를 들어, 선택된 크리덴셜에 대한 카드 검증 값(card verification value, "CVV"), 선택된 크리덴셜에 대한 만료일, 선택된 크리덴셜에 대한 청구서 발송 주소(billing address) 등)를 포함할 수 있다. 예를 들어, GUI(180)는 전자 디바이스(100)로 하여금, (예를 들어, 선택된 크리덴셜의 CVV, 및/또는 디바이스(100) 상에 선택된 크리덴셜을 프로비저닝하기 위해 시스템(1)에 의해(예를 들어, 금융 기관 서브시스템(350)에 의해) 요구될 수 있는 임의의 다른 적합한 보안 정보와 같은, 보안 정보를 입력함으로써) 선택된 크리덴셜을 하나 이상의 방법으로 인증하도록 사용자에게 프롬프트하게 할 수 있다. 게다가, GUI(180)는 또한, 디바이스(100) 상에 선택된 크리덴셜을 프로비저닝하는 데 적용될 수 있는 다양한 계약 조건(terms and conditions)을 고려 및 수락하도록 사용자에게 프롬프트할 수 있다. 추가적으로 또는 대안적으로, 크리덴셜 프로비저닝 요청 데이터(552)는 디바이스(100) 상의 선택된 크리덴셜의 프로비저닝을 가능하게 하기 위해 상업적 엔티티 서브시스템(400)에 유용할 수 있는 임의의 다른 적합한 정보(예컨대, 그러한 프로비저닝된 크리덴셜을 수신할 수 있는 디바이스(100)의 NFC 컴포넌트(120)의 이용가능한 SSD(154)를 나타낼 수 있는, SSD 식별자)를 포함할 수 있다. 그러한 사용자 선택 카드 요청은 도 1의 통신 경로(65)를 통해 상업적 엔티티 서브시스템(400)으로(예컨대, 상업적 엔티티 서브시스템(400)의 SMP 브로커(410)로) 크리덴셜 프로비저닝 요청 데이터(552)의 적어도 일부분으로서 전자 디바이스(100)에 의해 전송될 수 있다. 예를 들어, 전자 디바이스(100)의 통신 컴포넌트(106)는 임의의 적합한 통신 프로토콜을 이용하여 임의의 적합한 통신 경로(65)를 통해 크리덴셜 프로비저닝 요청 데이터(552)를 전송하도록 구성될 수 있다.

[0028] 도 5에 도시된 바와 같이, 단계(502) 후에, 프로세스(500)는 단계(503)를 포함할 수 있으며, 여기서 단계(502)의 데이터(552)에 의해 식별될 수 있는 선택된 상업 크리덴셜에 대해 위험 분석이 실행될 수 있다. 예를 들어, 위험 분석 단계(503)는 프로비저닝되도록 선택된 크리덴셜에 대한 적어도 하나의 적합한 위험 평가를 포함할 수 있으며, 여기서 그러한 위험 평가는 디바이스(100) 자체의 특정 속성들을 고려할 수 있다. 단지 하나의 예로서, 단계(503)의 위험 분석은 상업적 엔티티 서브시스템(400)에 의해 이행될 수 있는 상업적 엔티티 사기 위험 분석 및/또는 금융 기관 서브시스템(350)에 의해 이행될 수 있는 금융 엔티티 사기 위험 분석을 포함할 수 있다(예컨대, 2013년 11월 27일자로 출원된, 미국 특허 출원 제14/092,205호에 기술된 바와 같으며, 이는 본 명세서에서 참고로 포함됨). 디바이스(100) 상에 프로비저닝하도록 단계(502)에서 선택된 크리덴셜이 단계(503)의 위험 분석을 성공적으로 통과하는 경우, 이어서 상업적 엔티티 서브시스템(400)은 단계(504)로 진행할 수 있다. 그러나, 디바이스(100) 상에 프로비저닝하도록 단계(502)에서 선택된 크리덴셜이 단계(503)의 위험 분석의 적합한 위험 임계치들을 충족하지 않는 경우, 상업적 엔티티 서브시스템(400)은, 크리덴셜이 디바이스(100) 상에 프로비저닝되어야 한다고 시스템(1)이 결정할 수 있는 확실성을 증가시키기 위해 추가적인 예방 단계들(도 5

에 도시되지 않음)을 취할 수 있다(예를 들어, 금융 기관 서브시스템(350)과 디바이스(100) 사이의 1회용 패스워드 데이터의 통신을 가능하게 하기 위해 단계들이 취해질 수 있다).

[0029] 단계(502)에서 크리덴셜 프로비저닝 요청 데이터(552)의 적어도 일부분으로서 사용자 선택 카드 요청을 수신하는 것에 응답하여, 단계(504)에서 상업적 엔티티 서브시스템(400)에 의해(예컨대, SMP 브로커 컴포넌트(410)에 의해) SSD가 생성될 수 있다. 예를 들어, 크리덴셜이 그 안에 프로비저닝될, 디바이스(100)의 SSD(예컨대, NFC 컴포넌트(120)의 SSD(154))에 대한 식별자가 단계(504)에서 생성될 수 있으며, 여기서 SSD는, 단계(502)의 요청 데이터(552)에 의해 제공될 수 있는 보안 요소 정보(예컨대, SSD 식별자)에 기초하여 적어도 부분적으로 결정될 수 있다. 다음으로, 단계(504) 후에, 상업적 엔티티 서브시스템(400)(예컨대, SMP 브로커 컴포넌트(410))은, (예를 들어, 임의의 적합한 통신 프로토콜을 이용하여 임의의 적합한 통신 경로(55)를 통해(예컨대, 경로(55)의 TSM을 통해)) 디바이스(100) 상의 선택된 크리덴셜의 프로비저닝을 위한 요청을 금융 기관 서브시스템(350)으로 전송할 수 있다. 예를 들어, 도 5의 프로세스(500)의 단계(506)에서, 상업적 엔티티 서브시스템(400)은 크리덴셜 프로비저닝 명령 데이터(credential provisioning instruction data)(556)를 생성하고 이를 금융 기관 서브시스템(350)으로(예컨대, 금융 기관 서브시스템(350)의 결제 네트워크 서브시스템(360)으로) 전송할 수 있다. 일부 실시예들에서, 그러한 크리덴셜 프로비저닝 명령은, 선택된 크리덴셜이 디바이스(100) 상에 프로비저닝되어야 한다고 상업적 엔티티 서브시스템(400)이 결정하는 경우에만, 생성되고 전송될 수 있다. 예를 들어, 그러한 결정은, 선택된 크리덴셜이 단계(503)의 위험 분석을 성공적으로 통과하는 경우에, 이루어질 수 있다. 대안적으로, 선택된 크리덴셜이 단계(503)의 위험 분석을 성공적으로 통과하지 않는 경우, 상업적 엔티티 서브시스템(400)은 여전히 단계(506)를 진행하기로 결정할 수 있다. 크리덴셜 프로비저닝 명령 데이터(556)는 금융 기관 서브시스템(350)이 디바이스(100) 상에 선택된 크리덴셜을 프로비저닝하기 시작하는 데 사용할 수 있는 임의의 적합한 데이터를 포함할 수 있으며, 예컨대 선택된 크리덴셜을 나타내는 데이터(예를 들어, 선택된 크리덴셜에 대한 보안 데이터(예컨대, 데이터(552)의 크리덴셜의 PAN) 및/또는 프로비저닝된 크리덴셜을 수신하기 위한(예컨대, 단계(504)에서의) 디바이스(100)의 이용가능한 SSD(154)의 식별, 이는 금융 기관 서브시스템(350)으로 통신 경로(55)를 통해 상업적 엔티티 서브시스템(400)에 의해 통신하기에 적합한 방식으로 보안 키로 인코딩될 수 있음)를 포함할 수 있다.

[0030] 상업적 엔티티 서브시스템(400)으로부터 그러한 크리덴셜 프로비저닝 명령 데이터(556)를 수신하는 것에 응답하여, 금융 기관 서브시스템(350)(예컨대, 결제 네트워크 서브시스템(360))은, 프로비저닝될 선택된 크리덴셜의 디스크립터뿐만 아니라, 일단 프로비저닝된 크리덴셜과의 사용자 상호작용을 돕기 위해 디바이스(100) 상에 제공될 수 있는 시각적 삽화 및 다른 메타데이터를 생성하도록 구성될 수 있다. 예를 들어, 도 5의 프로세스(500)의 단계(510)에서, 금융 기관 서브시스템(350)은, 크리덴셜 프로비저닝 명령 데이터(556)로부터 특정 데이터(예컨대, 선택된 크리덴셜에 대한 크리덴셜 식별 정보)를 끌어내고, 디바이스(100)에 일단 프로비저닝된 크리덴셜과의 임의의 최종적인(eventual) 사용자 상호작용을 도울 수 있는 하나 이상의 디스크립터 및/또는 다양한 유형의 메타데이터를 생성하는 데 유용할 수 있는 금융 기관 서브시스템(350)에 이용가능한 정보의 하나 이상의 데이터베이스에 액세스할 수 있고, 이어서, 금융 기관 서브시스템(350)은 크리덴셜 프로비저닝 응답 데이터(560)를 생성하고 이를 상업적 엔티티 서브시스템(400)으로 다시 전송할 수 있다. 그러한 크리덴셜 프로비저닝 응답 데이터(560)는 프로비저닝될 크리덴셜의 디스크립터 및 프로비저닝될 크리덴셜과의 사용자 상호작용을 돕기 위해 디바이스(100) 상에 제공되어야 하는 임의의 적합한 메타데이터를 포함할 수 있다. 예를 들어, 그러한 크리덴셜 프로비저닝 응답 데이터(560)는, 디바이스(100)로 하여금 크리덴셜을 디바이스(100)에 이용가능한 것으로서 시각적으로 나타나게 하도록 할 수 있는 적합한 데이터의 일부 또는 모두, 예컨대, 시각적 로고들/아이콘들 및 사용자에게 제공될 수 있는 크리덴셜과 연관된 다른 사용자 인식가능 데이터를 포함할 수 있다(예컨대, 도 3의 "Passbook" 텍스트 표시자(181)로 라벨링된 특정 아이콘(182)(즉, 특정 아이콘(184))이 선택될 때, 디바이스(100)는 특정 passbook 또는 wallet 애플리케이션을 시작하거나 달리 그에 액세스할 수 있고, 크리덴셜의 하나 이상의 시각적 디스크립터를 포함할 수 있는 특정 사용자 인터페이스의 스크린들을 디스플레이할 수 있다). 금융 기관 서브시스템(350)에 의해 생성된 그러한 크리덴셜 프로비저닝 응답 데이터(560)는, 임의의 적합한 통신 경로 유형을 통해 임의의 적합한 통신 프로토콜을 이용하여 도 1의 통신 경로(55)를 통해 (예컨대, 통신 경로(55)의 TSM을 통해) 상업적 엔티티 서브시스템(400)으로(예컨대, SMP 브로커 컴포넌트(410)로) 금융 기관 서브시스템(350)에 의해(예컨대, 적절한 결제 네트워크 서브시스템(360)에 의해) 전송될 수 있다.

[0031] 일부 실시예들에서, 시스템(1) 및/또는 프로세스(500)는, 단계(502)에서 식별될 수 있고/있거나 단계(503)의 사기 위험 분석에 사용될 수 있는 실제 크리덴셜보다는, 가상 크리덴셜을 디바이스(100) 상에 프로비저닝하도록 구성될 수 있다. 예를 들어, 크리덴셜이 디바이스(100) 상에 프로비저닝될 것으로 결정되면, 실제 크리덴셜 대신에 가상 크리덴셜이 생성되고, 실제 크리덴셜에 링크되며, 디바이스(100) 상에 프로비저닝되도록, (예컨대,

단계(508)에서 금융 기관 서브시스템(350)에 의해, 단계(506)에서 상업적 엔티티 서브시스템(400)에 의해, 그리고/또는 단계(502)에서 디바이스(100)의 사용자에 의해) 요청될 수 있다. 즉, 상업적 엔티티 서브시스템(400)은 단계(506)에서 크리덴셜 프로비저닝 명령 데이터(556)를 생성하고 이를 금융 기관 서브시스템(350)으로 전송할 수 있으며, 이는 또한, 새로운 가상 크리덴셜(예컨대, 디바이스 주 계좌 번호(device primary account number, "D-PAN"))을 생성하고, 그 가상 크리덴셜을 선택된 실제 크리덴셜(즉, 발행 은행에 의해 처음에 발행된 자금 주 계좌 번호(funding primary account number, "F-PAN"))과 링크시키며, 이어서 그 가상 크리덴셜을 디바이스(100) 상에 프로비저닝하기 위한 금융 기관 서브시스템(350)에 대한 특정 명령을 포함할 수 있다. 따라서, 그러한 실시예들에서, 금융 기관 서브시스템(350)은 단계(510)에서 크리덴셜 프로비저닝 응답 데이터(560)를 생성하고 이를 다시 상업적 엔티티 서브시스템(400)으로 전송할 수 있으며, 이는, 프로비저닝될 가상 크리덴셜(예컨대, D-PAN)의 디스크립터, 및 프로비저닝될 가상 크리덴셜과의 사용자 상호작용을 돕기 위해 디바이스(100) 상에 제공되어야 하는 임의의 적합한 메타데이터를 포함할 수 있다. 대안적으로, 일부 실시예들에서, 전자 디바이스(100)는 단계(502)에서 크리덴셜 프로비저닝 요청 데이터(552)를 생성하고 전송할 수 있으며, 이는 또한, 크리덴셜 프로비저닝 요청 데이터(552)에 의해 나타내어진 실제 크리덴셜보다는 그러한 새로운 가상 크리덴셜을 생성하고, 링크시키며, 프로비저닝하기 위한 금융 기관 서브시스템(350)에 대한 특정 명령을 포함할 수 있고, 여기서 그러한 특정 명령은 단계(506)에서 크리덴셜 프로비저닝 명령 데이터(556)를 통해 금융 기관 서브시스템(350)에 전달될 수 있다. 대안적으로, 일부 실시예들에서, 금융 기관 서브시스템(350)은 데이터(552/556)에 의해 나타내어진 실제 크리덴셜보다는 새로운 가상 크리덴셜을 생성하고, 링크시키며, 프로비저닝하기로 결정할 수 있다.

[0032] 가상 크리덴셜과 실제 크리덴셜의 그러한 링킹(linking) 또는 다른 적합한 연관(association)은, 금융 기관 서브시스템(350)의 임의의 적합한 컴포넌트에 의해 수행될 수 있다. 예를 들어, 금융 기관 서브시스템(350)(예컨대, 단계(502)에서 식별된 실제 크리덴셜의 상표와 연관될 수 있는 특정 결제 네트워크 서브시스템(360))은 프로세스(500)의 단계(508)에서 (예를 들어, 도 1 및 도 7에 도시된 바와 같이) 엔트리(702)를 정의하고 이를 가상-링킹 테이블 또는 데이터 구조(352)에 저장할 수 있으며, 여기서 그러한 엔트리(702)는 실제 크리덴셜과 가상 크리덴셜 사이의 연관 또는 링크를 생성할 수 있다. 따라서, 가상 크리덴셜이 디바이스(100)에 의해 판매자 서브시스템(200)과의 금융 거래에 이용되는 경우(예를 들어, 가상 크리덴셜이 디바이스(100) 상에 프로비저닝된 후), 금융 기관 서브시스템(350)은 그 가상 크리덴셜을 나타내는 인가 요청을 (예컨대, 이하에 기술되는, 데이터(576)로서) 수신할 수 있고, (예컨대, 이하에서 기술되는, 프로세스(500)의 단계(528) 및/또는 단계(536)에서) 가상-링킹 테이블(352)에 의해 결정된 바와 같은 식별된 가상 크리덴셜과 연관되거나 다른 식으로 그와 링크된 실제 크리덴셜에 비추어, 그 인가 요청의 분석을 이행할 수 있다. 실제 크리덴셜보다는 가상 크리덴셜을 디바이스(100) 상에 프로비저닝함으로써, 금융 기관 서브시스템(350)은, 가상 크리덴셜이 비인가된 사용자에 의해(예컨대, 디바이스(100) 및/또는 판매자 단말기(220)에 인접하여 위치된 NFC 통신(15) 신호 스틸러(signal stealer)에 의해) 차단되는 경우 초래될 수 있는 사기성 행위(fraudulent activity)를 제한하도록 구성될 수 있으며, 이는 금융 기관 서브시스템(350)(예컨대, 결제 네트워크 서브시스템(360))이 단지, 소정 거래들 동안에(예컨대, 크리덴셜 정보가 사용자에 의해 수동으로 입력되도록 허용할 수 있는 온라인 거래들 또는 다른 거래들 동안이 아닌, 판매자 단말기(220)에 의해 수신된 NFC 거래들 동안에) 가상 크리덴셜을 실제 크리덴셜에 링크시키기 위한 가상-링킹 테이블(352)을 이용하도록 구성될 수 있기 때문이다. 따라서, 가상 크리덴셜을 사용하는 그러한 실시예들에서, 금융 기관 서브시스템(350)에 의해 생성된 프로비저닝 응답 데이터(560)는 테이블(352) 내의 엔트리(702)로부터의 새로운 D-PAN(예컨대, 새로운 가상 크리덴셜 정보)을 포함할 수 있으며, 테이블(352)은 데이터(552)로부터의 선택된 크리덴셜의 F-PAN(예컨대, 실제 크리덴셜 뱅킹 번호)과 이 새로운 D-PAN 사이의 링크를 정의할 수 있다. 프로비저닝 응답 데이터(560)는 또한, F-PAN의 해싱된 버전을 생성하기 위한, 링크된 F-PAN의 마지막 4자리 또는 임의의 적합한 데이터를 포함할 수 있다. 가상 D-PAN 및 실제 F-PAN의 해싱된 버전 둘 다를 디바이스(100) 상에 제공하는 것은, 그 둘 사이에서의 사용자 혼란을 방지할 수 있고, 금융 거래에서 가상 크리덴셜을 이용할 때에 그 둘의 더욱 용이한 사용자 연관을 가능하게 할 수 있다. 따라서, 일부 실시예들에서, F-PAN의 완전한 버전(예컨대, 실제 크리덴셜 뱅킹 번호)은 디바이스(100) 상에 결코 저장될 수 없으며, 오히려 연관된 D-PAN(예컨대, 링크된 가상 크리덴셜)만이 디바이스(100) 상에 비-해싱된 형태로 저장될 수 있다. 프로비저닝 응답 데이터(560)는 또한 고유 D-PAN 해시(예컨대, D-PAN의 보안을 유지하는 동안에 이 D-PAN을 참조하기 위해 모든 후속 호출들에서 사용될 수 있는 D-PAN의 해싱된 버전을 생성하기 위한, D-PAN의 마지막 4자리 및/또는 임의의 적합한 데이터)를 포함할 수 있다. 프로비저닝 응답 데이터(560)는 또한, "AuthToken" 또는 크리덴셜의 프로비저닝을 인에이블하기 위한 1회 사용 토큰일 수 있는 임의의 다른 적합한 토큰을 포함할 수 있다.

