(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년12월20일
(11) 등록번호 10-2058304
(24) 등록일자 2019년12월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
H04L 9/14 (2006.01)
(52) CPC특허분류
H04L 9/321 (2013.01)
H04L 63/0876 (2013.01)
(21) 출원번호 10-2018-7011150
(22) 출원일자(국제) 2016년09월13일
심사청구일자 2018년04월19일
(85) 번역문제출일자 2018년04월19일
(65) 공개번호 10-2018-0056727
(43) 공개일자 2018년05월29일
(86) 국제출원번호 PCT/CN2016/098815
(87) 국제공개번호 WO 2017/050147
국제공개일자 2017년03월30일
(30) 우선권주장
201510604244.5 2015년09월21일 중국(CN)
(56) 선행기술조사문헌
KR101446504 B1*
US20080215890 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐피탈 플레이스 4층
(72) 발명자
쑨 유안보
중국 저장성 311121 항저우 유 항 디스트릭트 넘버 969 웨스트 웬이 로드 빌딩 3 알리바바 그룹 리걸 디파트먼트 5층
(74) 대리인
특허법인아주김장리

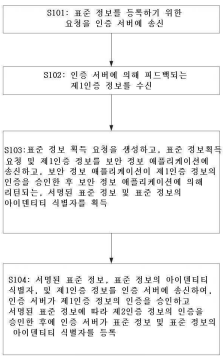
전체 청구항 수 : 총 34 항 심사관 : 박보미

(54) 발명의 명칭 **정보 등록 및 인증 방법 및 장치**

(57) 요 약

정보 등록 및 인증을 위한 방법 및 장치를 개시한다. 등록 방법은, 표준 정보 등록 요청을 인증 서버에 송신하는 단계; 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하는 단계; 표준 정보 획득 요청을 생성하고, 표준 정보 획득 요청과 제1 인증 정보를 보안 정보 애플리케이션에 송신하며, 제1 인증 정보의 인증이 통과된 후에 보안 정보 애플리케이션에 의해 리턴되는, 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 획득하는 단계로서, 서명된 표준 정보는 보안 정보 애플리케이션에 의해 제1 인증 정보를 사용하여 서명된 것인, 상기 아이덴티티 식별자를 획득하는 단계; 및 서명된 표준 정보, 표준 정보의 아이덴티티 식별자, 및 제1 인증 정보를 인증 서버에 송신하여, 제1 인증 정보의 인증이 통과되고 서명된 표준 정보에 따라 제2 인증 정보의 인증이 통과된 후에 인증 서버가 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록하게 하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/14 (2013.01)

명 세 서

청구범위

청구항 1

비즈니스 애플리케이션에 의해 구현되는 정보 등록 방법으로서,

표준 정보를 등록하기 위한 요청을 인증 서버에 송신하는 단계;

상기 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하는 단계;

표준 정보 획득 요청을 생성하고, 상기 표준 정보 획득 요청과 상기 제1 인증 정보를 보안 정보 애플리케이션에 송신하고, 상기 보안 정보 애플리케이션이 상기 제1 인증 정보의 인증을 승인한 후에 상기 보안 정보 애플리케이션에 의해 리턴되는 서명된 표준 정보 및 상기 표준 정보의 아이덴티티 식별자를 획득하는 단계로서, 상기 서명된 표준 정보는 상기 보안 정보 애플리케이션에 의해 제2 인증 정보를 사용하여 서명된 것인, 상기 아이덴티티 식별자를 획득하는 단계; 및

상기 서명된 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 상기 제1 인증 정보를 상기 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보의 인증을 승인하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보의 인증을 승인한 후에 상기 인증 서버가 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하게 하는 단계를 포함하는, 정보 등록 방법.

청구항 2

제1항에 있어서, 상기 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하는 단계는, 상기 인증 서버에 의해 송신되고 상기 인증 서버의 고유한 제1암호화 키를 사용하여 서명된 인증서를 수신하는 단계, 및 상기 서명된 인증서를 상기 제1 인증 정보로서 사용하는 단계를 포함하는, 정보 등록 방법.

청구항 3

정보 등록 방법으로서,

비즈니스 애플리케이션에 의해 송신되는 제1 인증 정보와 표준 정보 획득 요청을 수신하는 단계; 및

상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후, 제2 인증 정보를 사용하여 서명된 표준 정보를 리턴하며, 상기 표준 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션으로 다시 리턴하여, 상기 비즈니스 애플리케이션이 상기 서명된 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 인증 서버에 송신하게 하고, 상기 인증 서버가 상기 제1 인증 정보의 인증을 승인하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보의 인증을 승인한 후에 상기 인증 서버가 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하게 하는 단계를 포함하는, 정보 등록 방법.

청구항 4

제3항에 있어서, 제2 인증 정보를 사용하여 서명된 표준 정보를 리턴하며, 상기 표준 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션으로 다시 리턴하는 단계는,

사용자에 의해 입력되는 표준 정보를 수신하는 단계;

상기 제2 인증 정보를 사용하여 상기 표준 정보에 서명하고, 상기 표준 정보에 대하여 상기 표준 정보의 아이덴티티 식별자를 결정하는 단계; 및

상기 서명된 표준 정보 및 상기 표준 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션으로 다시 리턴하는 단계를 포함하는, 정보 등록 방법.

청구항 5

제4항에 있어서, 상기 표준 정보의 아이덴티티 식별자는 상기 표준 정보의 아이덴티티 키 정보를 포함하고, 상

기 아이덴티티 키 정보는 상기 사용자의 계정 정보에 연관된, 정보 등록 방법.

청구항 6

제3항에 있어서, 상기 제1 인증 정보는 상기 인증 서버의 서명된 인증서를 포함하고,

상기 제1 인증 정보를 인증하는 단계는, 상기 인증 서버의 제1암호화 키와 일치하는 제1복호화 키를 사용하여 상기 서명된 인증서를 복호화하고 인증하는 단계를 포함하는, 정보 등록 방법.

청구항 7

제4항에 있어서, 상기 제2 인증 정보는 상기 인증 서버와 미리 합의된 제2키 정보를 포함하고, 상기 제2키 정보는 제2암호화 키와 제2복호화 키를 포함하며,

상기 제2 인증 정보를 사용하여 상기 표준 정보에 서명하는 단계는, 상기 인증 서버와 미리 합의된 상기 제2암호화 키를 사용하여 상기 표준 정보에 서명하는 단계를 포함하는, 정보 등록 방법.

청구항 8

정보 등록 방법으로서,

인증 서버에 의해, 비즈니스 애플리케이션에 의해 송신되는 표준 정보를 등록하기 위한 요청을 수신하는 단계;

상기 표준 정보를 등록하기 위한 요청에 따라, 제1 인증 정보를 생성하고 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하는 단계;

상기 비즈니스 애플리케이션에 의해 송신되는, 서명된 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 제1 인증 정보를 수신하는 단계로서, 상기 서명된 표준 정보는, 보안 정보 애플리케이션에 의해 제2 인증 정보를 사용하여 서명되고 상기 비즈니스 애플리케이션에 송신되는, 상기 서명된 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 제1 인증 정보를 수신하는 단계;

상기 제1 인증 정보를 인증하고, 상기 서명된 표준 정보에 따라 상기 제2 인증 정보를 인증하는 단계; 및

상기 제1 인증 정보와 상기 제2 인증 정보의 인증을 승인한 후에 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하는 단계를 포함하는, 정보 등록 방법.

청구항 9

제8항에 있어서, 상기 표준 정보를 등록하기 위한 요청에 따라, 제1 인증 정보를 생성하고 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하는 단계는,

상기 표준 정보를 등록하기 위한 요청에 따라 상기 인증 서버의 고유한 인증서를 인보크(invoke)하는 단계; 및

상기 인증 서버의 고유한 제1암호화 키를 사용하여 상기 인증서를 상기 제1 인증 정보로서 서명하고, 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하는 단계를 포함하는, 정보 등록 방법.

청구항 10

제8항에 있어서, 상기 제1 인증 정보를 인증하는 단계는 제1복호화 키를 사용하여 상기 제1 인증 정보를 복호화하고 인증하는 단계를 포함하는, 정보 등록 방법.