[0033] 다음으로, 크리덴셜 프로비저닝 응답 데이터(560)를 수신하는 것에 응답하여, 상업적 엔티티 서브시스템(400)(예컨대, SMP 브로커 컴포넌트(410))은, 크리덴셜이 그 위에 프로비저닝되도록 적어도 부분적으로 디바이스(100)를 준비시키기 위하여, 그 크리덴셜 프로비저닝 응답 데이터(560)에 포함된 정보의 일부 또는 모두를 디바이스(100)로 전달할 수 있다. 예를 들어, 도 5의 프로세스(500)의 단계(512)에서, 상업적 엔티티 서브시스템(400)(예컨대, SMP 브로커 컴포넌트(410))은 수신된 크리덴셜 프로비저닝 응답 데이터(560)를 분석할 수 있고, 이어서 통과 데이터(pass data)(562)를 생성하고 이를 전자 디바이스(100)로 전송할 수 있다. 그러한 통과 데이터(562)는 프로비저닝될 크리덴셜의 임의의 적합한 디스크립션 또는 식별(예를 들어, 가상 및/또는 실제의(예컨대, D-PAN 및/또는 F-PAN), 크리덴셜의 PAN의 해싱된-버전) 뿐만 아니라, 임의의 연관된 메타데이터를 포함할 수 있으며, 이들 모두는 단계(510)의 크리덴셜 프로비저닝 응답 데이터(560)에 의해 제공될 수 있다. 그러한 통과 데이터(562)는 또한, 크리덴셜이 프로비저닝되어 있을 수 있는 디바이스(100)의 특정 SSD(154)와 연관된 정보(예컨대, 단계(502)의 데이터(552)에 의해 제공된 보안 요소 정보에 기초하여 적어도 부분적으로 결정될 수 있는, 단계(504)에 의해 제공될 수 있는 바와 같은, 특정 SSD(154)의 SSD 식별자)를 포함할 수 있다. 그러한 통과 데이터(562)는 도 1의 통신 경로(65)를 통해 전자 디바이스(100)로 상업적 엔티티 서브시스템(400)에 의해 전송될 수 있다. 예를 들어, 전자 디바이스(100)의 통신 컴포넌트(106)는 임의의 적합한 통신 프로토콜을 이용하여 임의의 적합한 통신 경로(65)를 통해 통과 데이터(562)를 수신하도록 구성될 수 있다.

[0034] 다음으로, 상업적 엔티티 서브시스템(400)으로부터 그러한 통과 데이터(562)를 수신하는 것에 응답하여, 디바이스(100)는 (예를 들어, 디바이스(100)에서 어떠한 요구되는 사용자 상호작용도 없이, 자동으로) 디스에이블된 통과(disabled pass)를 생성하고 이를 NFC 메모리 모듈(150)의 SSD(154)에 추가하도록 구성될 수 있다. 예를 들어, 도 5의 프로세스(500)의 단계(514)에서, 디바이스(100)는 수신된 통과 데이터(562)를 처리할 수 있고, 이어서, "디스에이블된 통과"를 생성하고 이를 NFC 메모리 모듈(150)의 SSD(154)에(예를 들어, 수신된 통과 데이터(562)에 의해 식별될 수 있는 특정 SSD(154)에) 추가할 수 있다. 단계(514)에서, 단계(512)로부터의 통과 데이터(562)는, 예컨대, 시각적 로고들/아이콘들 및/또는 (예컨대, I/O 인터페이스(114a) 상의 디바이스(100)의 Passbook 또는 Wallet 애플리케이션을 통해) 사용자에게 제공될 수 있는 크리덴셜 및 크리덴셜 디스크립터 정보와 연관된 임의의 다른 적합한 사용자 인식가능 데이터를 통해, 디바이스(100)로 하여금 크리덴셜을 디바이스(100)에서 사용 가능한 것으로 보이게 만들도록 할 수 있다.

[0035] 게다가, 단계(510) 전이나, 후에, 또는 그와 적어도 부분적으로 동시에, 금융 기관 서브시스템(350)은 상업적 엔티티 서브시스템(400)에 대한, 이에 따라 디바이스(100)에 대한, 계류 커맨드 입력(put pending commands)의 생성 및 전송을 개시할 수 있다. 예를 들어, 도 5의 프로세스(500)의 단계(516)에서, 금융 기관 서브시스템(350)은 계류 커맨드 입력 데이터(put pending command data)(566)를 생성하고 이를 상업적 엔티티 서브시스템(400)으로(예컨대, 상업적 엔티티 서브시스템(400)의 SMP-TSM 컴포넌트(420)로) 전송할 수 있다. 일부 실시예들에서, 그러한 계류 커맨드 입력 데이터(566)는 프로비저닝되는 크리덴셜의 주 계좌 번호(예컨대, 해싱되거나 해싱되지 않은, D-PAN 또는 F-PAN), SSD 식별자, 및/또는 SSD 카운터를 포함할 수 있다. 이어서, 계류 커맨드 입력 데이터(566)를 수신하는 것에 응답하여, 상업적 엔티티 서브시스템(400)(예컨대, SMP-TSM 컴포넌트(420))은 계류 커맨드 입력 데이터(566)에 기초하여 도 5의 프로세스(500)의 단계(518)에서 통지 데이터(notification data)(568)를 디바이스(100)에 발행할 수 있다. 그러한 계류 커맨드 입력 데이터(566) 및/또는 통지 데이터(568)는 하나 이상의 펄소스크립트(persoScript) 또는 글로벌플랫폼 APDU 스크립트(예를 들어, 임의의 스크립트들, 임의의 회전 키(rotate key)들(예컨대, 필요한 경우에), 및 디바이스(100) 상에 사용가능한 PAN을 프로비저닝하는 데 사용될 수 있는 임의의 다른 적합한 관리 요소들)를 포함할 수 있다. 단계(520)에서, 디바이스(100)는, 단계(518)의 통지 데이터(568)로부터의 수신된 스크립트들 중 임의의 것을 완성하고/하거나, 크리덴셜을 인에이블하기 위한(예를 들어, 디스에이블된/계류중인 활성화 상태로부터 사용을 위한 인에이블된/활성 상태로 크리덴셜을 토글링하기 위한) 임의의 다른 적합한 동작을 행할 수 있다.

[0036] 따라서, 디바이스(100) 상의 보안 요소의 상태(예컨대, 크리덴셜의 PAN이 NFC 컴포넌트(120)에서 사용하기 위해 인에이블되어 있는지의 여부)는 단계(520)에서 크리덴셜의 가용성 상태와 비동기로(예를 들어, 그보다 이후에) 업데이트될 수 있으며, 가용성 상태는 단계(514)에서 디바이스(100)의 사용자에게 제공될 수 있다(예를 들어, I/O 인터페이스(114a) 상의 Passbook 또는 Wallet 애플리케이션에서 시각적으로 제공될 수 있음). 이것은, 크리덴셜이 실제로 사용할 준비가 되기 전에, 디바이스(100)의 사용자에게 사용할 준비가 된 것으로 보이게 할 수 있음으로써, 보다 바람직한 사용자 경험을 제공할 수 있다(예를 들어, 더 빨라 보이는 프로비저닝 시간). 선택된 크리덴셜이 적어도 단계(514)에서 (예를 들어, 실제 크리덴셜 또는 링크된 가상 크리덴셜 중 어느 하나로서) 디바이스(100) 상에서 디스에이블되고/되거나 단계(520)에서 인에이블되면, 디바이스(100)는 크리덴셜이 성공적

으로 프로비저닝되었음을 사용자에게 알릴 수 있는 사용자 인터페이스를 자동으로 생성할 수 있다. 예를 들어, GUI(180)는 I/O 인터페이스(114a) 상에 스크린을 제공할 수 있으며, 여기서 전자 디바이스(100)는 선택된 크리덴셜의 프로비저닝 완료 및 인에이블을 나타내는 메시지를 사용자에게 제공할 수 있다. 대안적으로, 금융 기관 서브시스템(350)은 크리덴셜 프로비저닝 응답 데이터(560) 및 계류 커맨드 데이터(566)의 내용들을, 상이한 단계들에서 데이터의 개별 세트들로서가 아니라 단일 단계(예컨대, 단계(510))에서 동시에 생성하고 이를 전송하도록 구성될 수 있다. 추가적으로 또는 대안적으로, 상업적 엔티티 서브시스템(400)은 통과 데이터(562) 및 통지 데이터(568)의 내용들을, 상이한 단계들에서 데이터의 개별 세트들로서가 아니라 단일 단계(예컨대, 단계(518))에서 동시에 생성하고 이를 전송하도록 구성될 수 있다. 대안적으로 또는 추가적으로, 도 5에 도시되지는 않지만, 추가의 데이터(예컨대, 1회용 패스워드)가 단계(520) 전에 디바이스(100)에 전달될 수 있다. 일부 실시예들에서, 단계들(510 내지 520)의 크리덴셜의 디바이스(100) 상의 프로비저닝은 더 적은 단계들로 조합될 수 있다. 예를 들어, 금융 기관 서브시스템(350)은 상업적 엔티티 서브시스템(400)을 통한 통신 없이 크리덴셜을 디바이스(100) 상으로 직접 프로비저닝하도록 구성될 수 있다(예컨대, 단계들(510, 512, 516, 518)은 임의의 적합한 통신 프로토콜 또는 프로토콜들을 이용하여 (예컨대, 도 1의 통신 경로(75)를 통해) 금융 기관 서브시스템(350)과 디바이스(100) 사이에서 직접적으로 하나 이상의 통신으로 조합될 수 있다). 따라서, 프로세스(500)는 적어도 하나의 선택된 크리덴셜이, 금융 기관 서브시스템(350)에 의해 실제 크리덴셜 또는 실제 크리덴셜에 링크된 가상 크리덴셜 중 하나로서 전자 디바이스(100) 상에 프로비저닝되게 할 수 있다. 게다가, 디바이스(100)는 단계(521)에서 계류 커맨드 처리 데이터(process pending command data)(571)를 생성하고 이를 금융 기관 서브시스템(350)으로 (예컨대, 통신 경로(75)를 통해) 직접적으로 또는 상업적 엔티티 서브시스템(350)을 통해(예컨대, SMP-TSM 컴포넌트(420)를 통해) 간접적으로 전송할 수 있으며, 여기서 계류 커맨드 처리 데이터(571)는 크리덴셜의 프로비저닝이 디바이스(100)에서 완료되었음을 금융 기관 서브시스템(350)에 나타낼 수 있다.

[0037] 크리덴셜이 디바이스(100) 상에서 프로비저닝되고 (예컨대, 단계(520)에서) 인에이블되었으면, 프로세스(500)는 또한 금융 거래에서 그 크리덴셜을 인증하고 사용할 수 있다. 도 1의 시스템(1)을 다시 참조하면, NFC 컴포넌트(120)가 디바이스(100)의 인에이블된 크리덴셜과 연관된 상업 크리덴셜 데이터(예를 들어, 프로세스(500)의 크리덴셜 프로비저닝 단계들(502 내지 520)에 따른 것과 같은, NFC 컴포넌트(120)의 SSD(154)의 인에이블된 애플릿(153)과 연관된 실제의 그리고/또는 가상 상업 크리덴셜 데이터)를 갖는 NFC 통신(15)을 전달하도록 적절하게 인에이블되면, 판매자 서브시스템(200)의 판매자 단말기(220)는 그러한 통신(15)을 수신할 수 있고, 매수 은행 서브시스템(300)은 결과적으로, 그 상업 크리덴셜 데이터의 사용을 인증하고/하거나 금융 기관 서브시스템(350)과의 금융 거래를 완료하기 위해 NFC 통신(15) 중에서 그러한 상업 크리덴셜 데이터를 수신하고 이용할 수 있다. 예를 들어, 전자 디바이스(100)의 사용자가 구매할 제품을 선택하고 결제에 사용될 디바이스(100)의 특정한 프로비저닝된/인에이블된 크리덴셜을 선택한 후에, 디바이스(100)는 도 5의 프로세스(500)의 단계(522)에서, 선택된 크리덴셜에 대한 상업 크리덴셜 데이터를 나타내는 적절한 NFC 통신(15)을 전송하도록 구성될 수 있으며, 판매자 서브시스템(200)의 판매자 단말기(220)는 NFC 통신(15)을 수신하도록 구성될 수 있다. 판매자 서브시스템(200)은, 디바이스(100)가 결제 크리덴셜들을 통신(15)을 통해 판매자 서브시스템(200)으로 제공하는 것에 응답하여 디바이스(100)의 사용자에게 제품 또는 서비스를 제공할 수 있는, 임의의 적합한 판매자(merchant)에 의해 제공될 수 있다. 그러한 수신된 NFC 통신(15)에 기초하여, 판매자 서브시스템(200)(예컨대, 판매자 애플리케이션(203)에 따라 기능할 수 있는 판매자 프로세서(202))은 도 5의 프로세스(500)의 단계(524)에서 (예컨대, 판매자 통신 컴포넌트(206)를 통해) 판매자 시도 구매 데이터(merchant attempted purchase data)(574)를 생성하고 이를 (예컨대, 판매자 서브시스템(200)과 매수 은행 서브시스템(300) 사이의 통신 경로(25)를 통해) 매수 은행 서브시스템(300)으로 전송하도록 구성될 수 있으며, 여기서 판매자 시도 구매 데이터(574)는 사용자의 상업 크리덴셜(예컨대, NFC 통신(15) 중에서 크리덴셜의 PAN) 및 제품 또는 서비스에 대한 판매자의 구매 가격을 나타낼 수 있는 결제 정보 및 인가 요청을 포함할 수 있다. 결제 프로세서 또는 매수자(acquirer)로도 알려진, 매수 은행 서브시스템(300)은 판매자 서브시스템(200)과 연관된 판매자의 은행 파트너일 수 있고, 매수 은행 서브시스템(300)은 금융 기관 서브시스템(350)과 협력하여, 전자 디바이스(100)에 의해 판매자 서브시스템(200)과의 NFC 통신(15)을 통해 시도된 크리덴셜 거래들을 승인 및 결제하도록 구성될 수 있다. 단계(524)에서 판매자 시도 구매 데이터(574)를 수신하는 것에 응답하여, 매수 은행 서브시스템(300)은 이어서 도 5의 프로세스(500)의 단계(526)에서 (예컨대, 매수 은행 서브시스템(300)과 금융 기관 서브시스템(350) 사이의 통신 경로(35)를 통해) 시도 구매 데이터(574)로부터의 인가 요청을 금융 기관 서브시스템(350)으로 매수 은행 시도 구매 데이터(acquiring bank attempted purchase data)(576)로서 포워드할 수 있으며, 여기서 매수 은행 시도 구매 데이터(576)는, 사용자의 상업 크리덴셜(예컨대, NFC 통신(15) 중에서 크리덴셜의 PAN) 및

제품 또는 서비스에 대한 판매자의 구매 가격을 나타낼 수 있는 결제 정보 및 인가 요청, 및/또는 매수 은행 서브시스템(300)에 대한 판매자의 은행 계좌를 나타내는 정보를 포함할 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.

[0038] 금융 기관 서브시스템(350)이 (예컨대, 매수 은행 시도 구매 데이터(576)로서 매수 은행 서브시스템(300)으로부터) 인가 요청을 수신하는 경우, 결제 정보는 식별된 상업 크리덴셜이 금융 거래에서 사용하기 위해 인증되었는지 여부를 결정하기 위해 도 5의 프로세스(500)의 단계(528)에서 금융 기관 서브시스템(350)에 의해 분석될 수 있다. 예를 들어, 디바이스(100)로부터 전송되고 매수 은행 시도 구매 데이터(576)에 포함된 통신(15) 중에서 상업 크리덴셜 정보가 가상 크리덴셜(예컨대, D-PAN)을 나타내는 경우, 금융 기관 서브시스템(350)은, (예컨대, 거래에 실제로 자금을 제공하기 위해) 연관된 실제 크리덴셜이 시도된 금융 거래 동안 사용되게 할 수 있기 전에 가상 크리덴셜과 그것의 연관된 실제 크리덴셜(즉, 그것의 연관된 F-PAN) 사이의 링크가 하나 이상의 적합한 방식으로 인증되었는지 여부를 결정하기 위하여, 가상-링킹 데이터 구조(352) 또는 임의의 다른 적합한 데이터를 참고하거나 달리 레버리지할 수 있다. (예를 들어, 디바이스(100) 상에 연관된 가상 크리덴셜을 프로비저닝하는 동안에 단계(502)에서 또는 다른 곳에서 개인 사용자-식별가능 정보(personal user-identifiable information)를 디바이스(100)로부터 금융 기관 서브시스템(350)으로(예컨대, 발행 은행 서브시스템(370)으로) 제공함으로써 - 여기서, 그러한 개인 사용자-식별가능 정보는 실제 크리덴셜과 연관되어 발행 은행 서브시스템(370)에 이미 알려진 검증된 사용자 정보에 기초하여 발행 은행 서브시스템(370)에 의해 인증될 수 있음) 디바이스(100) 상의 연관된 가상 크리덴셜의 프로비저닝 동안에 사용자가 단계(502)에서 선택된 실제 크리덴셜의 정당한 소유자임을 인증하도록 디바이스(100)의 사용자에게 요구하기보다는, 프로세스(500)는 시도된 금융 거래 동안에(예를 들어, 가상 크리덴셜이 디바이스(100) 상에 프로비저닝된 후, 예컨대 단계(521) 후에) 디바이스(100)의 사용자로 하여금, 사용자가 프로비저닝된 가상 크리덴셜과 연관된 실제 크리덴셜의 정당한 소유자임을 인증할 수 있게 하도록 구성될 수 있다. 따라서, 가상 크리덴셜이 사용자의 디바이스(100) 상에 프로비저닝된 후 실제 크리덴셜로 가상 크리덴셜의 사용자를 인증하기 위한 하나 이상의 방식이 프로세스(500)에 의해 제공될 수 있으며, 여기서 그러한 인증은 프로비저닝된 가상 크리덴셜을 이용하는 시도된 금융 거래 동안에 일어날 수 있다.

[0039] 언급한 바와 같이, (예를 들어, 매수 은행 시도 구매 데이터(576)로서 매수 은행 서브시스템(300)으로부터의) 인가 요청에서 가상 상업 크리덴셜 데이터를 수신하는 것에 응답하여, 금융 기관 서브시스템(350)은, 가상 크리덴셜과 그것의 연관된 실제 크리덴셜(즉, 그것의 연관된 F-PAN) 사이의 링크가 가상 크리덴셜이 금융 거래에서 사용될 수 있도록 하나 이상의 적합한 방식으로 인증되었는지 여부를 결정하기 위하여, 가상-링킹 데이터 구조(352) 또는 임의의 다른 적합한 데이터를 레버리지할 수 있다. 예를 들어, 도 7에 도시된 바와 같이, 그리고 도 5a의 프로세스(500')에 관하여 아래에서 더욱 상세히 기술되는 바와 같이, 데이터 구조(352)는 하나 이상의 엔트리(702)를 포함할 수 있으며, 여기서 각각의 엔트리(702)는 (예컨대, 단계(508)에서 생성될 수 있는 바와 같은) 실제 크리덴셜 또는 F-PAN(706)과 링크된 특정 가상 크리덴셜 또는 D-PAN(704)을 포함할 수 있다. 게다가, 도 7에 도시된 바와 같이, 데이터 구조(352)의 각 엔트리(702)는 링크 인증 상태(708)를 포함할 수 있으며, 이는, 그 엔트리(702)의 가상 크리덴셜 또는 D-PAN(704)과 실제 크리덴셜 또는 F-PAN(706) 사이의 링크가, 가상 크리덴셜이 금융 거래에서 사용될 수 있도록, 현재 인증되어 있는지 여부를 나타낼 수 있다. 특정 가상 크리덴셜 또는 D-PAN(704)이 초기에 데이터 구조(352)의 새로운 엔트리(702) 내의 실제 크리덴셜 또는 F-PAN(706)과 링크되는 경우(예를 들어, 프로세스(500)의 단계(508)에서 디바이스(100) 상의 그 가상 크리덴셜의 프로비저닝 동안에), 그 엔트리(702)의 링크 인증 상태(708)는 초기에 (예컨대, 엔트리(702a)에 의해 도시된 바와 같이) "인증되지 않음(not authenticated)"으로 설정될 수 있으며, 그것에 의하여 그러한 상태는 나중에 (예컨대, 프로세스(500)의 단계(528)에서 시도된 금융 거래 동안에) 금융 기관 서브시스템(350)에 의해 액세스되어, 그 엔트리(702)의 특정 가상 크리덴셜 또는 D-PAN(704)과 실제 크리덴셜 또는 F-PAN(706) 사이의 링크가, 특정 가상 크리덴셜 또는 D-PAN(704)이 시도된 금융 거래를 완료하는 데 사용될 수 있기 전에 그리고/또는 그 엔트리(702)의 링크 인증 상태(708)가 (예컨대, 엔트리(702b)에 도시된 바와 같이) "인증됨(authenticated)"으로 업데이트될 수 있기 전에, 인증되어야 한다고 결정할 수 있다. 데이터 구조(352)는 임의의 적합한 방법으로 시스템(1)에(예컨대, 금융 기관 서브시스템(350)에) 액세스가능할 수 있는 임의의 적합한 데이터베이스 또는 임의의 적합한 순서화된 데이터 저장소일 수 있다.

[0040] 따라서, (예를 들어, 매수 은행 시도 구매 데이터(576)로서 매수 은행 서브시스템(300)으로부터의) 인가 요청에

서 가상 상업 크리덴셜 데이터를 수신하는 것에 응답하여, 금융 기관 서브시스템(350)은 프로세스(500)의 단계(528)에서 가상-링킹 데이터 구조(352)를 레버리지하여, (예컨대, 특정 엔트리(702)의 매칭되는 D-PAN(704)에 의해 나타내어진 바와 같은) 그 가상 크리덴셜과 (예컨대, 그 엔트리(702)의 F-PAN(706)에 의해 나타나는 바와 같은) 그것의 연관된 실제 크리덴셜 사이의 링크가 (예컨대, 그 엔트리(702)의 링크 인증 상태(708)에 의해 나타내어진 바와 같이) 인증되었는지 여부를 결정할 수 있다. 단계(528)에서, 시도된 금융 거래에서 식별된 가상 크리덴셜과, 연관된 실제 크리덴셜 사이의 링크가 인증된다고 결정되는 경우, 프로세스(500)는 단계(538)로 건너뛸 수 있고, 그것에 의하여 그 연관된 실제 크리덴셜은 아래에서 더 상세히 기술되는 바와 같이 금융 거래에 자금을 제공하는 데 사용될 수 있다. 그러나, 단계(528)에서, 시도된 금융 거래에서 식별된 가상 크리덴셜과, 연관된 실제 크리덴셜 사이의 링크가 인증되지 않는다고 결정되는 경우, 프로세스(500)는 단계(530)로 진행할 수 있고, 그것에 의하여 시스템(1)은 그 링크를 적절하게 인증하려고 시도할 수 있다.

[0041] 전자 디바이스(100) 상에 프로비저닝된 가상 크리덴셜과 연관된 실제 크리덴셜 사이의 링크는 다양한 적합한 방법으로 인증될 수 있다. 예를 들어, 일부 실시예들에서, 금융 기관 서브시스템(350)은, 링크된 실제 크리덴셜에 대한 사용자의 적절한 인증을 할 수 있는 적합한 정보를 디바이스(100)의 사용자로부터 획득하려고 시도하기 위하여, 판매자 서브시스템(200)을 레버리지할 수 있다. 도 5에 도시된 바와 같이, 프로세스(500)의 단계(530)에서, 금융 기관 서브시스템은 인증 요청 데이터(authentication request data)(580)를 생성하고 이를 판매자 서브시스템(200)으로, 직접적으로(예컨대, 임의의 적합한 통신 프로토콜을 이용해 도 1의 통신 경로(85)를 통해) 또는 매수 은행 서브시스템(300)을 통해 간접적으로(예컨대, 임의의 적합한 통신 프로토콜 또는 프로토콜들을 이용해 도 1의 통신 경로들(35, 25)을 통해) 전송할 수 있다. 인증 요청 데이터(580)는 특정한 목표 판매자 서브시스템(target merchant subsystem)(200)을 식별할 수 있는 단순한 명령일 수 있다(예를 들어, 동일한 판매자 단말기 서브시스템(200)은 판매자 시도 구매 데이터(574)를 매수 은행 서브시스템(300)으로 전송했으며, 이는 금융 기관 서브시스템(350)에 의해 수신되고 이전 단계(528) 동안에 의존되는 매수 은행 시도 구매 데이터(576)를 생성함). 대안적으로 또는 추가적으로, 인증 요청 데이터(580)는 링크를 인증하는 데 사용될 수 있는 하나 이상의 대답을 구하는 하나 이상의 질문 또는 프롬프트를 설명하는 정보(예컨대, "사용되고 있는 크리덴셜과 연관된 PIN을 입력하세요", "당신의 어머니의 결혼 전 성은 무엇입니까" 등)를 포함할 수 있다. 대안적으로 또는 추가적으로, 인증 요청 데이터(580)는, 단계(528)에서 그것의 비-인증된 링크가 식별된 가상 크리덴셜 및 실제 크리덴셜 중 하나 또는 둘 다를 나타내는 정보(예컨대, D-PAN(704)의 완전한 또는 해싱된 버전 및/또는 F-PAN(706)의 완전한 또는 해싱된 버전)를 포함할 수 있다.

[0042] 다음으로, (예컨대, 도 1의 판매자 통신 컴포넌트(206)에서) 그러한 인증 요청 데이터(580)를 수신하는 것에 응답하여, 판매자 서브시스템(200)은 인증 요청에 응답하는 정보를 제공하도록 디바이스(100)의 사용자에게 프롬프트하도록 구성될 수 있다. 예를 들어, 프로세스(500)의 단계(532)에서, 판매자 서브시스템(200)은 인증 정보에 대한 요청을 디바이스(100)의 사용자에게 디스플레이하거나 다른 식으로 전달하도록 구성될 수 있다(예를 들어, 단계(522)에서 디바이스(100)가 판매자 서브시스템(200)으로 NFC 통신(15)을 최근에 전송한 것으로 인하여, 디바이스(100)의 사용자가 판매자 서브시스템(200)에 근접해 있을 수 있다고 가정될 수 있음에 따라, 판매자 I/O 인터페이스(214)를 통해). 단지 하나의 예로서, 판매자 I/O 인터페이스(214)는 도 3의 디바이스(100)의 터치 스크린 I/O 인터페이스(114a)와 유사할 수 있으며, 여기서 판매자 I/O 인터페이스(214)는 디바이스(100)의 사용자에게 하나 이상의 질문을 디스플레이하고 그 판매자 I/O 인터페이스(214)에서 사용자 입력을 통해 그러한 사용자로부터 응답을 수신하도록 구성될 수 있다. 단계(532)에서 제기된 하나 이상의 질문은, 사용자로 하여금, 단계(528)에서 식별된 실제 크리덴셜과 연관되어 금융 기관 서브시스템(350)에 이미 알려진 검증된 사용자 정보에 기초하여 금융 기관 서브시스템(350)(예컨대, 발행 은행 서브시스템(370))에 의해 인증될 수 있는 개인 사용자-식별가능 정보(예컨대, 개인 식별 번호("PIN"), 사용자의 어머니의 결혼 전 성, 또는 금융 기관 서브시스템(350)이 이미 실제 크리덴셜과 연관시켰을 수 있는 임의의 다른 적합한 개인 정보)를 입력할 것을 요청할 수 있다. 단계(532)에서 제기된 하나 이상의 질문은, 단계(528)에서 그것의 비-인증된 링크가 식별된 가상 크리덴셜 및 실제 크리덴셜 중 하나 또는 둘 다(예컨대, D-PAN(704)의 완전한 또는 해싱된 버전 및/또는 F-PAN(706)의 완전한 또는 해싱된 버전)를 식별할 수 있으며, 이는 제공될 정확한 인증 정보를 사용자가 재수집하도록 도울 수 있다.

[0043] 다음으로, 단계(532)에서 (예컨대, 판매자 I/O 인터페이스(214)를 통해) 그러한 사용자 인증 정보를 수신하는 것에 응답하여, 판매자 서브시스템(200)은 사용자의 응답을 나타내는 데이터를 생성하고 이를 금융 기관 서브시스템(350)으로 전송하도록 구성될 수 있다. 예를 들어, 프로세스(500)의 단계(534)에서, 판매자 서브시스템(200)은 사용자의 인증 정보를 나타내는 인증 응답 데이터(584)를 생성하고 이를 (예컨대, 판매자 통신 컴포넌트(206)를 통해) 금융 기관 서브시스템(350)으로 다시, 직접적으로(예컨대, 임의의 적합한 통신 프로토콜을 이

용해 도 1의 통신 경로(85)를 통해) 또는 매수 은행 서브시스템(300)을 통해 간접적으로(예컨대, 임의의 적합한 통신 프로토콜 또는 프로토콜들을 이용해 도 1의 통신 경로들(25, 35)을 통해), 전송하도록 구성될 수 있다. 인증 응답 데이터(584)는, 판매자 서브시스템(200)이 단계(532)에서 사용자에게 인증 정보에 대해 프롬프트하는 것에 응답하여 디바이스(100)의 사용자에 의해 판매자 서브시스템(200)에 제공된 인증 정보를 나타내는 임의의 적합한 데이터일 수 있다. 예를 들어, 일부 실시예들에서, 인증 응답 데이터(584)는, 단계(532)에서 디바이스(100)의 사용자로부터 수신된 하나 이상의 대답뿐만 아니라, 단계(528)에서 그것의 비-인증된 링크가 식별된 가상 크리덴셜 및 실제 크리덴셜 중 하나 또는 둘 다의 식별(예컨대, D-PAN(704)의 완전한 또는 해싱된 버전 및/또는 F-PAN(706)의 완전한 또는 해싱된 버전)을 포함할 수 있다. 일부 다른 실시예들에서, 인증 요청(580)은 금융 기관 서브시스템(350)으로부터 전자 디바이스(100)로 전송되어서, 디바이스(100)가, 단계(532)에서의 인증 요청에 응답하는 정보를 제공하도록 디바이스(100)의 사용자에게 프롬프트하도록 구성될 수 있고, 이어서 디바이스(100)가 사용자의 응답을 나타내는 인증 응답 데이터(584)를 생성하고 이를 금융 기관 서브시스템(350)으로 다시 전송하도록 구성될 수 있다. 또 다른 실시예들에서, 인증 요청(580)은 금융 기관 서브시스템(350)으로부터 판매자 서브시스템(200)으로 전송될 수 있고, 이어서 판매자 서브시스템(200)은 그 요청(580)의 적어도 일부분을 전자 디바이스(100)로 포워드할 수 있어서, 디바이스(100)(및/또는 디바이스(100)와 판매자 서브시스템(200))는 단계(532)에서의 인증 요청에 응답하는 정보를 제공하도록 디바이스(100)의 사용자에게 프롬프트하도록 구성될 수 있고, 이어서 디바이스(100)는 사용자의 응답을 나타내는 인증 응답 데이터(584)를 생성하고 이를, 금융 기관 서브시스템(350)에 최종적으로 포워드하기 위해, 판매자 서브시스템(200)으로 다시 전송하도록 구성될 수 있다.