청구항 11

제8항에 있어서, 상기 제2 인증 정보는, 상기 인증 서버와 상기 보안 정보 애플리케이션에 의해 미리 합의된 제2키 정보를 포함하고, 상기 제2키 정보는 제2암호화 키와 제2복호화 키를 포함하며, 상기 서명된 표준 정보는 상기 제2암호화 키를 사용하여 상기 보안 정보 애플리케이션에 의해 서명된 것이고,

상기 서명된 표준 정보에 따라 상기 제2 인증 정보를 인증하는 단계는, 미리 합의된 상기 제2키 정보에 따라, 상기 보안 정보 애플리케이션과 미리 합의된 상기 제2복호화 키를 사용하여 상기 서명된 표준 정보를 복호화하여 상기 제2 인증 정보를 인증하는 단계를 포함하는, 정보 등록 방법.

청구항 12

비즈니스 애플리케이션에 의해 구현되는 정보 인증 방법으로서,

인증될 정보에 대한 검증 요청을 인증 서버에 송신하는 단계;

상기 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하는 단계;

인증될 정보 획득 요청을 생성하고, 상기 인증될 정보 획득 요청과 상기 제1 인증 정보를 보안 정보 애플리케이션에 송신하며, 상기 보안 정보 애플리케이션이 상기 제1 인증 정보의 인증을 승인한 후에 상기 보안 정보 애플리케이션에 의해 리턴되는 인증될 정보 및 상기 인증될 정보의 인증될 아이덴티티 식별자를 획득하는 단계; 및

상기 인증될 정보, 상기 인증될 아이덴티티 식별자, 및 상기 제1 인증 정보를 상기 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보, 상기 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하게 하는 단계를 포함하는, 정보 인증 방법.

청구항 13

정보 인증 방법으로서,

비즈니스 애플리케이션에 의해 송신되며 제1 인증 정보를 반송하는 인증될 정보 획득 요청을 수신하는 단계; 및

상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후, 인증될 정보 및 상기 인증될 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션을 통해 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보, 상기 인증될 정보의 아이덴티티 식별자, 및 상기 인증될 정보를 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하게 하는 단계를 포함하는, 정보 인증 방법.

청구항 14

제13항에 있어서, 상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후, 인증될 정보 및 상기 인증될 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션을 통해 인증 서버에 송신하는 단계는,

표준 정보 획득 요청에 반송되는 상기 제1 인증 정보를 인증하는 단계;

상기 인증이 승인된 후, 사용자에 의해 입력되는 인증될 정보를 수신하는 단계;

상기 인증될 정보가 속하는 표준 정보를 식별하고, 상기 표준 정보와 일치하는 아이덴티티 표준을 상기 인증될 정보의 인증될 아이덴티티 식별자라고 결정하는 단계; 및

상기 인증될 정보와 상기 인증될 정보의 인증될 아이덴티티 식별자를 상기 비즈니스 애플리케이션으로 다시 리턴하는 단계를 포함하는, 정보 인증 방법.

청구항 15

정보 인증 방법으로서,

인증 서버에 의해, 비즈니스 애플리케이션에 의해 송신되는 인증될 정보에 대한 검증 요청을 수신하는 단계;

상기 검증 요청에 따라, 제1 인증 정보를 생성하고 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하는 단계;

상기 비즈니스 애플리케이션에 의해 송신되는, 상기 인증될 정보, 상기 인증될 정보의 인증될 아이덴티티 식별자, 및 상기 제1 인증 정보를 수신하는 단계; 및

상기 제1 인증 정보, 상기 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 각각 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하는 단계를 포함하는, 정보 인증 방법.

청구항 16

제15항에 있어서, 상기 제1 인증 정보, 상기 아이덴티티 식별자, 및 상기 인증될 정보를 각각 인증하는 단계는,

상기 제1 인증 정보에 관하여, 상기 인증 서버의 제1복호화 키를 사용하여 상기 제1 인증 정보를 복호화하고 복호화된 인증서를 인증하는 단계;

상기 인증될 아이덴티티 식별자에 관하여, 등록된 표준 정보의 아이덴티티 식별자에 따라, 상기 인증될 아이덴티티 식별자가 상기 등록된 표준 정보의 아이덴티티 식별자와 일치하는지를 결정하는 단계; 및

인증을 위해 상기 인증될 정보를 상기 등록된 표준 정보와 비교하는 단계를 포함하는, 정보 인증 방법.

청구항 17

제16항에 있어서, 상기 인증 결과를 생성하고 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하는 단계는,

상기 제1 인증 정보에 관하여, 상기 인증이 승인되면 상기 인증될 정보와 인증될 아이덴티티 식별자를 인증하고, 상기 인증이 승인되지 않으면 인증 실패 통지를 리턴하는 단계;

상기 아이덴티티 식별자에 관하여, 상기 인증이 승인되면 상기 인증될 정보를 인증하고, 상기 인증이 승인되지 않으면 인증 실패 통지를 리턴하는 단계; 및

상기 인증될 정보에 관하여, 상기 인증이 승인되면 성공 통지를 리턴하고, 상기 인증이 승인되지 않으면 인증 실패 통지를 리턴하는 단계를 포함하는, 정보 인증 방법.

청구항 18

정보 등록 장치로서,

표준 정보를 등록하기 위한 요청을 인증 서버에 송신하도록 구성된 등록 요청 모듈;

상기 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하도록 구성된 수신 모듈;

표준 정보 획득 요청을 생성하고, 상기 표준 정보 획득 요청과 상기 제1 인증 정보를 보안 정보 애플리케이션에 송신하고, 상기 보안 정보 애플리케이션이 상기 제1 인증 정보의 인증을 승인한 후에 상기 보안 정보 애플리케이션에 의해 리턴되는 서명된 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 획득하도록 구성된 획득 모듈로서, 상기 서명된 표준 정보는 제2 인증 정보를 사용하여 상기 보안 정보 애플리케이션에 의해 서명된 것인, 획득 모듈; 및

상기 서명된 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 상기 제1 인증 정보를 상기 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보의 인증을 승인하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보의 인증을 승인한 후에 상기 인증 서버가 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하게 하도록 구성된 송신 모듈을 포함하는, 정보 등록 장치.

청구항 19

제18항에 있어서, 상기 수신 모듈은, 상기 인증 서버에 의해 송신되고 상기 인증 서버의 고유한 제1암호화 키를 사용하여 서명된 인증서를 수신하고, 상기 서명된 인증서를 상기 제1 인증 정보로서 사용하도록 구성된, 정보 등록 장치.

청구항 20

정보 등록 장치로서,

비즈니스 애플리케이션에 의해 송신되는 제1 인증 정보 및 표준 정보 획득 요청을 수신하도록 구성된 수신 모듈; 및

상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후, 제2 인증 정보를 사용함으로써 서명된 표준 정보를 리턴하고 상기 표준 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션으로 다시 리턴하여, 상기 비즈니스 애플리케이션이 상기 서명된 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 인증 서버에 송신하게 하고, 상기 인증 서버가 상기 제1 인증 정보의 인증을 승인하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보의 인증을 승인한 후에 상기 인증 서버가 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하게 하도록 구성된 서명 모듈을 포함하는, 정보 등록 장치.

청구항 21

제20항에 있어서, 상기 서명 모듈은, 사용자에 의해 입력되는 표준 정보를 수신하고, 상기 제2 인증 정보를 사

용하여 상기 표준 정보에 서명하며, 상기 표준 정보에 대하여 상기 표준 정보의 아이덴티티 식별자를 결정하고, 상기 서명된 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션으로 다시 리턴하도록 구성된, 정보 등록 장치.

청구항 22

제21항에 있어서, 상기 표준 정보의 아이덴티티 식별자는 상기 표준 정보의 아이덴티티 키 정보를 포함하고, 상기 아이덴티티 키 정보는 상기 사용자의 계정 정보에 연관된, 정보 등록 장치.

청구항 23

제20항에 있어서, 상기 제1 인증 정보는 상기 인증 서버의 서명된 인증서를 포함하고, 상기 서명 모듈은, 상기 인증 서버의 제1암호화 키와 일치하는 제1복호화 키를 사용하여 상기 서명된 인증서를 복호화하고 인증하도록 구성된, 정보 등록 장치.

청구항 24

제21항에 있어서, 상기 제2 인증 정보는 상기 인증 서버와 미리 합의된 제2키 정보를 포함하고, 상기 제2키 정보는 제2암호화 키와 제2복호화 키를 포함하며, 상기 서명 모듈은, 상기 인증 서버와 미리 합의된 상기 제2암호화 키를 사용하여 상기 표준 정보에 서명하도록 구성된, 정보 등록 장치.

청구항 25

정보 등록 장치로서,

비즈니스 애플리케이션에 의해 송신되는 표준 정보를 등록하기 위한 요청을 수신하도록 구성된 등록 요청 수신 모듈;

상기 표준 정보를 등록하기 위한 요청에 따라 제1 인증 정보를 생성하고 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하도록 구성된 피드백 모듈;

상기 비즈니스 애플리케이션에 의해 송신되는, 서명된 상기 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 상기 제1 인증 정보를 수신하도록 구성된 등록 정보 수신 모듈로서, 상기 서명된 표준 정보는 보안 정보 애플리케이션에 의해 제2 인증 정보를 사용하여 서명되고 상기 비즈니스 애플리케이션에 송신되는 것인, 등록 정보 수신 모듈;

상기 제1 인증 정보를 인증하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보를 인증하도록 구성된 인증 모듈; 및

상기 제1 인증 정보와 상기 제2 인증 정보의 인증을 통과한 후 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하도록 구성된 등록 모듈을 포함하는, 정보 등록 장치.

청구항 26

제25항에 있어서, 상기 피드백 모듈은, 상기 표준 정보를 등록하기 위한 요청에 따라, 인증 서버의 고유한 인증서를 인보크하고, 상기 인증 서버의 고유한 제1암호화 키를 사용하여 상기 인증서를 상기 제1 인증 정보로서 서명하고, 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하도록 구성된, 정보 등록 장치.

청구항 27

제25항에 있어서, 상기 인증 모듈은 제1복호화 키를 사용하여 상기 제1 인증 정보를 복호화하고 인증하도록 구성된, 정보 등록 장치.

청구항 28

제25항에 있어서, 상기 제2 인증 정보는 인증 서버 및 상기 보안 정보 애플리케이션과 미리 합의된 제2키 정보를 포함하고, 상기 제2키 정보는 제2암호화 키와 제2복호화 키를 포함하고, 상기 서명된 표준 정보는 상기 제2암호화 키를 사용하여 상기 보안 정보 애플리케이션에 의해 서명되고,

상기 인증 모듈은, 미리 합의된 상기 제2키 정보에 따라, 상기 보안 정보 애플리케이션과 미리 합의된 상기 제2

복호화 키를 사용하여 상기 서명된 정보를 복호화하여 상기 제2 인증 정보를 인증하도록 구성된, 정보 등록 장치.

청구항 29

정보 인증 장치로서,

인증될 정보에 대한 검증 요청을 인증 서버에 송신하도록 구성된 등록 요청 모듈;

상기 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하도록 구성된 수신 모듈;

인증될 정보 획득 요청을 생성하고, 상기 인증될 정보 획득 요청과 상기 제1 인증 정보를 보안 정보 애플리케이션에 송신하고, 상기 보안 정보 애플리케이션이 상기 제1 인증 정보의 인증을 승인한 후에 상기 보안 정보 애플리케이션에 의해 리턴되는 인증될 정보와 상기 인증될 정보의 인증될 아이덴티티 식별자를 획득하도록 구성된 획득 모듈; 및

상기 인증될 정보, 상기 인증될 아이덴티티 식별자, 및 상기 제1 인증 정보를 상기 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보, 상기 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 비즈니스 애플리케이션으로 피드백하게 하도록 구성된 송신 모듈을 포함하는, 정보 인증 장치.

청구항 30

정보 인증 장치로서,

비즈니스 애플리케이션에 의해 송신되고 제1 인증 정보를 반송하는 인증될 정보 획득 요청을 수신하도록 구성된 수신 모듈; 및

상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후에, 인증될 정보와 상기 인증될 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션을 통해 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보, 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하게 하도록 구성된 서명 모듈을 포함하는, 정보 인증 장치.

청구항 31

제30항에 있어서, 상기 서명 모듈은, 표준 정보 획득 요청에 반송되는 상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후에, 상기 인증될 정보가 속하는 표준 정보를 식별하며, 상기 표준 정보와 일치하는 아이덴티티 표준을 상기 인증될 정보의 인증될 아이덴티티 식별자라고 결정하고, 상기 인증될 정보와 상기 인증될 정보의 인증될 아이덴티티 식별자를 상기 비즈니스 애플리케이션으로 다시 리턴하도록 구성된, 정보 인증 장치.

청구항 32

정보 인증 장치로서,

비즈니스 애플리케이션에 의해 송신되는 인증될 정보에 대한 검증 요청을 수신하도록 구성된 인증 요청 수신 모듈;

상기 검증 요청에 따라, 제1 인증 정보를 생성하고 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하도록 구성된 피드백 모듈;

상기 비즈니스 애플리케이션에 의해 송신되는, 상기 인증될 정보, 상기 인증될 정보의 인증될 아이덴티티 식별자, 및 상기 제1 인증 정보를 수신하도록 구성된 인증 정보 수신 모듈; 및

상기 제1 인증 정보, 상기 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 각각 인증하여 인증 결과를 생성하고 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하도록 구성된 인증 모듈을 포함하는, 정보 인증 장치.

청구항 33

제32항에 있어서, 상기 인증 모듈은, 상기 제1 인증 정보에 관하여, 정보 인증 장치의 제1복호화 키를 사용하여 상기 제1 인증 정보를 복호화하고 복호화된 인증서를 인증하고, 상기 인증될 아이덴티티 식별자에 관하여, 등록

된 표준 정보의 아이덴티티 식별자에 따라 상기 인증될 아이덴티티 식별자가 상기 등록된 표준 정보의 아이덴티티 식별자와 일치하는지를 결정하며, 인증을 위해 상기 인증될 정보를 상기 등록된 표준 정보와 비교하도록 구성된, 정보 인증 장치.

청구항 34

제33항에 있어서, 상기 인증 모듈은, 상기 제1 인증 정보에 관하여, 인증이 승인되면 상기 인증될 정보와 인증될 아이덴티티 식별자를 인증하고, 인증이 승인되지 않으면 인증 실패 통지를 리턴하며, 상기 아이덴티티 식별자에 관하여, 인증이 승인되면 상기 인증될 정보를 인증하고, 인증이 승인되지 않으면 인증 실패 통지를 리턴하며, 상기 인증될 정보에 관하여, 인증이 승인되면 성공 통지를 리턴하고 인증이 승인되지 않으면 인증 실패 통지를 리턴하도록 구성된, 정보 인증 장치.

발명의 설명

기 술 분 야

[0001] 본 출원은, 컴퓨터 기술 분야에 관한 것으로서, 구체적으로는, 정보 등록 및 인증 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 정보 기술이 발달함에 따라, 사용자는, 단말(예를 들어, 휴대 전화, 태블릿 컴퓨터 등)에 설치된 서비스 제공자(예를 들어, 소프트웨어 개발자, 웹사이트 등)에 의한 애플리케이션 프로그램(이하 "비즈니스 애플리케이션")을 통해 다양한 비즈니스 서비스를 편리하고 신속하게 수신할 수 있다. 비즈니스 애플리케이션에서 제공되는 비즈니스 서비스와 관련하여, 일부 유형의 비즈니스 서비스는 지불 서비스, 송신 서비스 등과 같이 비교적 높은 보안 수준을 갖는다. 비교적 높은 보안 수준을 갖는 비즈니스 서비스는, 일반적으로 대응하는 보안 정보(예를 들어, 패스워드, 생체인증(biometric) 정보 등)를 제공할 것을 사용자에게 요구하며, 비즈니스 서비스는 사용자에 의해 제공된 보안 정보가 인증된 후에만 완료될 수 있다.