[0044] 다음으로, 판매자 서브시스템(200)으로부터 그러한 인증 응답 데이터(584)를 수신하는 것에 응답하여, 금융 기관 서브시스템(350)은, 사용자의 대답(들)이 단계(528)에서 식별된 실제 크리덴셜 또는 F-PAN(706)에 대해서 사용자를 적절히 인증할 수 있고 따라서 단계(528)에서 식별된 실제 크리덴셜과 가상 크리덴셜 사이의 비-인증된 링크를 적절히 인증할 수 있는지 여부를 결정하도록 구성될 수 있다. 예를 들어, 프로세스(500)의 단계(536)에서, 금융 기관 서브시스템(350)은, 판매자 서브시스템(200)으로부터 인증 응답 데이터(584)를 수신하고, (예를 들어, 인증 응답 데이터(584)의 사용자의 응답과, 단계(528)에서 식별된 실제 크리덴셜과 연관되어 금융 기관 서브시스템(350)에 이미 알려진 검증된 사용자 정보(예컨대, 실제 크리덴셜을 그것의 정당한 사용자에게 처음에 발행한 발행 은행 서브시스템(370)에 의해 이미 알려지고 그에 액세스가능할 수 있는, 특정한 검증된 사용자 정보)를 비교함으로써) 그 인증 응답 데이터(584)에 의해 제공된 사용자의 대답(들)이 단계(528)에서 식별된 실제 크리덴셜 또는 F-PAN(706)에 대해서 사용자를 인증하는 데 사용될 수 있는지 여부를 결정하도록 구성될 수 있다. 단계(536)에서, 인증 응답 데이터(584)가 단계(528)에서 식별된 실제 크리덴셜로 디바이스(100)의 사용자를 인증할 수 없다고 금융 기관 서브시스템(350)에 의해 결정되는 경우, 단계(528)에서 또한 식별된 그 실제 크리덴셜과 특정 가상 크리덴셜 사이의 링크는 (예를 들어, 그 실제 크리덴셜과 그 가상 크리덴셜을 링크시키는 데이터 구조(352)의 적절한 엔트리(702)의 링크 인증 상태(708)를 "인증되지 않음"으로 유지함으로써) 비-인증된 상태로 남아있을 수 있고, 이어서 프로세스(500)는 다시 한번 링크를 인증하려고 시도하기 위하여 단계(530)로 복귀할 수 있거나 또는 프로세스(500)는 임의의 다른 적합한 동작 과정으로 진행할 수 있다. 그러나, 단계(536)에서, 인증 응답 데이터(584)가 단계(528)에서 식별된 실제 크리덴셜로 디바이스(100)의 사용자를 인증할 수 있다고 금융 기관 서브시스템(350)에 의해 결정되는 경우, 단계(528)에서 또한 식별된 그 실제 크리덴셜과 특정 가상 크리덴셜 사이의 링크는 (예를 들어, 그 실제 크리덴셜과 그 가상 크리덴셜을 링크시키는 데이터 구조(352)의 적절한 엔트리(702)의 링크 인증 상태(708)를 "인증되지 않음"에서 "인증됨"으로 업데이트함으로써) 인증될 수 있고, 프로세스(500)는 단계(538)로 진행할 수 있으며, 그것에 의하여 그 연관되고 인증된 실제 크리덴셜은 금융 거래에 자금을 제공하는 데 사용될 수 있다. 따라서, (예컨대, 단계(502)에서) 실제 크리덴셜이 디바이스(100) 상의 크리덴셜 프로비저닝을 위한 기초로서 식별될 수 있고, 이어서 (예컨대, 단계(508)에서) 가상 크리덴셜이 그 실제 크리덴셜과 연관되거나 링크될 수 있으며, 이어서 (예컨대, 단계들(510 내지 520)에서) 그 가상 크리덴셜은 디바이스(100) 상에 프로비저닝될 수 있으며, 여기서 그러한 프로비저닝은, 그 가상 크리덴셜 및 실제 크리덴셜 사이의 링크를 인증하기 위한 그리고/또는 실제 크리덴셜에 대한 사용자의 연관을 인증하기 위한 어떠한 정보도 디바이스(100) 또는 디바이스(100)의 사용자가 제공하지 않으면서, 일어날 수 있다. 이어서, 실제 크리덴셜이 식별된 후, 가상 크리덴셜이 그 실제 크리덴셜과 연관되거나 링크된 후, 그리고 그 가상 크리덴셜이 디바이스(100) 상에 프로비저닝된 후에, 그 가상 크리덴셜과 그 실제 크리덴셜 사이의 링크가 (예컨대, 단계들(528 내지 536)에서) 인증될 수 있다. 그러한 인증은 디바이스(100)와의 어떠한 상호작용(예를 들어, 임의의 사용자 상호작용, 및/또는 시스템(1)의 임의의 서브시스템과 디바이스(100) 간의 임의의 통신)도 요구하지 않을 수 있다. 게다가, 그러한 인증은, 디바이스(100) 상의 데이터

의 어떠한 변경, 디바이스(100)로부터 데이터의 어떠한 제거, 및/또는 디바이스(100)에 대한 데이터의 어떠한 추가도 요구하지 않을 수 있다.

[0045] 단계(536)에서 수신된 인증 응답 데이터(584)를 분석하는 것에 응답하여, 다양한 다른 유형들의 데이터가 금융 기관 서브시스템(350)에 의해 생성되고/되거나 (예컨대, 데이터 구조(352)에) 저장될 수 있다. 예를 들어, 도 7에 도시된 바와 같이, 데이터 구조(352)의 각 엔트리(702)는 인증 데이터(710)를 포함할 수 있으며, 이는 그 엔트리(702)의 D-PAN(704)과 F-PAN(706) 사이의 링크의 인증과 연관된 임의의 적합한 유형의 정보 또는 다수의 유형들의 정보를 나타낼 수 있다. 단지 하나의 예로서, 특정 엔트리(702)에 대한 인증 데이터(710)(예컨대, 엔트리(702a)에 대한 <인증1(AUTHENTICATION1)> 데이터(710))는 그 엔트리(702)에 대한 링크가 인증된 시간(예컨대, 그 엔트리(702)에 대한 링크 인증 상태(708)가 "인증되지 않음"에서 "인증됨"으로 변경된 시간)을 나타낼 수 있으며, 여기서 그러한 인증 데이터(710)는 금융 기관 서브시스템(350)에 의해 임의의 적합한 방식으로 엔트리(702)의 인증 상태(708)를 관리하는 데 이용될 수 있다(예를 들어, 엔트리(702)의 인증 상태(708)는, 그 엔트리가 마지막으로 인증된 이래로 특정 양의 시간이 경과한 경우, 자동으로 "인증됨"에서 "인증되지 않음"으로 변경될 수 있다). 이는 금융 기관 서브시스템(350)으로 하여금, 크리덴셜의 사용자 인증을 임의의 적합한 시간 간격으로 일상적으로 요구하게 하도록 할 수 있다. 추가적으로 또는 대안적으로, 특정 엔트리(702)에 대한 인증 데이터(710)는 그 엔트리(702)에 대해 몇 번의 실패된 인증 시도들이 발생했는지를 나타낼 수 있으며(예컨대, 단계(536)가, 의도된 엔트리(702)의 링크를 인증하기 위해, 수신된 인증 응답 데이터(584)를 사용할 수 없었던 횟수), 여기서 그러한 인증 데이터(710)는 금융 기관 서브시스템(350)에 의해 그 엔트리(702)의 링크를 유지하거나, 삭제하거나, 또는 달리 조정하는 데 이용될 수 있다(예를 들어, 특정 D-PAN(704)을 특정 F-PAN(706)에 링크시키는 엔트리(702)는, 그 링크에 대해 특정 수의 실패된 인증 시도들이 발생했을 경우에, 데이터 구조(352)로부터 삭제될 수 있다). 이는 금융 기관 서브시스템(350)으로 하여금, 사용자가 소정 수의 시도들 후에 실제 크리덴셜로 그것의 링크를 인증할 수 없는 경우, 이전에 프로비저닝된 가상 크리덴셜을 쓸모없게(useless) 만들도록 할 수 있다.

[0046] 금융 기관 서브시스템(350)이, (예를 들어, 단계(528) 및/또는 단계(536)에서 데이터 구조(352)를 레버리징하는 것을 통해) (예컨대, 매수 은행 시도 구매 데이터(576)의) 특정 가상 크리덴셜과 연관된 실제 크리덴셜 사이의 인증된 링크를 식별하면, 프로세스(500)는 단계(538)로 진행할 수 있으며, 그것에 의하여 그 연관된 실제 크리덴셜은 금융 기관 서브시스템(350)에 의해 요청된 금융 거래에 자금을 제공하려고 시도하는 데 사용될 수 있다. 예를 들어, 금융 기관 서브시스템(350)이 테이블(352)을 레버리지하여 디바이스(100)와 판매자 단말기(220) 사이의 NFC 통신(15) 중의 상업 크리덴셜 정보가 실제 크리덴셜(예컨대, 데이터 구조(352)의 연관된 F-PAN(706))에 대한 인증된 링크를 갖는 가상 크리덴셜(예컨대, 데이터 구조(352)의 D-PAN(704))을 나타낸다고 결정할 수 있는 경우, 이어서 금융 기관 서브시스템(350)은 단계(538)에서, 실제 크리덴셜 또는 F-PAN(706)과 연관된 계좌가 (예를 들어, 매수 은행 시도 구매 데이터(576)에 의해 식별될 수 있는 바와 같이) 시도된 금융 거래의 구매금액(purchase amount)을 커버할 만큼 충분한 신용을 갖는지 여부를 결정할 수 있다. 충분한 자금이 존재하지 않는 경우, 금융 기관 서브시스템(350)은 단계(538)에서 매수 은행 서브시스템(300)으로 부정적인 인가 응답 데이터(588)를 전송함으로써 요청된 거래를 거절할 수 있다. 그러나, 충분한 자금이 존재하는 경우, 금융 기관 서브시스템(350)은 단계(538)에서 매수 은행 서브시스템(300)으로 긍정적인 인가 응답 데이터(588)를 전송함으로써 요청된 거래를 승인할 수 있고, 금융 거래가 완료될 수 있다. 어느 유형의 인가 응답이든, 도 5의 프로세스(500)의 단계(538)에서 (예컨대, 임의의 적합한 통신 프로토콜을 이용해 통신 경로(35)를 통해) 인가 응답 데이터(588)로서 매수 은행 서브시스템(300)으로 금융 기관 서브시스템(350)에 의해 제공될 수 있다. 이어서, 그러한 인가 응답 데이터(588)는 (예컨대, 실제 상업 크리덴셜 또는 F-PAN(706)과 연관된 계좌로부터의 자금으로 매수 은행 서브시스템(300)에서 판매자 서브시스템(200)의 판매자의 은행 계좌에 신용을 적용하기 위해) 매수 은행 서브시스템(300)에 의해 이용될 수 있고, 연관된 인가 응답 데이터(589)는 도 5의 프로세스(500)의 단계(539)에서 인가 응답 데이터(388)에 기초하여 (예를 들어, 통신 경로(25)를 통해) 판매자 서브시스템(200)으로 매수 은행 서브시스템(300)에 의해 제공될 수 있으며, 여기서 금융 거래를 나타내는 임의의 적합한 데이터는 이어서 판매자 서브시스템(200)을 통해(예컨대, 판매자 I/O 인터페이스(214)를 통해) 디바이스(100)의 사용자에게 제공될 수 있다.

[0047] 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.

[0048] 도 5a의 설명

[0049] 언급한 바와 같이, 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 있으며, 여기서 결제 네트워크 서브시스템(360) 및 발행 은행 서브시스템(370)은 단일 엔티티 또는 별개의 엔티티들일 수 있다. 예를 들어, 아메리칸 익스프레스는 결제 네트워크 서브시스템(360) 및 발행 은행 서브시스템(370) 둘 다일 수 있다. 그에 반해, 비자 및 마스터카드는 결제 네트워크 서브시스템들(360)일 수 있고, 체이스, 웰스 파고, 뱅크 오브 아메리카 등과 같은 발행 은행 서브시스템들(370)과 협력하여 동작할 수 있다. 결제 네트워크 서브시스템(360) 및 발행 은행 서브시스템(370)이 별개의 엔티티들인 경우들에서, 결제 네트워크 서브시스템(360)과 발행 은행 서브시스템(370)은 가상 크리덴셜과 실제 크리덴셜 사이의 링크의 적절한 인증을 보장하기 위해 그리고/또는 금융 거래를 완료하기 위해 서로 통신할 수 있다. 예를 들어, 도 5a에 도시된 바와 같이, 프로세스(500A)는 도 5의 프로세스(500)와 유사할 수 있지만, 다만 특정 금융 기관 서브시스템(350)의 특정 결제 네트워크 서브시스템(360)과 특정 발행 은행 서브시스템(370) 사이의 다양한 통신들을 갖는다. 프로세스(500A)는 시스템(1)의 다양한 요소들(예컨대, 판매자 서브시스템(200), 매수 은행 서브시스템(300), 특정 결제 네트워크 서브시스템(360), 및 특정 발행 은행 서브시스템(370))에 의해 구현되는 것으로 도시되지만, 프로세스(500A)는 임의의 다른 적합한 컴포넌트들 또는 서브시스템들을 이용해 구현될 수 있다.

[0050] 도 5a에 도시된 바와 같이, 프로세스(500A)의 단계들(524 내지 534)은 전술한 프로세스(500)의 단계들(524 내지 534)과 실질적으로 유사하거나 동일할 수 있다. 예를 들어, 도시된 바와 같이, 결제 네트워크 서브시스템(360)은 단계(526)에서 매수 은행 서브시스템(300)으로부터 전송된 매수 은행 시도 구매 데이터(576)를 수신하고, 단계(528)에서 (예컨대, 데이터 구조(352)를 레버리지함으로써) 데이터(576)의 가상 크리덴셜과 실제 크리덴셜 사이의 링크가 금융 거래에서 사용하기 위해 인증되었는지 여부를 결정하고, 단계(530)에서 인증 요청 데이터(580)를 전송하고, 그리고/또는 단계(534)에서 전송된 인증 응답 데이터(584)를 수신하도록 구성될 수 있다. 게다가, 프로세스(500A)의 단계들(538, 539)은 전술한 프로세스(500)의 단계들(538, 539)과 실질적으로 유사하거나 동일할 수 있다. 예를 들어, 도 5a에 도시된 바와 같이, 결제 네트워크 서브시스템(360)은 단계(538)에서 인가 응답 데이터(588)를 매수 은행 서브시스템(300)으로 전송하도록 구성될 수 있다. 그러나, 도 5a에 또한 도시된 바와 같이, 단계(534)에서 결제 네트워크 서브시스템(360)이 판매자 서브시스템(200)으로부터 인증 응답 데이터(584)를 수신한 이후에, 그러나 단계(538)에서 결제 네트워크 서브시스템(360)이 인가 응답 데이터(588)를 매수 은행 서브시스템(300)으로 전송하기 전에, 프로세스(500')는 단계들(536a 내지 536e)을 포함할 수 있으며, 여기서 결제 네트워크 서브시스템(360)과 특정 발행 은행 서브시스템(370)은 가상 크리덴셜과 실제 크리덴셜 사이의 링크의 적절한 인증을 보장하기 위해 그리고/또는 금융 거래를 완료하기 위해 협력할 수 있다.