[0003] 사용자가 보안 정보를 제공하도록 요구하는 전술한 비즈니스 서비스의 경우, 일반적으로, 사용자에 의해 후속 입력되는 보안 정보와의 비교를 위해 사용자가 비즈니스 서비스를 처음으로 이용하기 전에 사용자의 보안 정보를 표준 정보(표준 정보는 후속 인증 프로세스에서 인증 기준으로서 사용됨)로서 획득한다. 사용자의 보안 정보를 획득하는 프로세스에서, 비즈니스 애플리케이션은, 사용자의 보안 정보를 획득하도록 단말의 보안 정보 애플리케이션(예를 들어, 사용자에 의해 입력되는 생체인증 정보의 수집 및 보관을 담당하는 바이오인포매틱스 관리 애플리케이션이며, 바이오인포매틱스 관리 애플리케이션은 단말 제조사에 의해 단말에 설치됨)을 사용할 필요가 있다.

[0004] 애플리케이션 인보크(invoke) 및 비즈니스 애플리케이션과 보안 정보 애플리케이션 간의 정보 송신이 용이하도록, 종래 기술의 단말 시스템(예를 들어, Android M 시스템)은 리치 실행 환경(REE)이라고 하는 아키텍처에서 보안 정보 애플리케이션을 실행한다. REE는 많은 인보크 지원을 보유하며, REE에서 실행되는 보안 정보 애플리케이션은, 다양한 비즈니스 서비스에 의해 더욱 편리하고 신속하게 인보크될 수 있고, 모든 비즈니스 애플리케이션에 의해 요구되는 정보를 더욱 편리하고 신속하게 송신할 수 있다.

[0005] 그러나, REE는 안전한 환경이 아니다. 보안 정보 애플리케이션과 비즈니스 애플리케이션 간의 정보 송신 프로세스에서, 보안 정보는 송신 중에 불법 조작자에 의해 인터셉트되고 조작되는 경향이 있다. 특히, 표준 정보의 경우, 서비스 제공자가 사용자에 의해 제공된 표준 정보를 이전에 저장하지 않았기 때문에 표준 정보가 참인지 거짓인지를 식별하는 것이 불가능하다. 일단 표준 정보가 송신 중에 조작되었다면, 서비스 제공자는 후속 인증 프로세스에서 조작된 표준 정보를 인증 기준으로서 여전히 수신할 것이다. 명백하게, 불법 조작자는 결국 사용자의 이름으로 다양한 비즈니스 서비스를 획득하게 된다.

발명의 내용

[0006] 본 출원의 실시형태들은, 보안 정보가 등록에 사용되는 경우 보안이 열악한 종래 기술의 문제점을 해결하도록 정보를 등록 및 인증하기 위한 방법 및 장치를 제공한다.

[0007] 본 출원의 실시형태에 의해 제공되는 정보 등록 방법은, 표준 정보를 등록하기 위한 요청을 인증 서버에 송신하는 단계; 상기 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하는 단계; 표준 정보 획득 요청을 생성하고, 상기 표준 정보 획득 요청과 상기 제1 인증 정보를 보안 정보 애플리케이션에 송신하며, 상기 보안 정보 애플리

케이션이 상기 제1 인증 정보의 인증을 승인한 후에 상기 보안 정보 애플리케이션에 의해 리턴되는 서명된 표준 정보 및 상기 표준 정보의 아이덴티티 식별자를 획득하는 단계로서, 상기 서명된 표준 정보는 제2 인증 정보를 사용하여 상기 보안 정보 애플리케이션에 의해 서명된 것인, 상기 아이덴티티 식별자를 획득하는 단계; 및 상기 서명된 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 상기 제1 인증 정보를 상기 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보의 인증을 승인하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보의 인증을 승인한 후에 상기 인증 서버가 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하게 하는 단계를 포함한다.

[0008] 본 출원의 실시형태에 의해 또한 제공되는 정보 등록 방법은, 비즈니스 애플리케이션에 의해 송신되는 제1 인증 정보와 표준 정보 획득 요청을 수신하는 단계; 및 상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후, 제2 인증 정보를 사용하여 서명된 표준 정보를 리턴하고 상기 표준 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션으로 다시 리턴하여, 상기 비즈니스 애플리케이션이 상기 서명된 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 인증 서버에 송신하게 하고, 상기 인증 서버가 상기 제1 인증 정보의 인증을 승인하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보의 인증을 승인한 후에 상기 인증 서버가 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하게 하는 단계를 포함한다.

[0009] 본 출원의 실시형태에 의해 또한 제공되는 정보 등록 방법은, 인증 서버에 의해, 비즈니스 애플리케이션에 의해 송신되는 표준 정보를 등록하기 위한 요청을 수신하는 단계; 상기 표준 정보를 등록하기 위한 요청에 따라, 제1 인증 정보를 생성하고 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하는 단계; 상기 비즈니스 애플리케이션에 의해 송신되는, 서명된 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 제1 인증 정보를 수신하는 단계로서, 상기 서명된 표준 정보는, 보안 정보 애플리케이션에 의해 제2 인증 정보를 사용하여 서명되고 상기 비즈니스 애플리케이션에 송신되는, 상기 서명된 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 제1 인증 정보를 수신하는 단계; 상기 제1 인증 정보를 인증하고, 상기 서명된 표준 정보에 따라 상기 제2 인증 정보를 인증하는 단계; 및 상기 제1 인증 정보와 상기 제2 인증 정보의 인증을 승인한 후에 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하는 단계를 포함한다.

[0010] 본 출원의 실시형태에 의해 또한 제공되는 정보 인증 방법은, 인증될 정보에 대한 검증 요청을 인증 서버에 송신하는 단계; 상기 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하는 단계; 인증될 정보 획득 요청을 생성하고, 상기 인증될 정보 획득 요청과 상기 제1 인증 정보를 보안 정보 애플리케이션에 송신하고, 상기 보안 정보 애플리케이션이 상기 제1 인증 정보의 인증을 승인한 후에 상기 보안 정보 애플리케이션에 의해 리턴되는 인증될 정보 및 상기 인증될 정보의 인증될 아이덴티티 식별자를 획득하는 단계; 및 상기 인증될 정보, 상기 인증될 아이덴티티 식별자, 및 상기 제1 인증 정보를 상기 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보, 상기 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하게 하는 단계를 포함한다.

[0011] 본 출원의 실시형태에 의해 또한 제공되는 정보 인증 방법은, 비즈니스 애플리케이션에 의해 송신되며 제1 인증 정보를 반송하는 인증될 정보 획득 요청을 수신하는 단계; 및 상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후, 인증될 정보 및 상기 인증될 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션을 통해 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보, 상기 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하게 하는 단계를 포함한다.

[0012] 본 출원의 실시형태에 의해 또한 제공되는 정보 인증 방법은, 인증 서버에 의해, 비즈니스 애플리케이션에 의해 송신되는 인증될 정보에 대한 검증 요청을 수신하는 단계; 상기 검증 요청에 따라, 제1 인증 정보를 생성하고 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하는 단계; 상기 비즈니스 애플리케이션에 의해 송신되는, 상기 인증될 정보, 상기 인증될 정보의 인증될 아이덴티티 식별자, 및 상기 제1 인증 정보를 수신하는 단계; 및 상기 제1 인증 정보, 상기 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 각각 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하는 단계를 포함한다.

[0013] 본 출원의 실시형태에 의해 또한 제공되는 정보 등록 장치는, 표준 정보를 등록하기 위한 요청을 인증 서버에 송신하도록 구성된 등록 요청 모듈; 상기 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하도록 구성된 수신 모듈; 표준 정보 획득 요청을 생성하고, 상기 표준 정보 획득 요청과 상기 제1 인증 정보를 보안 정보 애플리케이션에 송신하고, 상기 보안 정보 애플리케이션이 상기 제1 인증 정보의 인증을 승인한 후에 상기 보안 정보 애플리케이션에 의해 리턴되는 서명된 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 획득하도록 구성

된 획득 모듈로서, 상기 서명된 표준 정보는 제2 인증 정보를 사용하여 상기 보안 정보 애플리케이션에 의해 서명된 것인, 획득 모듈; 및 상기 서명된 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 상기 제1 인증 정보를 상기 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보의 인증을 승인하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보의 인증을 승인한 후에 상기 인증 서버가 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하게 하도록 구성된 송신 모듈을 포함한다.