[0051] 프로세스(500)에서와 같이, (예를 들어, 디바이스(100) 상의 연관된 가상 크리덴셜의 프로비저닝 동안에 개인 사용자-식별가능 정보를 디바이스(100)로부터 금융 기관 서브시스템(350)으로 제공함으로써 - 여기서, 그러한 개인 사용자-식별가능 정보는 실제 크리덴셜과 연관되어 금융 기관 서브시스템(350)에 이미 알려진 검증된 사용자 정보에 기초하여 금융 기관 서브시스템(350)에 의해 인증될 수 있음) 디바이스(100) 상의 연관된 가상 크리덴셜의 프로비저닝 동안에 사용자가 선택된 실제 크리덴셜의 정당한 소유자임을 인증하도록 디바이스(100)의 사용자에게 요구하기보다는, 프로세스(500A)는 시도된 금융 거래 동안에 디바이스(100)의 사용자로 하여금, 사용자가 프로비저닝된 가상 크리덴셜과 연관된 실제 크리덴셜의 정당한 소유자임을 인증할 수 있게 하도록 구성될 수 있다. 그러나, 결제 네트워크 서브시스템(360)이 시스템(1)에서, (예를 들어, (예컨대, 금융 거래들 동안에) 다양한 발행 은행들(370) 및/또는 다양한 매수 은행들(300)에 대한 통합관리자(aggregator)로서 역할을 함으로써 금융 기관 서브시스템(350)의 직접적인 통합 지점(integration point)들을 최소화하기 위하여) 발행 은행 서브시스템(370)과 다양한 매수 은행 서브시스템들(300) 사이의 인터페이스로서, 그리고/또는 (예를 들어, (예컨대, 크리덴셜 프로비저닝 동안에) 다양한 발행 은행들(370) 및/또는 다양한 상업적 엔티티 서브시스템들(400)/디바이스들(100)에 대한 통합관리자로서 역할을 함으로써 금융 기관 서브시스템(350)의 직접적인 통합 지점들을 최소화하기 위하여) 발행 은행 서브시스템(370)과 다양한 상업적 엔티티 서브시스템들(400)/디바이스들(100) 사이의 인터페이스로서 제공될 수 있는 경우에, 실제 크리덴셜과 연관된 검증된 개인 사용자-식별가능 정보가 결제 네트워크 서브시스템(360)에 액세스가능하지 않을 수 있으므로, 그러한 결제 네트워크 서브시스템(360)이 사용자를 실제 크리덴셜로 인증하는 것은 어려울 수 있다(예를 들어, 실제 크리덴셜과 연관된 그러한 검증된 개인 사용자-식별가능 정보는 그 실제 크리덴셜을 처음에 발행한 특정 발행 은행 서브시스템(370)에 의해서만 액세스가능할 수 있음). 따라서, 프로세스(500A)의 단계들(536a 내지 536e)에 의해 도시된 바와 같이, 결제 네트워크 서브시스템(360)과 특정 발행 은행 서브시스템(370)은, 가상 크리덴셜과 실제 크리덴셜 사이의 링크의 적절한 인증을 보장하기 위해 그리고/또는 금융 거래를 완료하기 위해 협력할 수 있다.

[0052] 프로세스(500)의 단계(536a)에서, 결제 네트워크 서브시스템(360)은, 판매자 서브시스템(200)으로부터 인증 응답 데이터(584)를 수신하고, 예를 들어, 단계(528)에서 식별된 D-PAN(704)을 포함할 수 있는 데이터 구조(352)

의 적절한 엔트리(702)에 그러한 인증 응답 데이터(584)를 저장함으로써, 그러한 인증 응답 데이터(584)를 적절한 실제 크리덴셜(예컨대, 단계(528)에서 식별된 F-PAN(706))과 연관시키도록 구성될 수 있다. 다음으로, 단계(536b)에서, 결제 네트워크 서브시스템(360)은 인증/거래 요청 데이터(586b)를 특정 발행 은행 서브시스템(370)으로 (예컨대, 임의의 적합한 통신 프로토콜을 이용해 도 1의 통신 경로(45)를 통해) 전송하도록 구성될 수 있으며, 여기서 특정 발행 은행 서브시스템은, 실제 크리덴셜(예컨대, 단계(528)에서 식별된 F-PAN(706))을 발행할 책임이 있는 발행 은행 서브시스템으로서 (예컨대, 단계(536a)에서) 결제 네트워크 서브시스템(360)에 의해 식별될 수 있다. 그러한 인증/거래 요청 데이터(586b)는 인증 응답 데이터(584), 실제 크리덴셜(예컨대, 단계(528)에서 식별된 F-PAN(706))의 식별뿐만 아니라, 시도된 구매 데이터(576)로부터의 임의의 적합한 정보(예컨대, 시도된 금융 거래의 중심에서 제품 또는 서비스에 대한 판매자의 구매 가격)를 포함할 수 있다. 다음으로, 단계(536c)에서, 특정 발행 은행 서브시스템(370)은 그러한 인증/거래 요청 데이터(586b)를 수신하고, 실제 크리덴셜(예컨대, 단계(528)에서 식별된 F-PAN(706))이 시도된 금융 거래(예컨대, (예를 들어, 데이터 구조(352)에서) 결제 네트워크 서브시스템(360)에 의해 그 실제 크리덴셜과 연관된 가상 크리덴셜을 이용하는, 시도된 금융 거래)에서 사용하기 위해 인증되어야 하는지 여부를 결정할 수 있다. 예를 들어, 발행 은행 서브시스템(370)은, 그러한 인증/거래 요청 데이터(586b)를 수신하고, 사용자의 인증 응답 데이터(584) 및 인증/거래 요청 데이터(586b)의 F-PAN(706)을, 그 F-PAN(706)에 대해 발행 은행 서브시스템(370)에 의해 이미 알려지고 그에 액세스가능할 수 있는 특정한 검증된 사용자 정보와 비교하도록 구성될 수 있다. 예를 들어, 그러한 검증된 사용자 정보는 디바이스(100)의 메모리 컴포넌트(104)와 유사할 수 있는 발행 은행 서브시스템(370)의 임의의 적합한 메모리 컴포넌트에 저장될 수 있으며, 여기서 그러한 검증된 사용자 정보는 발행 은행 서브시스템(370)에 의해 다른 서브시스템들과 공유되지 않을 수 있다(예를 들어, 발행 은행 서브시스템(370)은 그러한 검증된 사용자 정보를 결제 네트워크 서브시스템(360)과 공유하지 않을 수 있다).

[0053] 단계(536c)에서 발행 은행 서브시스템(370)에 의해, 인증/거래 요청 데이터(586b)에 의해 식별된 인증 응답 데이터(584)가 인증/거래 요청 데이터(586b)에 의해 식별된 실제 크리덴셜 또는 F-PAN(706)을 인증할 수 없다고 결정되는 경우, 이어서 발행 은행 서브시스템(370)은 단계(536d)에서 제1 유형의 인증/거래 응답 데이터(586d)를 생성하고 이를 결제 네트워크 서브시스템(360)으로 (예컨대, 임의의 적합한 통신 프로토콜을 이용해 도 1의 통신 경로(45)를 통해) 전송할 수 있다. 이러한 제1 유형의 인증/거래 응답 데이터(586d)는 인증 응답 데이터(584)가 실제 크리덴셜 또는 F-PAN(706)을 인증할 수 없다는 발행 은행 서브시스템(370)에 의한 결정을 나타낼 수 있으며, 결제 네트워크 서브시스템(360)은 단계(536e)에서 그러한 제1 유형의 인증/거래 응답 데이터(586d)를 수신하고 이용할 수 있다. 결제 네트워크 서브시스템(360)은 단계(536e)에서 이러한 제1 유형의 인증/거래 응답 데이터(586d)를 이용하여, (예를 들어, 그 실제 크리덴셜과 특정 가상 크리덴셜을 링크시키는 데이터 구조(352)의 적절한 엔트리(702)의 링크 인증 상태(708)를 "인증되지 않음"으로 설정 또는 유지함으로써) 단계(528)에서 또한 식별된 그 실제 크리덴셜 또는 F-PAN(706)과 그 가상 크리덴셜 사이의 링크가 비-인증되는 것을 보장할 수 있다. 이어서, 프로세스(500A)는 링크를 인증하려고 다시 한번 시도하기 위하여 단계(530)로 복귀할 수 있거나, 또는 프로세스(500A)는 임의의 다른 적합한 동작 과정으로 진행할 수 있다.

[0054] 그러나, 단계(536c)에서 발행 은행 서브시스템(370)에 의해, 인증/거래 요청 데이터(586b)에 의해 식별된 인증 응답 데이터(584)가 인증/거래 요청 데이터(586b)에 의해 식별된 실제 크리덴셜 또는 F-PAN(706)을 인증할 수 있다고 결정되는 경우, 이어서 발행 은행 서브시스템(370)은 또한 단계(536c)에서, 그 실제 크리덴셜 또는 F-PAN(706)과 연관된 계좌가 (예를 들어, 인증/거래 요청 데이터(586b)에 의해 식별될 수 있는 바와 같이) 시도된 금융 거래의 구매금액을 커버할 만큼 충분한 신용을 갖는지 여부를 결정할 수 있다. 발행 은행 서브시스템(370)이 단계(536c)에서 충분한 자금이 존재하지 않는다고 결정하는 경우, 금융 기관 서브시스템(350)은 단계(536d)에서 제2 유형의 인증/거래 응답 데이터(586d)를 생성하고 이를 결제 네트워크 서브시스템(360)으로 (예컨대, 임의의 적합한 통신 프로토콜을 이용해 도 1의 통신 경로(45)를 통해) 전송함으로써 요청된 거래를 거절할 수 있다. 이러한 제2 유형의 인증/거래 응답 데이터(586d)는, 인증 응답 데이터(584)가 실제 크리덴셜 또는 F-PAN(706)을 인증할 수는 있지만 연관된 계정이 시도된 거래에 자금을 제공할 수 없다는, 발행 은행 서브시스템(370)에 의한 결정을 나타낼 수 있으며, 결제 네트워크 서브시스템(360)은 단계(536e)에서 그러한 제2 유형의 인증/거래 응답 데이터(586d)를 수신하고 이용할 수 있다. 결제 네트워크 서브시스템(360)은 단계(536e)에서 이러한 제2 유형의 인증/거래 응답 데이터(586d)를 이용하여, (예를 들어, 그 실제 크리덴셜과 특정 가상 크리덴셜을 링크시키는 데이터 구조(352)의 적절한 엔트리(702)의 링크 인증 상태(708)를 "인증됨"으로 설정함으로써) 단계(528)에서 또한 식별된 그 실제 크리덴셜 또는 F-PAN(706)과 그 가상 크리덴셜 사이의 링크가 인증되는 것을 보장할 수 있다. 이어서, 프로세스(500A)는 단계(538)로 진행할 수 있으며, 그것에 의하여 결제 네트워크 서브시스템(360)은 매수 은행 서브시스템(300)으로 부정적인 인가 응답 데이터(588)를 전송함으로써 요청된 거

래를 거절할 수 있다.

[0055] 그러나, 단계(536c)에서 발행 은행 서브시스템(370)에 의해, 인증/거래 요청 데이터(586b)에 의해 식별된 인증 응답 데이터(584)가 인증/거래 요청 데이터(586b)에 의해 식별된 실제 크리덴셜 또는 F-PAN(706)을 인증할 수 있고 시도된 금융 거래의 구매금액을 커버할 만큼 충분한 자금이 존재한다고 결정되는 경우, 금융 기관 서브시스템(350)은 단계(536d)에서 제3 유형의 인증/거래 응답 데이터(586d)를 생성하고 이를 결제 네트워크 서브시스템(360)으로 (예컨대, 임의의 적합한 통신 프로토콜을 이용해 도 1의 통신 경로(45)를 통해) 전송함으로써 요청된 거래를 수락할 수 있다. 이러한 제3 유형의 인증/거래 응답 데이터(586d)는, 인증 응답 데이터(584)가 실제 크리덴셜 또는 F-PAN(706)을 인증할 수 있고 연관된 계정이 시도된 거래에 자금을 제공할 수 있다는, 발행 은행 서브시스템(370)에 의한 결정을 나타낼 수 있으며, 결제 네트워크 서브시스템(360)은 단계(536e)에서 그러한 제3 유형의 인증/거래 응답 데이터(586d)를 수신하고 이용할 수 있다. 결제 네트워크 서브시스템(360)은 단계(536e)에서 이러한 제3 유형의 인증/거래 응답 데이터(586d)를 이용하여, (예를 들어, 그 실제 크리덴셜과 특정 가상 크리덴셜을 링크시키는 데이터 구조(352)의 적절한 엔트리(702)의 링크 인증 상태(708)를 "인증됨"으로 설정함으로써) 단계(528)에서 또한 식별된 그 실제 크리덴셜 또는 F-PAN(706)과 그 가상 크리덴셜 사이의 링크가 인증되는 것을 보장할 수 있다. 이어서, 프로세스(500A)는 단계(538)로 진행할 수 있으며, 그것에 의하여 결제 네트워크 서브시스템(360)은 매수 은행 서브시스템(300)으로 긍정적인 인가 응답 데이터(588)를 전송함으로써 요청된 거래를 수락할 수 있다.

[0056] 게다가, 일부 실시예들에서, 단계(526)에서 매수 은행 시도 구매 데이터 또는 인가 요청(576)을 수신하는 것에 응답하여 단계(530)에서 인증 요청(580)을 생성하기 전에, 결제 네트워크 서브시스템(360)은 인가 요청(576)에 의해 식별된 D-PAN에 링크된 F-PAN과 연관될 수 있는 소정의 인증 요청 데이터를 발행 은행 서브시스템(370)으로부터 요청할 수 있다. 즉, 식별된 D-PAN과 링크된 F-PAN 사이의 링크를 인증하기 위해 사용자로부터 인증 데이터를 얻으려는 시도에서 인증 요청(580)을 판매자 서브시스템(200)에 전달하기 전에, 결제 네트워크 서브시스템(360)은 발행 은행 서브시스템(370)으로부터, 링크를 인증하는 데 사용될 수 있는 보안 데이터와 같은, 링크를 인증하는 데 사용될 수 있는 F-PAN에 관하여 발행 은행 서브시스템(370)에 알려진 유형의 정보(예컨대, F-PAN의 소유자의 알려진 결혼 전 성 등)를 요청할 수 있고, 결제 네트워크 서브시스템(360)은 이어서 발행 은행 서브시스템(370)으로부터의 그 정보를 레버리지하여, (예를 들어, 단계(526)와 단계(530) 사이에 단계들(536a 내지 536e)과 유사한 단계들을 제공함으로써) 적절하고 효과적인 인증 요청(580)을 생성할 수 있다.

[0057] 도 5a의 프로세스(500A)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.

[0058] 도 6의 설명

[0059] 도 6은 전자 디바이스 상에 크리덴셜을 프로비저닝하기 위한 예시적인 프로세스(600)의 흐름도이다. 단계(602)에서, 프로세스(600)는 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 생성할 수 있다. 예를 들어, 도 5 및 도 5a에 관하여 전술한 바와 같이, 금융 기관 서브시스템(350)은 프로세스(500)의 단계(508)에서 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 생성하도록 구성될 수 있다. 다음으로, 단계(604)에서, 링크가 생성된 후, 프로세스(600)는 전자 디바이스 상의 가상 상업 크리덴셜의 프로비저닝을 가능하게 할 수 있다. 예를 들어, 도 5 및 도 5a에 관하여 전술한 바와 같이, 금융 기관 서브시스템(350)은 단계(508)에서 링크된 가상 크리덴셜의 전자 디바이스(100) 상으로의 프로비저닝을 직접적으로 그리고/또는 프로세스(500)의 단계들(510 내지 520)에서 상업적 엔티티 서브시스템(400)을 통해 가능하게 하도록 구성될 수 있다. 다음으로, 단계(606)에서, 프로비저닝하는 단계 후, 프로세스(600)는 실제 상업 크리덴셜과 가상 상업 크리덴셜 사이의 링크를 인증할 수 있다. 예를 들어, 도 5 및 도 5a에 관하여 전술한 바와 같이, 금융 기관 서브시스템(350)은 프로세스(500)의 단계(536) 및/또는 프로세스(500A)의 단계들(536a 내지 536e)에서 가상 상업 크리덴셜과 실제 상업 크리덴셜 사이의 이전에 생성된 링크를 인증하도록 구성될 수 있다.

[0060] 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.

[0061] 도 7의 설명

[0062] 언급한 바와 같이, 도 7은, 전자 디바이스(100) 상에서 크리덴셜들을 프로비저닝하고/하거나 인증하는 데 사용하기 위해 데이터를 하나 이상의 엔트리(702)에 저장할 수 있는 도 1의 시스템의 예시적인 데이터 구조(352)를 도시한다. 데이터 구조(352)가 도 7의 예에서 관계형 데이터베이스의 테이블의 형태를 취할 수 있지만, 임의의

다른 데이터 구조가 다른 실시예들에서 사용될 수 있다. 데이터 구조(352)는 다양한 유형의 정보를 저장할 수 있으며, 금융 기관 서브시스템(예컨대, 결제 네트워크 서브시스템(360)(예를 들어, 디바이스(100)의 메모리 컴포넌트(104)와 유사할 수 있는 결제 네트워크 서브시스템(360)의 메모리 컴포넌트 내)) 상에 저장되거나 그에 의해 달리 액세스가능할 수 있다. 도시된 바와 같이, 엔트리들(702a 내지 702d) 각각은, D-PAN 열(704), F-PAN 열(706), 링크 인증 상태 열(708), 및 인증 데이터 열(710)의 각각에 걸쳐 이어지는 자신의 행을 포함할 수 있다. D-PAN 열(704)의 각 행은, 하나의 D-PAN 또는 가상 크리덴셜을 데이터 구조(352) 내의 다른 것과 구별할 수 있는 고유 값 또는 고유 값과 연관된 식별자를 포함할 수 있다. 예를 들어, 도시된 바와 같이, 엔트리(702a)에 대한 열(704)의 제1 가상 크리덴셜 "D-PAN1"은 고유 식별자 또는 고유 D-PAN(예컨대, 12345678)을 가질 수 있고, 엔트리(702b)에 대한 열(704)의 제2 가상 크리덴셜 "D-PAN2"은 고유 식별자 또는 고유 D-PAN(예컨대, 34567812)을 가질 수 있고, 엔트리(702c)에 대한 열(704)의 제3 가상 크리덴셜 "D-PAN3"은 고유 식별자 또는 고유 D-PAN(예컨대, 56781234)을 가질 수 있고, 엔트리(702d)에 대한 열(704)의 제4 가상 크리덴셜 "D-PAN4"은 고유 식별자 또는 고유 D-PAN(예컨대, 78123456)을 가질 수 있다.

[0063] 데이터 구조(352)의 각 엔트리(702)는 열(704)의 고유 D-PAN과 연관될 수 있지만, 2개 이상의 엔트리(702)는 열(706)의 동일한 실제 크리덴셜 또는 F-PAN과 연관될 수 있다. 예를 들어, 도시된 바와 같이, 엔트리(702a)에 대한 열(706)의 제1 실제 크리덴셜 "F-PAN1"은 식별자 또는 F-PAN(예컨대, 23456781)을 가질 수 있고, 엔트리(702b)에 대한 열(706)의 제2 실제 크리덴셜 "F-PAN2"은 식별자 또는 F-PAN(예컨대, 45678123)을 가질 수 있는 한편, 열(706)의 제3 실제 크리덴셜 "F-PAN3"은 엔트리들(702c, 702d) 각각에 대해 식별자 또는 F-PAN(예컨대, 67812345)을 가질 수 있다. 즉, 단일의 실제 크리덴셜(즉, "F-PAN3")이 데이터 구조(352)의 2개의 상이한 엔트리들(즉, 엔트리들(702c, 702d))의 2개의 상이한 가상 크리덴셜들(즉, "D-PAN3", "D-PAN4")과 링크될 수 있어서, 사용자는 제1 디바이스(100) 상에 제1 가상 크리덴셜을 프로비저닝하고 제2 디바이스(100) 상에 제2 가상 크리덴셜을 프로비저닝할 수 있으며, 여기서 두 가상 크리덴셜은 동일한 단일의 실제 크리덴셜에 링크된다.

[0064] 링크 인증 상태 열(708)의 각 행은, 그 동일한 행에 대한(예컨대, 그 특정 엔트리(702)에 대한) 열(704)의 D-PAN과 열(706)의 F-PAN 사이의 링크가 "인증됨" 또는 "인증되지 않음"을 나타낼 수 있는 값 또는 값과 연관된 식별자를 포함할 수 있다. 도 7에 도시된 바와 같이, 예를 들어, 단일의 실제 크리덴셜(즉, "F-PAN3")은 데이터 구조(352)의 두 상이한 엔트리(즉, 엔트리들(702c, 702d))의 두 상이한 가상 크리덴셜(즉, "D-PAN3", "D-PAN4")과 링크될 수 있지만, 그 링크들 중 하나는 인증될 수 있는 한편 다른 것은 인증되지 않을 수 있다(예를 들어, F-PAN3과 D-PAN3 사이의 링크는 인증될 수 있는 한편 F-PAN3과 D-PAN4 사이의 링크는 인증되지 않을 수 있다). 언급한 바와 같이 다양한 유형의 인증 데이터가 각 엔트리(702)와 연관될 수 있다. 예를 들어, 인증 데이터 열(710)의 각 행은 하나 이상의 적합한 유형의 정보를 나타낼 수 있는 값 또는 값과 연관된 식별자를 포함할 수 있다(예를 들어, 엔트리(702a)에 대한 <인증1>, 엔트리(702b)에 대한 <인증2>, 엔트리(702c)에 대한 <인증3>, 및 엔트리(702d)에 대한 <인증4>).

[0065] 도 2 및 도 3의 추가 설명

[0066] 언급한 바와 같이, 그리고 도 2에 도시된 바와 같이, 전자 디바이스(100)는, 음악 재생기(예컨대, 미국 캘리포니아주 쿠퍼티노 소재의 애플 사에 의해 입수가능한 아이팟™), 비디오 재생기, 스틸 이미지 재생기, 게임 재생기, 기타 미디어 재생기, 음악 레코더, 영화 또는 비디오 카메라 또는 레코더, 스틸 카메라, 기타 미디어 레코더, 라디오, 의료 장비, 가전제품, 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), 붐 박스, 모뎀, 라우터, 프린터, 또는 이들의 임의의 조합을 포함할 수 있지만, 이들로 제한되지 않는다. 일부 실시예들에서, 전자 디바이스(100)는 단일 기능을 수행할 수 있고(예컨대, 금융 거래를 이행하는 것에 전용되는 디바이스), 다른 실시예들에서, 전자 디바이스(100)는 다수의 기능을 수행할 수 있다(예컨대, 금융 거래를 이행하고, 음악을 재생하고, 전화 통화를 수신 및 전송하는 디바이스). 전자 디바이스(100)는 사용자가 어디로 이동하든지 금융 거래를 이행하도록 구성될 수 있는 임의의 휴대용, 모바일, 핸드헬드, 또는 소형 전자 디바이스일 수 있다. 일부 소형 전자 디바이스들은 아이팟™과 같은 핸드헬드 전자 디바이스의 폼 팩터보다 작은 폼 팩터를 가질 수 있다. 예시적인 소형 전자 디바이스들은, 시계, 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.

[0067] 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.

[0068] 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, 선호도 정보(예컨대, 미디어 재생 선호도), 생활방식 정보(예컨대, 음식 선호도), 운동 정보(예컨대, 운동 모니터링 장비에 의해 획득된 정보), 거래 정보(예컨대, 신용 카드 정보와 같은 정보), 무선 접속 정보(예컨대, 디바이스(100)가 무선 접속을 설정할 수 있게 하는 정보), 가입 정보(예컨대, 사용자가 가입한 팟캐스트들 또는 텔레비전 쇼들 또는 다른 미디어의 추적을 유지하는 정보), 연락처 정보(예컨대, 전화번호들 및 이메일 주소들), 달력 정보, 임의의 다른 적합한 데이터, 또는 이들의 조합을 저장할 수 있다.

[0069] 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 ㎒, 2.4 ㎓, 및 5.6 ㎓ 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 쉘 프로토콜("SSH"), 무선 분산 시스템("WDS") 브리징, 무선 및 셀룰러 전화 및 개인용 이메일 디바이스에 의해 사용될 수 있는 임의의 통신 프로토콜(예컨대, 모바일 통신용 글로벌 시스템("GSM"), "EDGE"(GSM plus Enhanced Data rates for GSM Evolution), 코드 분할 다중 접속("CDMA"), 직교 주파수-분할 다중 접속("OFDMA"), 고속 패킷 접속("HSPA"), 다중-대역 등), 저전력 무선 근거리 개인 통신망("6LoWPAN") 모듈에 의해 사용될 수 있는 임의의 통신 프로토콜, 임의의 다른 통신 프로토콜, 또는 이들의 임의의 조합을 지원할 수 있다. 통신 컴포넌트(106)는 또한, 디바이스(100)가 다른 디바이스(예컨대, 호스트 컴퓨터 또는 액세서리 디바이스)에 통신가능하게 연결되고 무선으로 또는 유선 접속을 통해(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 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.

[0070] 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 있

다(예를 들어, 디바이스(100)가 휴대용 디바이스로서 동작하고 있는 경우). 예를 들어, 전원 공급장치(108)는 배터리(예컨대, 젤, 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.

[0071] 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.

[0072] 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.

[0073] 특정 예로서, 전자 디바이스(100)는 출력 컴포넌트(112)로서 디스플레이 출력 컴포넌트를 포함할 수 있다. 그러한 디스플레이 출력 컴포넌트는 시각적 데이터를 사용자에게 제시하기 위한 임의의 적합한 유형의 디스플레이 또는 인터페이스를 포함할 수 있다. 디스플레이 출력 컴포넌트는 디바이스(100)에 임베드되거나 디바이스(100)에 연결된 디스플레이(예컨대, 탈착가능한 디스플레이)를 포함할 수 있다. 디스플레이 출력 컴포넌트는, 예를 들어, 액정 디스플레이("LCD"), 발광 다이오드("LED") 디스플레이, 유기 발광 다이오드("OLED") 디스플레이, 면전도 전자총 디스플레이("SED"), 탄소 나노튜브 디스플레이, 나노크리스탈 디스플레이, 임의의 다른 적합한 유형의 디스플레이, 또는 이들의 조합을 포함할 수 있다. 대안적으로, 디스플레이 출력 컴포넌트는, 예를 들어, 비디오 프로젝터, 전방 디스플레이(head-up display), 또는 3차원(예컨대, 홀로그래픽) 디스플레이와 같은, 전자 디바이스(100)로부터 멀리 떨어진 표면 상에 콘텐츠의 디스플레이를 제공하기 위한 이동가능한 디스플레이 또는 프로젝션 시스템을 포함할 수 있다. 다른 예로서, 디스플레이 출력 컴포넌트는, 컴팩트 디지털 카메라, 반사 카메라, 또는 임의의 다른 적합한 스틸 또는 비디오 카메라에서 발견되는 유형의 뷰파인더와 같은, 디지털 또는 기계적 뷰파인더를 포함할 수 있다. 디스플레이 출력 컴포넌트는 디스플레이 드라이버 회로, 디스플레이 드라이버들을 구동하기 위한 회로, 또는 둘 다를 포함할 수 있으며, 그러한 디스플레이 출력 컴포넌트는, 프로세서(102)의 지시 하에 있을 수 있는 콘텐츠(예컨대, 미디어 재생 정보, 전자 디바이스(100) 상에서 구현되는 애플리케이션들을 위한 애플리케이션 스크린들, 진행중인 통신 동작들에 관한 정보, 유입 통신 요청들에 관한 정보, 디바이스 동작 스크린들 등)를 디스플레이하도록 동작할 수 있다.

[0074] 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.

[0075] 전자 디바이스(100)의 프로세서(102)는 전자 디바이스(100)의 하나 이상의 컴포넌트의 동작들 및 성능을 제어하

도록 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(113)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.

[0076] 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 근접-기반 거래들 또는 통신들(15)을 가능하게 할 수 있는 임의의 적합한 근접-기반 통신 메커니즘일 수 있다. NFC 컴포넌트(120)는 비교적 낮은 데이터 레이트들(예컨대, 424 kbps)에서 가까운 범위의 통신을 허용할 수 있으며, ISO/IEC 7816, ISO/IEC 18092, ECMA-340, ISO/IEC 21481, ECMA-352, ISO 14443, 및/또는 ISO 15693과 같은 임의의 적합한 표준들을 따를 수 있다. 대안적으로 또는 추가적으로, NFC 컴포넌트(120)는 비교적 높은 데이터 레이트들(예컨대, 370 Mbps)에서 가까운 범위의 통신을 허용할 수 있으며, 트랜스퍼젯(TransferJet)™ 프로토콜과 같은 임의의 적합한 표준들을 따를 수 있다. NFC 컴포넌트(120)와 판매자 서브시스템(200) 사이의 통신은 디바이스(100)와 판매자 서브시스템(200) 사이의 임의의 적합한 가까운 범위의 거리(예컨대, 도 1의 거리 D를 참조) 내에서, 예컨대 대략 2 내지 4 센티미터의 범위 내에서 일어날 수 있으며, 임의의 적합한 주파수(예컨대, 13.56 ㎒)에서 동작할 수 있다. 예를 들어, NFC 컴포넌트(120)의 그러한 가까운 범위의 통신은 자기장 유도를 통해 발생할 수 있으며, 이는 NFC 컴포넌트(120)가 다른 NFC 디바이스들과 통신하고/하거나 무선 주파수 식별("RFID") 회로를 갖는 태그들로부터 정보를 검색하게 할 수 있다. NFC 컴포넌트(120)는 상품 정보를 획득하고, 결제 정보를 전송하고, 외부 디바이스(예컨대, 판매자 서브시스템(200)의 단말기(220))와 다른 식으로 통신하는 방식을 제공할 수 있다.

[0077] NFC 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200) 사이에서 비접촉식 근접-기반 통신(15)을 가능하게 하기 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 NFC 메모리 모듈(150)을 포함할 수 있다.

[0078] NFC 디바이스 모듈(130)은 NFC 데이터 모듈(132), NFC 안테나(134), 및 NFC 부스터(136)를 포함할 수 있다. NFC 데이터 모듈(132)은, NFC 컴포넌트(120)에 의해 판매자 서브시스템(200)으로 비접촉식 근접-기반 또는 NFC 통신(15)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 근접-기반 통신(15)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.

[0079] 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 통신(15)의 전달을 가능하게 할 수 있는, 임의의 적합한 안테나 또는 다른 적합한 송수신기 회로일 수 있다. 따라서, NFC 안테나(134)(예컨대, 루프 안테나)는 특히 NFC 컴포넌트(120)의 비접촉식 근접-기반 통신 기능들을 가능하게 하기 위해 제공될 수 있다.

[0080] 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 레버리지하여 전자 디바이스(100)와 다른 원격 엔티티 사이의 Wi-Fi, 블루투스™, 셀룰러, 또는 GPS 통신을 가능하게 할 수 있는 한편, NFC 컴포넌트(120)는 안테나(116)를 레버리지하여 NFC 디바이스 모듈(130)의 NFC 데이터 모듈(132)과 다른 엔티티(예컨대, 판매자 서브시스템(200))

사이의 비접촉식 근접-기반 또는 NFC 통신(15)을 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 통신(15)으로서 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 근접-기반 또는 NFC 통신(15)을 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 있다).

[0081] 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 통신(15)을 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 wallet 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.

[0082] 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)으부터) NFC 데이터 모듈(132)로의 정보(예컨대, 통신(15))를 판독하기 위한 판독기/기록기 모드, 다른 NFC 인에이블된 디바이스(예컨대, 판매자 서브시스템(200))와 데이터(예컨대, 통신(15))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(15))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.

[0083] 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) 사이의 NFC 통신(15)을 허용할 수 있다. NFC 메모리 모듈(150)은 NFC 디바이스 하드웨어 내에 또는 NFC 집적회로("IC") 내에 임베드될 수 있다. NFC 메모리 모듈(150)은 변조 금지일 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, 변조 금지일 수 있는 보안 요소의 적어도 일부분을 제공할 수 있다. 예를 들어, 그러한 보안 요소는, 잘-식별된 신뢰 기관들의 세트에 의해 제시될 수 있는 규칙들 및 보안 요건들(예컨대, 금융 기관 서브시스템의 권한 및/또는 글로벌플랫폼과 같은 산업 표준)에 따라 애플리케이션들 및 그것들의 기밀의 암호화 데이터(예컨대, 애플릿(153) 및 키(155))를 안전

하게 호스팅할 수 있는 변조-금지 플랫폼을 (예컨대, 단일의 또는 다중 칩 보안 마이크로컨트롤러로서) 제공하도록 구성될 수 있다. NFC 메모리 모듈(150)은 메모리(104)의 일부분, 또는 NFC 컴포넌트(120)에 대해 특정한 적어도 하나의 전용 칩일 수 있다. NFC 메모리 모듈(150)은 전자 디바이스(100)의 마더보드 상의 전용 칩인 SIM 상에, 또는 메모리 카드 내의 외부 플러그로서 상주할 수 있다. NFC 메모리 모듈(150)은 NFC 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.