[0014] 본 출원의 실시형태에 의해 또한 제공되는 정보 등록 장치는, 비즈니스 애플리케이션에 의해 송신되는 제1 인증 정보 및 표준 정보 획득 요청을 수신하도록 구성된 수신 모듈; 및 상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후, 제2 인증 정보를 사용함으로써 서명된 표준 정보를 리턴하고 상기 표준 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션으로 다시 리턴하여, 상기 비즈니스 애플리케이션이 상기 서명된 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 인증 서버에 송신하게 하고, 상기 인증 서버가 상기 제1 인증 정보의 인증을 승인하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보의 인증을 승인한 후에 상기 인증 서버가 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하게 하도록 구성된 서명 모듈을 포함한다.

[0015] 본 출원의 실시형태에 의해 또한 제공되는 정보 등록 장치는, 비즈니스 애플리케이션에 의해 송신되는 표준 정보를 등록하기 위한 요청을 수신하도록 구성된 등록 요청 수신 모듈; 상기 표준 정보를 등록하기 위한 요청에 따라 제1 인증 정보를 생성하고 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하도록 구성된 피드백 모듈; 상기 비즈니스 애플리케이션에 의해 송신되는, 서명된 상기 표준 정보, 상기 표준 정보의 아이덴티티 식별자, 및 상기 제1 인증 정보를 수신하도록 구성된 등록 정보 수신 모듈로서, 상기 서명된 표준 정보는 보안 정보 애플리케이션에 의해 제2 인증 정보를 사용하여 서명되고 상기 비즈니스 애플리케이션에 송신되는 것인, 상기 등록 정보 수신 모듈; 상기 제1 인증 정보를 인증하고 상기 서명된 표준 정보에 따라 상기 제2 인증 정보를 인증하도록 구성된 인증 모듈; 및 상기 제1 인증 정보와 상기 제2 인증 정보의 인증을 통과한 후 상기 표준 정보와 상기 표준 정보의 아이덴티티 식별자를 등록하도록 구성된 등록 모듈을 포함한다.

[0016] 본 출원의 실시형태에 의해 또한 제공되는 정보 인증 장치는, 인증될 정보에 대한 검증 요청을 인증 서버에 송신하도록 구성된 등록 요청 모듈; 상기 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하도록 구성된 수신 모듈; 인증될 정보 획득 요청을 생성하고, 상기 인증될 정보 획득 요청과 상기 제1 인증 정보를 보안 정보 애플리케이션에 송신하고, 상기 보안 정보 애플리케이션이 상기 제1 인증 정보의 인증을 승인한 후에 상기 보안 정보 애플리케이션에 의해 리턴되는 인증될 정보와 상기 인증될 정보의 인증될 아이덴티티 식별자를 획득하도록 구성된 획득 모듈; 및 상기 인증될 정보, 상기 인증될 아이덴티티 식별자, 및 상기 제1 인증 정보를 상기 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보, 상기 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 비즈니스 애플리케이션으로 피드백하게 하도록 구성된 송신 모듈을 포함한다.

[0017] 본 출원의 실시형태에 의해 또한 제공되는 정보 인증 장치는, 비즈니스 애플리케이션에 의해 송신되고 제1 인증 정보를 반송하는 인증될 정보 획득 요청을 수신하도록 구성된 수신 모듈; 및 상기 제1 인증 정보를 인증하고, 상기 인증이 승인된 후에, 인증될 정보와 상기 인증될 정보의 아이덴티티 식별자를 상기 비즈니스 애플리케이션을 통해 인증 서버에 송신하여, 상기 인증 서버가 상기 제1 인증 정보, 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 인증하고, 인증 결과를 생성하고, 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하게 하도록 구성된 서명 모듈을 포함한다.

[0018] 본 출원의 실시형태에 의해 또한 제공되는 정보 인증 장치는, 비즈니스 애플리케이션에 의해 송신되는 인증될 정보에 대한 검증 요청을 수신하도록 구성된 인증 요청 수신 모듈; 상기 검증 요청에 따라, 제1 인증 정보를 생성하고 상기 제1 인증 정보를 상기 비즈니스 애플리케이션으로 피드백하도록 구성된 피드백 모듈; 상기 비즈니스 애플리케이션에 의해 송신되는, 상기 인증될 정보, 상기 인증될 정보의 인증될 아이덴티티 식별자, 및 상기 제1 인증 정보를 수신하도록 구성된 인증 정보 수신 모듈; 및 상기 제1 인증 정보, 상기 인증될 아이덴티티 식별자, 및 상기 인증될 정보를 각각 인증하여 인증 결과를 생성하고 상기 인증 결과를 상기 비즈니스 애플리케이션으로 피드백하도록 구성된 인증 모듈을 포함한다.

[0019] 본 출원의 실시형태들은 정보 등록 및 인증을 위한 방법 및 장치를 제공한다. 사용자가 비즈니스 서비스를 사용하는 동안 표준 정보를 등록해야 하는 경우, 비즈니스 애플리케이션은, 인증 서버에 표준 정보를 등록하기 위한 요청을 개시하고 인증 서버에 의해 피드백되는 제1 인증 정보를 수신한다. 이어서, 비즈니스 애플리케이션은, 표준 정보 획득 요청을 생성하고, 표준 정보 획득 요청 및 제1 인증 정보를 보안 정보 애플리케이션에 송신한다. 보안 정보 애플리케이션에 의한 제1 인증 정보의 인증이 승인된 후, 보안 정보 애플리케이션은, 자신

의 고유한 제2 인증 정보를 사용하여 표준 정보에 서명하고, 표준 정보의 아이덴티티 식별자를 결정한 후, 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 비즈니스 애플리케이션으로 피드백한다. 결과적으로, 비즈니스 애플리케이션은, 보안 정보 애플리케이션으로부터의 피드백 및 제1 인증 정보를 인증 서버에 송신하여, 인증 서버가 인증 후에 표준 정보 및 아이덴티티 표준 정보의 식별자를 등록하게 한다. 전술한 방식으로부터, 인증 서버의 식별자인 제1 인증 정보에 의해 보안 정보 애플리케이션이 표준 정보 등록자의 아이덴티티를 결정할 수 있고, 인증 서버에 의한 제1 인증 정보의 리턴에 의해, 인증 서버가 송신 중에 정보가 변조되었는지의 여부를 결정할 수 있는 한편, 인증 서버에 의한 서명된 표준 정보의 리턴에 의해, 표준 정보가 단말의 보안 정보 애플리케이션에 의해 제공된 것인지 여부를 인증 서버가 결정할 수 있음을 알 수 있다. 이러한 방식은, 송신 중에 인증 서버가 변조된 표준 정보를 정확하게 식별할 수 있음을 효과적으로 보장할 수 있으며, 이는 표준 정보 등록의 보안을 효과적으로 개선한다.

도면의 간단한 설명

[0020] 첨부 도면은 본 출원의 이해를 돕기 위해 제공된 것이며 본 출원의 일부를 구성한다. 본 출원의 예시적인 실시형태들 및 그 설명은, 본원을 설명하는 데 사용되며 본원에 대한 부적절한 한정사항을 구성하지 않는다. 첨부 도면에서,

도 1 내지 도 3은 본 출원의 일 실시형태에 따른 정보 등록 방법을 도시한 도면;

도 4는 본 출원의 일 실시형태에 따른 예시적인 애플리케이션 시나리오에서의 정보 등록 방법을 도시한 도면;

도 5 내지 도 7은 본 출원의 일 실시형태에 따른 정보 인증 방법을 도시한 도면;

도 8은 본 출원의 일 실시형태에 따라 예시적인 애플리케이션 시나리오에서의 정보 인증 프로세스를 도시한 도면;

도 9 내지 도 11은 본 출원의 일 실시형태에 따른 정보 등록 장치의 구조적 개략도;

도 12 내지 도 14는 본 출원의 일 실시형태에 관한 정보 인증 장치의 구조적 개략도.