[0084] 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("TSMSD") 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 기관이, 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 크리덴셜들)을 생성하거나 다른 식으로 전자 디바이스(100) 상에 프로비저닝하기 위한 키들 및/또는 다른 적합한 정보를 저장할 수 있는, NFC 메모리 모듈(150)의 일부분일 수 있다. 특정한 보충적 보안 도메인("SSD")(154)(예컨대, SSD들(154 내지 154b) 중 하나)은, 전자 디바이스(100)에 특정 특권들 또는 결제 권리들을 제공할 수 있는 특정 크리덴셜(예컨대, 특정 신용 카드 크리덴셜 또는 특정 대중 교통 카드 크리덴셜)과 연관될 수 있다. 각각의 SSD(154)는 자신의 애플리케이션 또는 애플릿(153)에 대한 자신의 관리자 키(155)를 가질 수 있으며, 이는 전자 디바이스(100)와 판매자 서브시스템(200) 사이의 NFC 통신(15)으로서 NFC 디바이스 모듈(130)에 의한 사용을 위해 그 SSD(154)의 특정 크리덴셜을 인에이블하도록 활성화될 필요가 있을 수 있다. 예를 들어, 특정 SSD(154)는 특정 신용 카드 크리덴셜과 연관될 수 있다. 그러나, 그 특정 크리덴셜은, 그 특정 SSD(154)의 특정 애플릿(153)이 그러한 사용을 위해 인에이블되거나 달리 활성화 또는 잠금해제되었을 때에만, NFC 컴포넌트(120)에 의해 판매자 서브시스템(200)으로 NFC 통신(15)으로서 전달될 수 있다(예를 들어, 그 특정 크리덴셜은 NFC 데이터 모듈(132)에 의해서만 액세스가능할 수 있다). 보안 특징들은 NFC 컴포넌트(120)의 사용을 인에이블하기 위해 제공될 수 있으며, 이는 크리덴셜의 신용 카드 정보 또는 은행 계좌 정보와 같은 기밀 결제 정보를 전자 디바이스(100)로부터 판매자 서브시스템(200)으로 NFC 통신(15)으로서 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, 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.

[0085] NFC 컴포넌트(120)가 근거리 통신에 관하여 기술되었지만, 컴포넌트(120)는 전자 디바이스(100)와 판매자 서브시스템(200) 사이의 임의의 적합한 비접촉식 근접-기반 모바일 결제 또는 임의의 다른 적합한 유형의 비접촉식 근접-기반 통신(15)을 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.

[0086] 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).

[0087] 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 디스에이블할 수 있는 2-위치 슬라이더를 포함할 수 있다. 입력 컴포넌트들(110d, 110e)은 음량 출력 또는 전자 디바이스(100)의 출력 컴포넌트(112)의 임의의

다른 특성 출력을 증가 및 감소시키기 위한 버튼들을 포함할 수 있다. 입력 컴포넌트들(110a 내지 110e) 각각은 기계적 입력 컴포넌트, 예컨대 돔 스위치에 의해 지지되는 버튼, 슬라이딩 스위치, 제어 패드, 키, 노브(knob), 스크롤 휠, 또는 임의의 다른 적합한 형태일 수 있다.

[0088] 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(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 내비게이팅하는 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.

[0089] 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, "설정 어시스턴트" 텍스트 표시자(181)로 라벨링된 특정 아이콘(182)(즉, 특정 아이콘(183))이 선택되면, 디바이스(100)는 특정 설정 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 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. 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.

[0090] 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 쿠퍼티노 소재의 애플사의 라이트닝(Lightning)™ 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.

[0091] 전자 디바이스(100)는 또한, 적어도 하나의 햅틱 또는 촉각적 출력 컴포넌트(112c)(예컨대, 럼블러), 카메라 및/또는 스캐너 입력 컴포넌트(110h)(예컨대, 비디오 또는 스틸 카메라, 및/또는 바코드 스캐너 또는 바코드, QR 코드 등과 같은 코드로부터 제품 식별 정보를 획득할 수 있는 임의의 다른 적합한 스캐너), 및 생체인식 입력 컴포넌트(110i)(예컨대, 사용자를 인증하기 위해 전자 디바이스(100)에 액세스가능할 수 있는 특징-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 일부분은 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.

[0092] 게다가, 도 1 내지 도 7에 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 있다). 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.

[0093] 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 모듈은 하나 이상의 특정한 태스크를 수행할 수 있거나 하나 이상의 특정한 추상 데이터 형(abstract 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.

[0094] 시스템(1)의 모듈들 또는 컴포넌트들 또는 서브시스템들 중 하나 이상의 적어도 일부분은, 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 엔티티에 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.

[0095] 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.

[0096] 언급한 바와 같이, 디바이스(100)의 입력 컴포넌트(110)(예컨대, 입력 컴포넌트(110f))는, 유선 또는 무선 버스(118)를 통해 디바이스(100)의 다른 컴포넌트들과 상호작용하기 위해 터치 입력을 수신할 수 있는 터치 입력 컴포넌트를 포함할 수 있다. 그러한 터치 입력 컴포넌트(110)는, 키보드, 마우스 등과 같은 다른 입력 컴포넌트들을 대신하여 또는 그것들과 조합하여 사용자 입력을 디바이스(100)에 제공하는 데 사용될 수 있다.

[0097] 터치 입력 컴포넌트(110)는 전체적으로 또는 부분적으로 투명한, 반투명한, 불투명한, 또는 이들의 임의의 조합일 수 있는 터치 감응형 패널을 포함할 수 있다. 터치 입력 컴포넌트(110)는 터치 스크린, 터치 패드, 터치 패드로서 기능하는 터치 스크린(예를 들어, 랩톱의 터치 패드를 대체하는 터치 스크린), 임의의 다른 입력 디바이스와 조합되거나 통합된 터치 스크린 또는 터치 패드(예를 들어, 키보드 상에 배치된 터치 스크린 또는 터치 패드), 또는 터치 입력을 수신하기 위한 터치 감응형 표면을 갖는 임의의 다차원 물체로 구현될 수 있다. 일부 실시예들에서, 터치 스크린 및 터치 패드라는 용어들은 상호교환가능하게 사용될 수 있다.

[0098] 일부 실시예들에서, 터치 스크린으로서 구현되는 터치 입력 컴포넌트(110)는 디스플레이의 적어도 일부분 위에, 아래에, 그리고/또는 그 내에 부분적으로 또는 전체적으로 위치하는 투명한 그리고/또는 반투명한 터치 감응형 패널을 포함할 수 있다(예를 들어, 디스플레이 출력 컴포넌트(112a)). 다른 실시예들에서, 터치 입력 컴포넌트(110)는, 터치 감응형 컴포넌트들/디바이스들이 디스플레이 컴포넌트들/디바이스들과 통합되는, 통합형 터치 스크린으로서 구현될 수 있다. 또 다른 실시예들에서, 터치 입력 컴포넌트(110)는, 보충적인 그래픽 데이터 또는 주 디스플레이와 동일한 그래픽 데이터를 디스플레이하기 위한 보충적인 또는 추가적인 디스플레이 스크린으로서 그리고 터치 입력을 수신하기 위해 사용될 수 있다.

[0099] 터치 입력 컴포넌트(110)는, 용량성, 저항성, 광학적, 음향적, 유도성, 기계적, 화학적 측정, 또는 입력 컴포넌트(110)에 근접한 하나 이상의 터치 혹은 준터치(near touch)의 발생들에 대하여 측정될 수 있는 임의의 현상에 기초하여, 하나 이상의 터치 또는 준터치의 위치를 검출하도록 구성될 수 있다. 소프트웨어, 하드웨어, 펌웨어 또는 이들의 임의의 조합이, 검출된 터치들의 측정들을 처리하여 하나 이상의 제스처를 식별하고 추적하는 데 사용될 수 있다. 제스처는 터치 입력 컴포넌트(110) 상의 정지된 또는 정지되지 않은, 단일 또는 다중의, 터치들 또는 준터치들에 대응할 수 있다. 본질적으로 동시에, 인접하게, 또는 연속하여, 두드리거나, 누르거나, 흔들거나, 문지르거나, 회전시키거나, 비틀거나, 배향을 바꾸거나, 변화하는 압력으로 누르는 것 등에 의한 것과 같이, 터치 입력 컴포넌트(110) 상에서 특정 방식으로 하나 이상의 손가락 또는 다른 물체를 움직임으로써, 제스처가 수행될 수 있다. 제스처는, 임의의 다른 손가락 또는 손가락들을 이용하거나 그 사이의 집기(pinching), 끌어당기기(pulling), 미끄러지기(sliding), 긁기(swiping), 회전시키기(rotating), 구부리기(flexing), 끌기(dragging), 또는 두드리기 모션으로 특징될 수 있지만, 이들로 제한되지 않는다. 한명 이상의 사용자에 의해, 하나 이상의 손으로, 또는 임의의 이들의 조합으로, 단일 동작이 수행될 수 있다.

[0100] 언급한 바와 같이, 전자 디바이스(100)는 디스플레이(예컨대, 디스플레이 출력 컴포넌트(112a))를 그래픽 데이터로 구동하여 그래픽 사용자 인터페이스("GUI")(180)를 디스플레이할 수 있다. GUI(180)는 터치 입력 컴포넌트(110f)를 통해 터치 입력을 수신하도록 구성될 수 있다. (예를 들어, 디스플레이 출력 컴포넌트(112a)를 I/O 컴포넌트(114a)로서 갖는) 터치 스크린으로서 구현된, 터치 I/O 컴포넌트(110f)는 GUI(180)를 디스플레이할 수 있다. 대안적으로, GUI(180)는 터치 입력 컴포넌트(110f)로부터 분리된 디스플레이(예컨대, 디스플레이 출력 컴포넌트(112a)) 상에 디스플레이될 수 있다. GUI(180)는 인터페이스 내의 특정 위치들에 디스플레이되는 그래

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

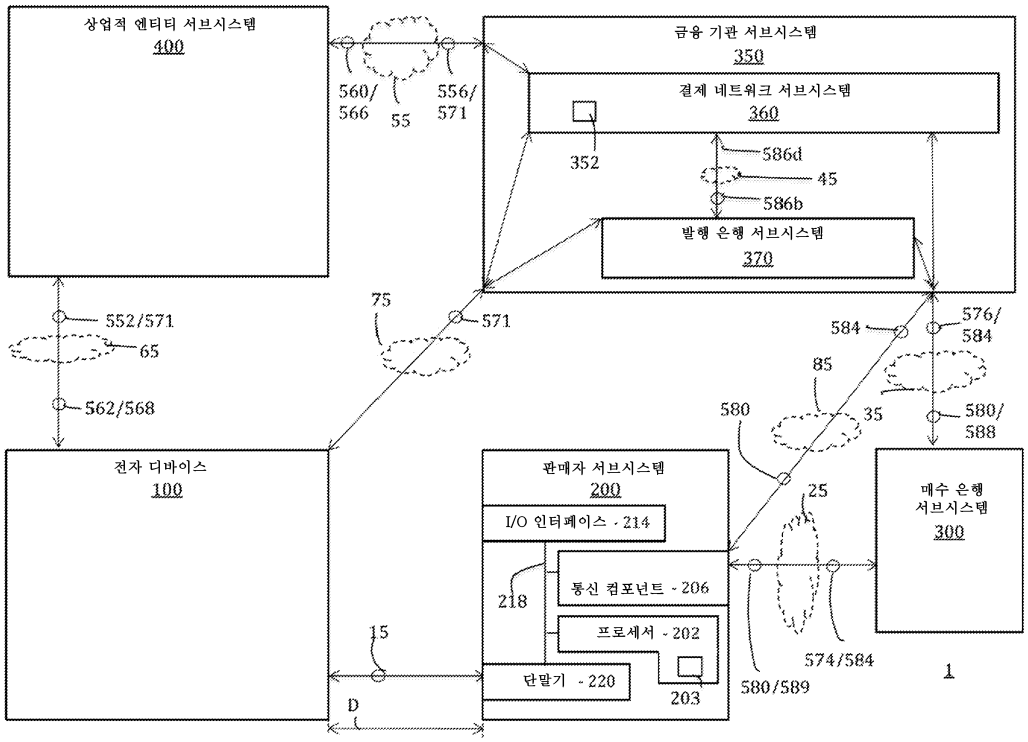
[0101] 설명한 개념들의 추가 응용들

[0102] 전자 디바이스 상에서 크리덴셜들을 안전하게 프로비저닝하고/하거나 인증하기 위한 시스템들, 방법들, 및 컴퓨터 판독가능 매체들이 기술되었지만, 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 알려지는 명확한 대안물들이, 정의된 요소들의 범주 내에 있는 것으로 규정된다.

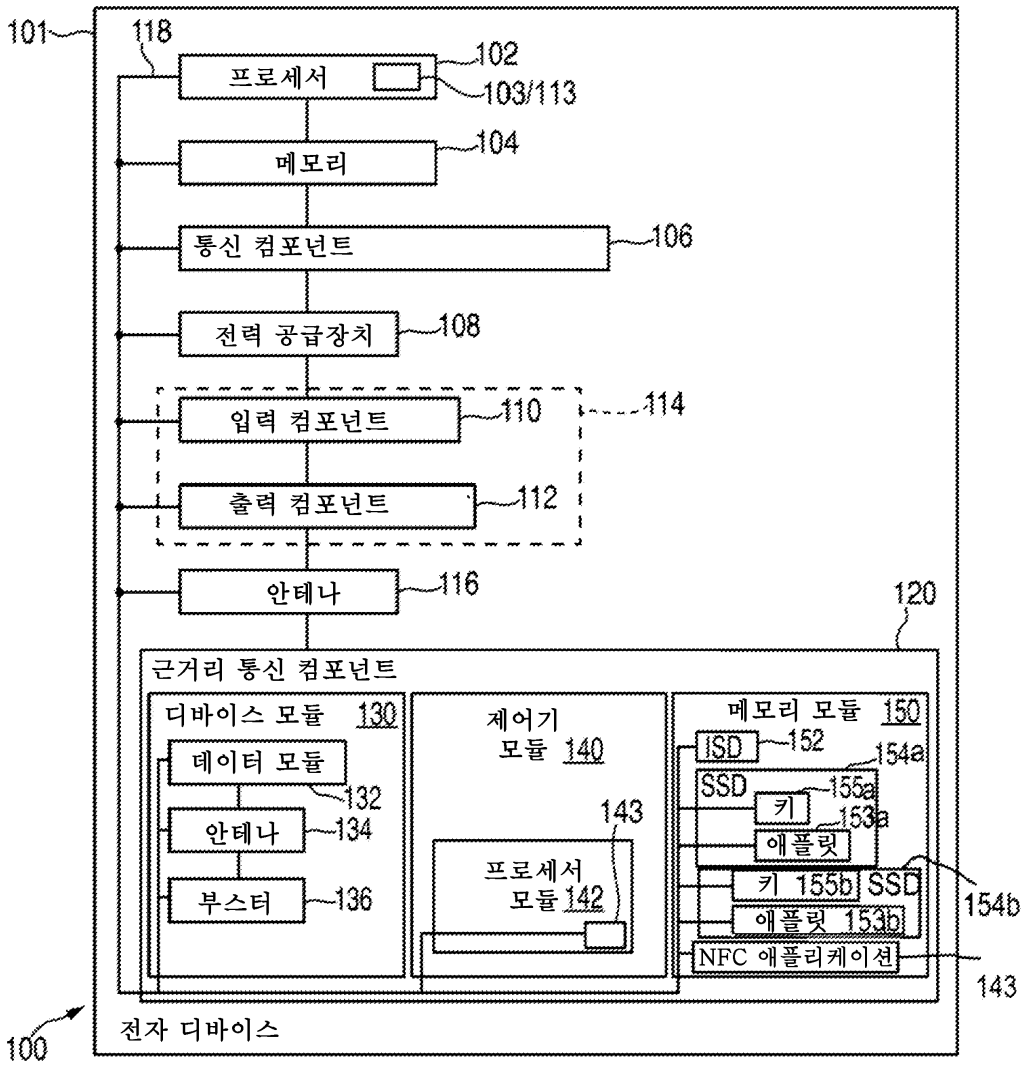
[0103] 따라서, 이들 통상의 기술자는, 본 발명이, 제한이라기보다는 예시의 목적으로 제시되는, 기술된 실시예들 이외의 것에 의해 실시될 수 있다는 것을 이해할 것이다.