발명을 실시하기 위한 구체적인 내용

[0021] 본 출원의 목적, 기술적 해결책, 및 이점을 더욱 명확하게 나타내도록, 이하에서는 본 출원의 기술적 해결책을 본 출원의 예시적 실시형태 및 첨부 도면을 참조하여 명확하고 완전하게 설명한다. 명백하게, 설명되는 실시형태들은 본 출원의 실시형태들 중 전부라기보다는 일부일 뿐이다. 본 출원의 실시형태를 기초로 하고 진보적 시도 없이 통상의 기술자가 취득할 수 있는 다른 모든 실시형태는 본 출원의 범위에 포함된다.

[0022] 전술한 바와 같이, 서비스 제공자가 표준 정보를 치음으로 수신한 경우, 표준 정보에 관련된 보안 정보를 미리 저장하지 않았기 때문에, 송신 동안 표준 정보가 조작된 것인지를 정확하게 결정할 수 없다. 그러나, 서비스 제공자와 단말이 일련의 인증 정보에 미리 합의하고 인증 정보를 사용하여 표준 정보를 인증하면, 송신 중에 표준 정보가 조작되었는지의 여부를 식별할 수 있다. 이에 기초하여, 이하의 정보 등록 및 인증 방법을 본원에 제공한다.

[0023] 도 1에 도시된 바와 같이, 본 출원의 일 실시형태에 따른 정보 등록 방법을 제공하며, 이 방법은 하기 단계들을 포함한다:

[0024] S101: 표준 정보를 등록하기 위한 요청을 인증 서버에 송신하는 단계.

[0025] 예시적인 응용 상황에서, 사용자가 비즈니스 애플리케이션에 제공된 상대적으로 높은 보안 수준의 비즈니스 서비스(예를 들어, 지문 지불 서비스)를 사용하는 경우, 사용자는 통상적으로 대응하는 보안 정보(예를 들어, 지문 정보)를 제공할 필요가 있다. 특히 사용자가 비즈니스 서비스를 처음으로 사용하는 경우, 사용자는, 통상적으로 비즈니스 서비스의 후속 사용에서 사용자가 입력한 보안 정보와의 비교 및 검증을 위해 보안 정보를 표준 정보로서 입력해야 한다.

[0026] 다시 말하면, 사용자가 비즈니스 서비스를 처음으로 사용하는 경우, 비즈니스 애플리케이션을 통해 대응 인증 서비스에 사용자에 의해 제공된 표준 정보를 등록할 필요가 있다. 따라서, 본 출원의 상술한 실시형태의 단계에서, 단말 내부에서 실행되는 비즈니스 애플리케이션은 표준 정보를 등록하기 위한 요청을 인증 서버에 송신할 수 있다.

[0027] 여기서, 본원에 설명되는 단말은, 휴대폰, 태블릿 컴퓨터, 및 스마트 시계와 같은 이동 단말을 포함하지만, 이에 한정되는 것은 아니며, 일부 상황에서는 컴퓨터 단말일 수도 있다. 인증 서버는, 서비스 공급자의 백엔드 서비스 시스템에서 보안 인증을 위한 서버일 수 있고 또는 보안 인증을 위한 전용 제삼자 서버일 수 있다. 분명하게, 이들은 본원에 대한 한정사항을 구성하지 않는다.

[0028] S102: 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하는 단계.

[0029] 제1 인증 정보는, 표준 정보를 등록하기 위한 요청을 송신하는 비즈니스 애플리케이션에 인증 서버에 의해 피드백되는 식별 정보이며, 인증 서버의 아이덴티티를 나타내는 데 사용된다. 본 출원의 실시형태의 상황에서, 제1 인증 정보는 인증 서비스의 인증서를 포함할 수 있다.

[0030] S103: 표준 정보 획득 요청을 생성하고, 표준 정보 획득 요청 및 제1 인증 정보를 보안 정보 애플리케이션에 송신하고, 보안 정보 애플리케이션이 제1 인증 정보의 인증을 승인한 후 보안 정보 애플리케이션에 의해 리턴되는, 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 획득하는 단계.

[0031] 여기서, 서명된 표준 정보는, 제2 인증 정보를 사용하여 보안 정보 애플리케이션에 의해 서명된 것이다.

[0032] 비즈니스 애플리케이션은, 인증 서버에 의해 피드백되는 제1 인증 정보를 수신함에 따라, 단말의 보안 정보 애플리케이션이 등록에 필요한 표준 정보를 제공하도록 표준 정보 획득 요청을 생성한다.

[0033] 본 출원의 보안 정보 애플리케이션은, 단말에서 실행되는 로컬 애플리케이션이며, 비즈니스 서비스에 필요한 (표준 정보를 포함하는) 보안 정보를 비즈니스 애플리케이션에 제공하는 데 사용된다는 점에 주목해야 한다. 그러나, 보안 정보는 사용자의 고유한 키 정보이다. 불법 조작자가 사용자의 보안 정보에 대한 보안 정보 애플리케이션을 요청하지 못하도록, 보안 정보 애플리케이션은 표준 정보를 사용하여 사용자의 아이덴티티를 인증한다. 이에 기초하여, 비즈니스 애플리케이션이 보안 정보 애플리케이션에 표준 정보 획득 요청을 송신할 때, 비즈니스 애플리케이션은 보안 정보 애플리케이션에 제1 인증 정보도 송신한다. 이어서, 보안 정보 애플리케이션은, 제1 인증 정보를 인증하여 인증 서버의 아이덴티티를 결정하고, 보안 정보 애플리케이션에 의한 제1 인증 정보의 인증이 승인된 후에만 표준 정보를 제공한다.

[0034] 보안 정보 애플리케이션에 의해 제공되는 표준 정보가 실제 애플리케이션에서 송신 동안 조작될 수 있다는 점을 고려할 때, 보안 정보 애플리케이션은, 현재 애플리케이션의 표준 정보를 피드백하기 전에 표준 정보에 대한 서명 동작을 수행하여, 표준 정보가 단말의 보안 정보 애플리케이션에 의해 송신되는 것임을 나타낸다. 한편, 표준 정보가 사용자에 의해 제공되는 것이라는 점도 고려할 때, 표준 정보의 아이덴티티 식별자를 결정하여, 표준 정보가 사용자에 의해 제공되는 것임을 나타낼 수 있다. 이처럼, 보안 정보 애플리케이션에 의해 비즈니스 애플리케이션으로 피드백되는 표준 정보에 대한 두 개의 식별자가 있으며, 이들 식별자는, 표준 정보가 단말의 보안 정보 애플리케이션에 의해 송신되는 것 및 표준 정보가 사용자에 의해 송신되는 것임을 각각 나타내도록 사용된다.

[0035] 일례로, 본 출원의 보안 정보 애플리케이션은, 제2 인증 정보를 사용하여 표준 정보가 보안 정보 애플리케이션에 의해 송신됨을 나타내는 표준 정보에 서명한다. 본원에서, 제2 인증 정보는, 인증 서버와 단말의 보안 정보 애플리케이션(또는 단말 자체) 간에 미리 합의된 제2키 정보일 수 있으며, 본원에서 특별히 한정되지는 않는다. 표준 정보의 아이덴티티 식별자는 또한 보안 정보 애플리케이션에 의해 결정될 수 있다. 본원에서, 표준 정보의 아이덴티티 식별자는 표준 정보의 아이덴티티 키 정보를 포함하고, 아이덴티티 키 정보는 통상적으로 사용자의 계정 정보에 연관된다. 다시 말하면, 한 쌍의 아이덴티티 키 정보는 하나의 계정 정보에 고유하게 대응하며, 이러한 점도, 표준 정보가 사용자에게 속한 것임을 나타낼 수 있다. 물론, 본원에서 특별한 제한은 없다.

[0036] S104: 서명된 표준 정보, 표준 정보의 아이덴티티 식별자, 및 제1 인증 정보를 인증 서버에 송신하여, 인증 서버가 제1 인증 정보의 인증을 승인하고 서명된 표준 정보에 따라 제2 인증 정보의 인증을 승인한 후에 인증 서버가 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록하게 하는 단계.

[0037] 비즈니스 애플리케이션은, 보안 정보 애플리케이션에 의한 피드백을 수신함에 따라, 보안 정보 애플리케이션에 의해 피드백되는 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를, 인증 서버에 의해 송신된 제1 인증 정보와 함께, 인증 및 등록을 위해 인증 서버에 송신한다.

[0038] 인증 서버는, 비즈니스 애플리케이션에 의해 송신된 상술한 정보를 수신하면, 수신된 정보에 대한 인증을 수행한다. 인증이 승인되면, 이것은, 보안 정보 애플리케이션에 의해 송신된 표준 정보가 송신 중에 조작되지 않았음을 나타내며, 이어서, 인증 서버는 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록할 수 있다. 이어서,

등록된 표준 정보 및 표준 정보의 아이덴티티 식별자는 사용자에 의해 후속 제공되는 보안 정보의 인증 및 식별에 사용될 수 있다.

[0039] 전술한 단계들을 대하여, 사용자가 비즈니스 서비스를 이용하면서 표준 정보를 등록할 필요가 있는 경우, 비즈니스 애플리케이션은 표준 정보를 등록하기 위한 요청을 인증 서버에 개시하고 인증 서버에 의해 피드백되는 제1 인증 정보를 수신한다. 이어서, 비즈니스 애플리케이션은, 표준 정보 획득 요청을 생성하고, 표준 정보 획득 요청 및 제1 인증 정보를 보안 정보 애플리케이션에 송신한다. 보안 정보 애플리케이션에 의한 제1 인증 정보의 인증이 승인된 후, 보안 정보 애플리케이션은, 자신의 고유한 제2 인증 정보를 사용하여 표준 정보에 서명하고, 표준 정보의 아이덴티티 식별자를 결정한 후, 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 비즈니스 애플리케이션으로 피드백한다. 결국, 비즈니스 애플리케이션은, 보안 정보 애플리케이션으로부터의 피드백 및 제1 인증 정보를 인증 서버에 송신하여, 인증 서버가 인증 후에 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록하게 한다. 전술한 방법으로부터, 인증 서버의 식별자인 제1 인증 정보에 의해, 보안 정보 애플리케이션이 표준 정보 등록자의 아이덴티티를 결정할 수 있고, 인증 서버의 제1 인증 정보의 리턴에 의해, 정보가 송신 중에 조작되었는지의 여부를 인증 서버가 결정할 수 있는 한편, 인증 서버의 서명된 표준 정보의 리턴에 의해, 표준 정보가 단말의 보안 정보 애플리케이션에 의해 제공된 것인지 여부를 인증 서버가 결정할 수 있음을 알 수 있다. 이러한 방법은, 인증 서버가 송신 중에 조작된 표준 정보를 정확하게 식별할 수 있음을 효과적으로 보장할 수 있으며, 이는 표준 정보 등록의 보안을 효과적으로 개선한다.

[0040] 전술한 제1 인증 정보와 관련하여, 제1 인증 정보는, 인증 서버의 식별자이며, 인증 서버의 아이덴티티를 식별하는 데 사용된다. 예를 들어, 인증 서버의 고유한 인증서가 제1 인증 정보로서 사용될 수 있다. 송신 중의 보안을 고려할 때, 인증 서버는 자신의 고유한 키 정보를 사용하여 인증서에 서명 동작을 수행할 수 있다. 이어서, 본 출원의 실시형태의 선택적 방식으로서, 전술한 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하는 단계(S102)는, 인증 서버에 의해 송신되고 인증 서버의 고유한 제1암호화 키를 이용하여 서명된 인증서를 수신하는 단계, 및 서명된 인증서를 제1 인증 정보로서 사용하는 단계를 포함한다.

[0041] 또한, 예시적인 애플리케이션의 일부 상황에서, 도전(challenge) 코드는, 인증 서버에 의해 비즈니스 애플리케이션으로 피드백되는 제1 인증 정보에 더 포함된다. 비즈니스 애플리케이션이 인증 서버에 요청을 송신한 후, 인증 서버는 비즈니스 애플리케이션으로 피드백되는 제1 인증 정보에 반송되는 고유 도전 코드를 생성한다. 하나의 도전 코드가 하나의 비즈니스 요청에만 해당하는 것으로 고려할 수 있다. 도전 코드를 채택함으로써, 재생 공격을 방지할 수 있다.

[0042] 위 내용은 단말의 비즈니스 애플리케이션의 관점에서 기술된 것이다. 표준 정보를 제공하는 보안 정보 애플리케이션과 관련하여, 본 출원의 일 실시형태에서는 정보 등록 방법을 또한 제공하며, 도 2에 도시된 바와 같이, 그 프로세스는 하기 단계들을 포함한다:

[0043] S201: 비즈니스 애플리케이션에 의해 송신되는, 제1 인증 정보와 표준 정보 획득 요청을 수신하는 단계.

[0044] 본 실시형태의 제1 인증 정보와 표준 정보 획득 요청은 전술한 바와 같으므로, 여기서 반복하지는 않는다.

[0045] S202: 제1 인증 정보를 인증하고, 인증이 승인된 후, 제2 인증 정보를 사용하여 서명된 표준 정보를 리턴하고 표준 정보의 아이덴티티 식별자를 비즈니스 애플리케이션으로 다시 리턴하여, 비즈니스 애플리케이션이 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 인증 서버에 송신하게 하고, 인증 서버가 제1 인증 정보의 인증을 승인하고 서명된 표준 정보에 따라 제2 인증 정보의 인증을 승인한 후에 인증 서버가 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록하게 하는 단계.

[0046] 보안 정보 애플리케이션은, 비즈니스 애플리케이션에 의해 송신된 제1 인증 정보 및 표준 정보 획득 요청을 수신하면, 제1 인증 정보를 먼저 인증하여 표준 정보 등록자의 아이덴티티를 결정한다. 보안 정보 애플리케이션이 인증 서버의 아이덴티티를 결정한 후에만, 보안 정보 애플리케이션은, 사용자가 제공한 표준 정보에 서명할 수 있고, 표준 정보의 아이덴티티 식별자를 결정할 수 있고, 서명된 표준 정보와 표준 정보의 아이덴티티 식별자를 비즈니스 애플리케이션으로 피드백할 수 있다. 이어서, 비즈니스 애플리케이션은, 보안 정보 애플리케이션에 의해 피드백된 일련의 정보를, 제1 인증 정보와 함께, 인증 서버에 의한 후속 인증을 위해 인증 서버에 송신한다. 또한, 인증이 승인되면, 인증 서버는 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록한다. 여기에서의 내용은 이전 방법의 프로세스와 동일하므로, 여기서 반복하지는 않는다.

[0047] 전술한 단계들에 대하여, 인증 서버의 아이덴티티는 인증 서버에 의해 제공되는 제1 인증 정보로 식별될 수 있고, 보안 정보 애플리케이션에 의한 제1 인증 정보의 인증은, 불법 조작자가 보안 정보 애플리케이션으로부터

표준 정보를 획득하는 것을 방지할 수 있다. 보안 정보 애플리케이션이 사용자에 의해 제공된 표준 정보에 서명하는 방식은 표준 정보가 보안 정보 애플리케이션에 의해 송신되었음을 나타내는 데 사용되는 한편, 표준 정보의 아이덴티티 식별자의 결정은 표준 정보가 사용자에 의해 제공되었음을 나타내는 데 사용된다. 명백하게, 보안 정보 애플리케이션에 의해 비즈니스 애플리케이션으로 피드백되는 표준 정보는 두 개의 식별자를 포함한다. 송신 중에 표준 정보가 조작되면, 표준 정보의 두 개의 식별자가 모두 변경된다. 이러한 방법은, 표준 정보가 송신 중에 조작되었는지의 여부를 효과적으로 반영할 수 있으므로, 결국 등록 동안 인증 서버의 보안을 보장한다.

[0048] 제2 인증 정보 및 표준 정보의 아이덴티티 식별자를 사용하여 서명된 표준 정보를 비즈니스 애플리케이션으로 다시 리턴하는 것은, 사용자에 의해 입력된 표준 정보를 수신하고, 제2 인증 정보를 사용하여 표준 정보에 서명하고, 표준 정보에 대하여 표준 정보의 아이덴티티 식별자를 결정하고, 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 비즈니스 애플리케이션으로 다시 리턴하는 것을 포함한다.