도면

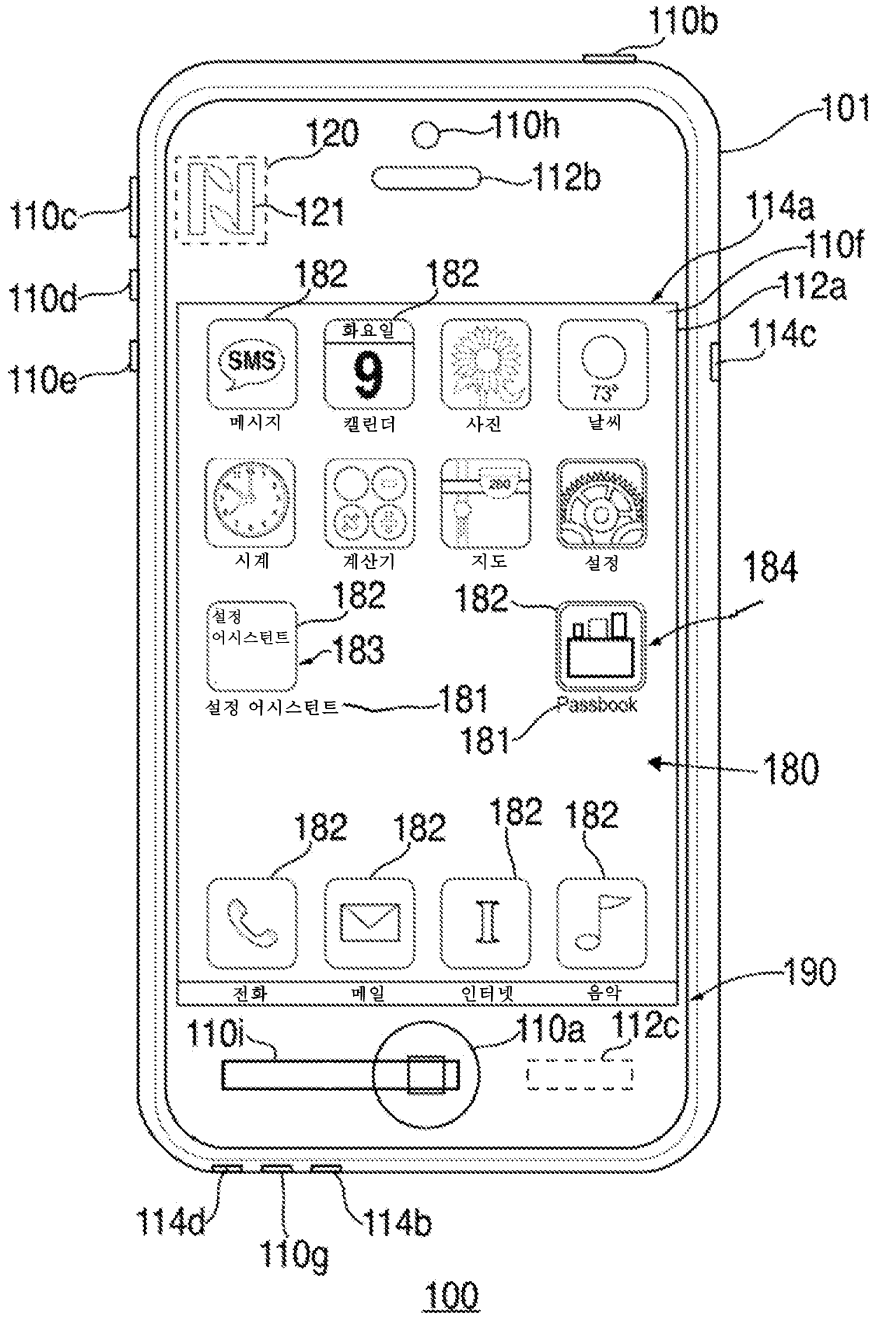
도면1


상업적 엔티티 서브시스템
400
560/
566
55
556/
571
금융 기관 서브시스템
350
결제 네트워크 서브시스템
360
352
586d
45
586b
발행 은행 서브시스템
370
552/571
65
562/568
75
571
584
576/
584
85
580
35
580/
588
전자 디바이스
100
판매자 서브시스템
200
I/O 인터페이스 - 214
25
매수 은행
서브시스템
300
218
통신 컴포넌트 - 206
프로세서 - 202
15
단말기 - 220
203
574/584
580/589
1
D

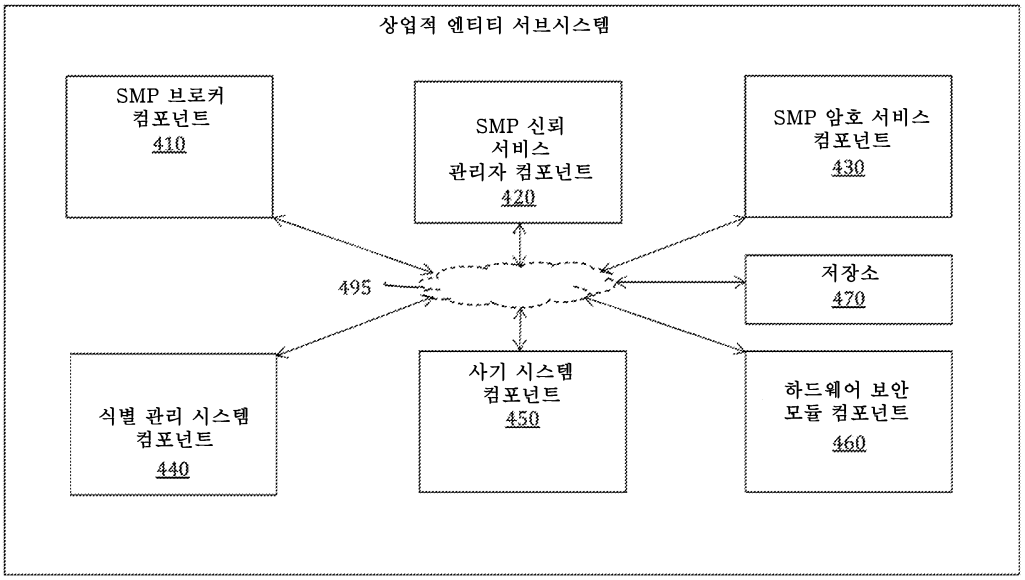
도면2


101
118
프로세서
102
103/113
메모리
104
통신 컴포넌트
106
전력 공급장치
108
입력 컴포넌트
110
114
출력 컴포넌트
112
안테나
116
120
근거리 통신 컴포넌트
디바이스 모듈 130
데이터 모듈
132
안테나
134
부스터
136
제어기
모듈 140
143
프로세서
모듈 142
메모리 모듈 150
ISD
152
154a
SSD
155a
키
153a
애플릿
키 155b
SSD
154b
애플릿 153b
NFC 애플리케이션
143
100
전자 디바이스

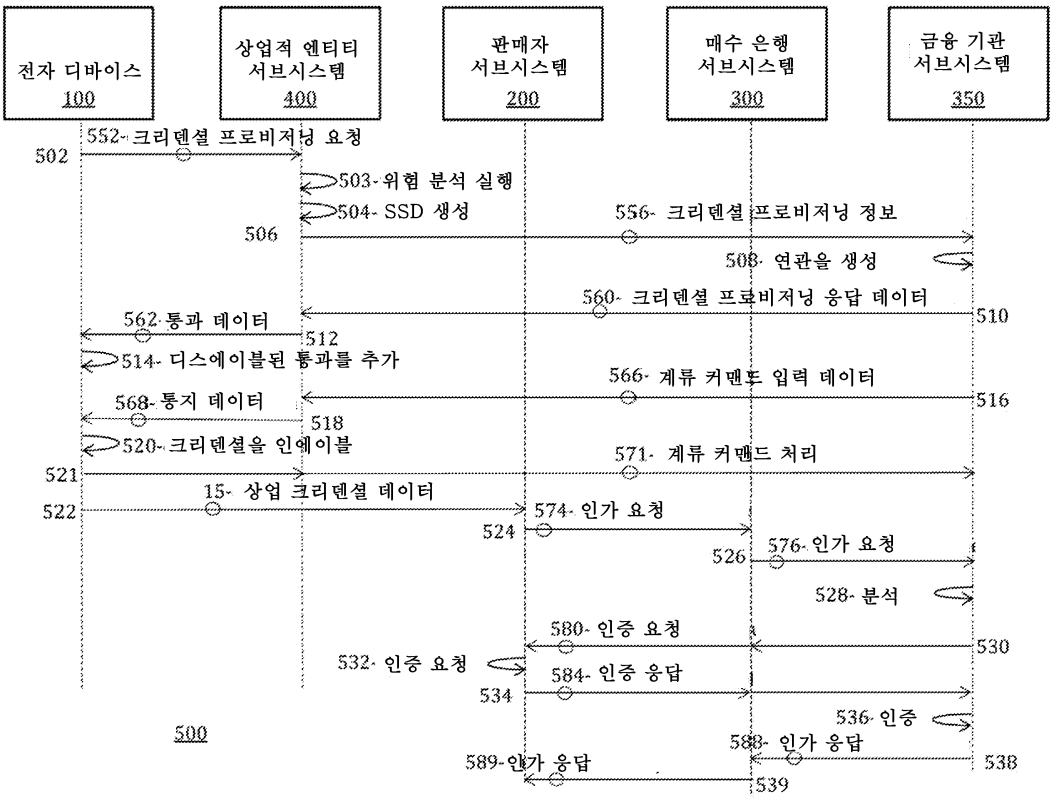
도면3


110b
101
120
110h
112b
110c
121
114a
110f
112a
110d
182
182
114c
110e
SMS
화요일
9
73°
메시지
캘린더
사진
날씨
시계
계산기
지도
설정
184
182
182
설정
어시스턴트
183
Passbook
설정 어시스턴트
181
181
180
182
182
182
182
190
전화
메일
인터넷
음악
110i
110a
112c
114d
110g
114b
100

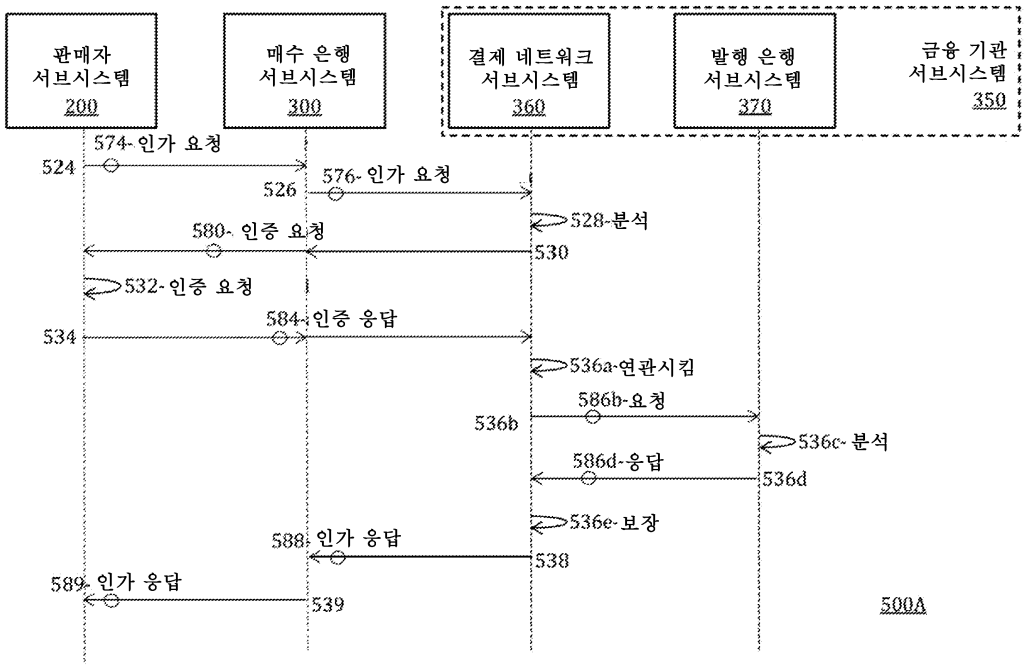
도면4


상업적 엔티티 서브시스템
SMP 브로커 컴포넌트 410
SMP 신뢰 서비스 관리자 컴포넌트 420
SMP 암호 서비스 컴포넌트 430
495
저장소 470
식별 관리 시스템 컴포넌트 440
사기 시스템 컴포넌트 450
하드웨어 보안 모듈 컴포넌트 460
400

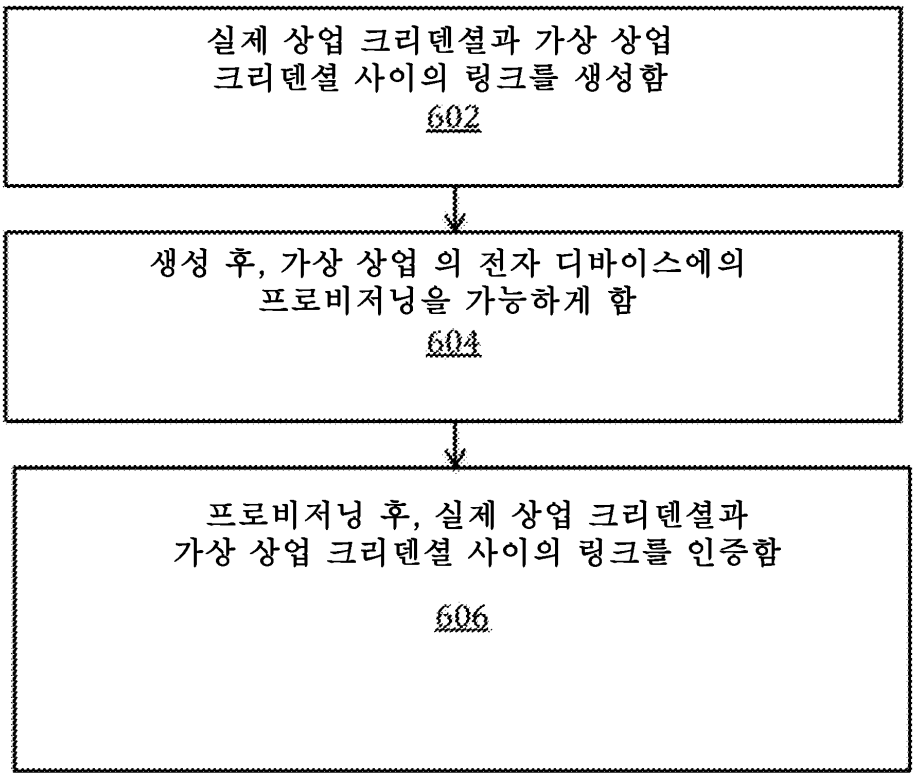
도면5


전자 디바이스 100
상업적 엔티티 서브시스템 400
판매자 서브시스템 200
매수 은행 서브시스템 300
금융 기관 서브시스템 350
552- 크리덴셜 프로비저닝 요청
502
503- 위험 분석 실행
504- SSD 생성
506
556- 크리덴셜 프로비저닝 정보
508- 연관을 생성
560- 크리덴셜 프로비저닝 응답 데이터
510
562- 통과 데이터
512
514- 디스에이블된 통과를 추가
566- 계류 커맨드 입력 데이터
516
568- 통지 데이터
518
520- 크리덴셜을 인에이블
571- 계류 커맨드 처리
521
15- 상업 크리덴셜 데이터
522
574- 인가 요청
524
576- 인가 요청
526
528- 분석
580- 인증 요청
530
532- 인증 요청
584- 인증 응답
534
536- 인증
588- 인가 응답
589- 인가 응답
538
539
500

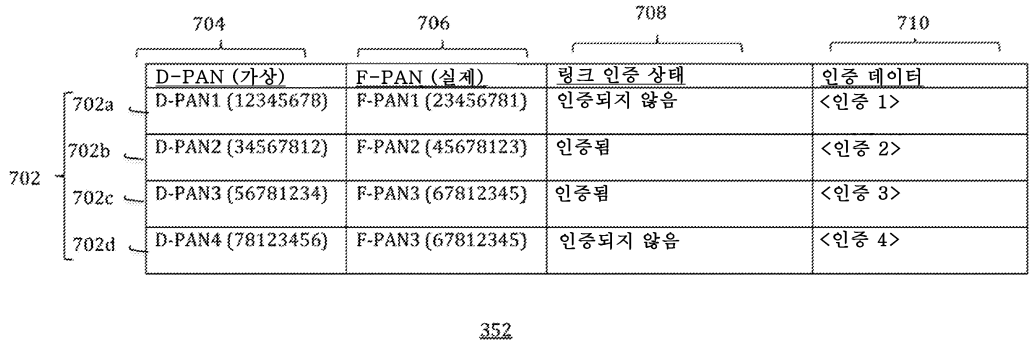
도면5a


판매자
서브시스템
200
매수 은행
서브시스템
300
결제 네트워크
서브시스템
360
발행 은행
서브시스템
370
금융 기관
서브시스템
350
574-인가 요청
524
576-인가 요청
526
528-분석
580- 인증 요청
530
532-인증 요청
584-인증 응답
534
536a-연관시킴
586b-요청
536b
536c-분석
586d-응답
536d
536e-보장
588-인가 응답
538
589-인가 응답
539
500A

도면6


실제 상업 크리덴셜과 가상 상업
크리덴셜 사이의 링크를 생성함
602
생성 후, 가상 상업 의 전자 디바이스에의
프로비저닝을 가능하게 함
604
프로비저닝 후, 실제 상업 크리덴셜과
가상 상업 크리덴셜 사이의 링크를 인증함
606
600

도면7



	704 D-PAN (가상)	706 F-PAN (실제)	708 링크 인증 상태	710 인증 데이터
702a	D-PAN1 (12345678)	F-PAN1 (23456781)	인증되지 않음	<인증 1>
702b	D-PAN2 (34567812)	F-PAN2 (45678123)	인증됨	<인증 2>
702c	D-PAN3 (56781234)	F-PAN3 (67812345)	인증됨	<인증 3>
702d	D-PAN4 (78123456)	F-PAN3 (67812345)	인증되지 않음	<인증 4>

702

352