[0049] 전술한 바와 같이, 본 출원의 표준 정보의 아이덴티티 식별자는 표준 정보의 아이덴티티 키 정보를 포함할 수 있고, 아이덴티티 키 정보는 통상적으로 사용자의 계정 정보에 연관된 것이다. 송신 중에 아이덴티티 키 정보의 보안을 보장하도록, 보안 정보 애플리케이션은, 또한, 제2 인증 정보를 사용하여 아이덴티티 키 정보(즉, 표준 정보의 아이덴티티 식별자)에 본 출원의 실시형태의 최적의 방식으로 서명할 수 있다. 물론, 이는 본 출원의 한 정사항을 구성하지 않는다.

[0050] 유사하게, 전술한 바와 같이, 제1 인증 정보는 인증 서버의 아이덴티티를 나타낼 수 있으나, 본 출원의 한 방식에 있어서, 제1 인증 정보는 인증 서버의 고유한 인증서를 포함한다. 이러한 경우, 제1 인증 정보의 인증은, 인증 서버의 제1암호화 키와 일치하는 제1복호화 키를 사용하여 서명된 인증서를 복호화 및 인증하는 것을 포함한다.

[0051] 제2 인증 정보에 관하여, 본 출원의 일 실시형태에 따른 한 방법에 있어서, 제2 인증 정보는 인증 서버와 미리 합의된 제2키 정보를 포함하며, 제2키 정보는 제2암호화 키 및 제2복호화 키를 포함한다. 이러한 상황에서, 제2 인증 정보를 사용하여 표준 정보에 서명하는 것은, 인증 서버와 미리 합의된 제2암호화 키를 사용하여 표준 정보에 서명하는 것을 포함한다.

[0052] 표준 정보의 아이덴티티 식별자가 표준 정보의 아이덴티티 키 정보를 포함하는 경우, 전술한 제2 인증 정보는 아이덴티티 키 정보에 서명하는 데 사용될 수 있다. 이에 대한 내용은, 전술한 방식의 내용과 유사하므로, 여기서 반복하지는 않는다.

[0053] 전술한 내용은 단말에서 실행되는 보안 정보 애플리케이션의 관점에서의 설명이다. 인증 서버에 관하여, 본 출원의 일 실시형태에서는 도 3에 도시된 바와 같이 정보 등록 방법을 또한 제공하며, 프로세스는 하기 단계들을 포함한다:

[0054] S301: 인증 서버에 의해, 비즈니스 애플리케이션에 의해 송신된 표준 정보를 등록하기 위한 요청을 수신하는 단계;

[0055] S302: 표준 정보를 등록하기 위한 요청에 따라, 제1 인증 정보를 생성하고 제1 인증 정보를 비즈니스 애플리케이션으로 피드백하는 단계;

[0056] S303: 비즈니스 애플리케이션에 의해 송신되는, 서명된 표준 정보, 표준 정보의 아이덴티티 식별자, 및 제1 인증 정보를 수신하는 단계로서, 서명된 표준 정보는, 제2 인증 정보를 사용함으로써 서명되고 보안 정보 애플리케이션에 의해 비즈니스 애플리케이션에 송신되는 것인, 단계;

[0057] S304: 제1 인증 정보를 인증하고 서명된 표준 정보에 따라 제2 인증 정보를 인증하는 단계; 및

[0058] S305: 제1 인증 정보와 제2 인증 정보의 인증을 승인한 후에 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록하는 단계.

[0059] 도 1과 도 2에 도시된 상술한 방법들과 유사하게, 인증 서버는, 비즈니스 애플리케이션에 의해 송신되는 표준 정보를 등록하기 위한 요청을 수신하면, 인증 서버의 고유한 아이덴티티를 나타낼 수 있는 제1 인증 정보를 비즈니스 애플리케이션으로 피드백하며, 이때, 비즈니스 애플리케이션이 표준 정보를 등록하기 위한 요청을 보안 정보에 송신한 후, 보안 정보 애플리케이션은 제1 인증 정보에 따라 인증 서버의 아이덴티티를 결정할 수 있고, 이어서, 보안 정보 애플리케이션은 제2 인증 정보를 사용하여 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 비즈니스 애플리케이션으로 피드백한다. 인증 서버는, 비즈니스 애플리케이션에 의해 리턴되는 제1 인증

정보와 서명된 표준 정보를 수신하면, 제1 인증 정보에 대한 인증을 수행하고, 서명된 표준 정보에 따라 제2 인증 정보에 대한 인증을 수행한다. 인증이 모두 승인되면, 이는 표준 정보가 송신 중에 조작되지 않았음을 나타내며, 이에 따라 인증 서버는 후속 프로세스에서의 인증과 식별을 위해 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록한다.

[0060] 전술한 바와 같이, 인증 서버의 고유한 인증서는 인증 서버의 아이덴티티를 유효하게 증명할 수 있다. 한편, 보안 정보 애플리케이션에 의해 수신되는 인증서의 유효성을 보장하도록, 인증 서버는 통상적으로 자신의 고유한 인증서에 서명한다. 이어서, 보안 정보 애플리케이션은, 인증서가 송신 중에 조작되었는지의 여부를 식별할 수 있다. 따라서, 전술한 단계(S302)에 관하여, 표준 정보를 등록하기 위한 요청에 따라 제1 인증 정보를 생성하고 제1 인증 정보를 비즈니스 애플리케이션으로 피드백하는 것은, 표준 정보를 등록하기 위한 요청에 따라 인증 서버의 고유한 인증서를 인보크하고, 인증 서버의 고유한 제1암호화 키를 사용하여 인증서를 제1 인증 정보로서 서명하고, 제1 인증 정보를 비즈니스 애플리케이션으로 피드백하는 것을 포함한다.

[0061] 전술한 방법의 내용과 유사하게, 본 출원의 실시형태의 상황에서, 인증 서버는, 또한, 제1 인증 정보에 도전 코드를 포함할 수 있고, 인증 서버의 고유한 제1암호화 키를 사용하여 도전 코드에 서명한 후 이것을 비즈니스 애플리케이션에 송신할 수 있다. 이는 본원에 대한 한정사항을 구성하지 않는다.

[0062] 비즈니스 애플리케이션이 서명된 표준 정보 및 제1 인증 정보를 인증 서버에 송신한 후, 인증 서버는, 제1 인증 정보에 대한 인증을 수행하고 서명된 표준 정보에 따라 제2 인증 정보에 대한 인증을 수행한다.

[0063] 일례로, 제1 인증 정보에 대한 인증을 수행하는 것은 제1복호화 키를 사용하여 제1 인증 정보를 복호화 및 인증하는 것을 포함한다. 인증 서버는 자신의 제1복호화 키를 사용하여 제1 인증 정보를 복호화하고 인증한다. 복호화된 인증서(또는 도전 코드)가 변경되면, 이는, 인증서(또는 도전 코드)가 송신 중에 조작되었을 가능성이 매우 높음을 나타낸다. 따라서 인증 서버는 인증이 승인되지 않았다고 결정한다. 복호화된 인증서(또는 도전 코드)가 인증 서버에 의한 복호화 후에 변경되지 않으면, 인증이 승인된다.

[0064] 제2 인증 정보에 관하여, 제2 인증 정보는, 인증 서버와 보안 정보 애플리케이션에 의해 미리 합의된 제2키 정보를 포함하고, 이는 전술한 방법의 내용과 유사하며, 여기서 제2키 정보는 제2암호화 키와 제2복호화 키를 포함한다. 또한, 서명된 표준 정보는, 제2암호화 키를 사용하여 보안 정보 애플리케이션에 의해 서명된다. 이러한 상황에서, 서명된 표준 정보에 따라 제2 인증 정보를 인증하는 것은, 미리 합의된 제2키 정보에 따라, 보안 정보 애플리케이션과 미리 합의된 제2복호화 키를 사용하여 서명된 표준 정보를 복호화하여 제2 인증 정보를 인증하는 것을 포함한다.

[0065] 인증 서버가 합의된 제2복호화 키를 사용하여 서명된 표준 정보를 복호화하여 표준 정보를 취득하면, 표준 정보가 송신 중에 조작되지 않았으며 인증이 승인된 것이라고 간주할 수 있다. 복호화 후에 사용불가 정보가 취득되면, 이는, 서명된 정보가 미리 합의된 제2암호화 키에 의해 서명되지 않은 것이며 그 서명된 정보가 조작된 정보일 가능성이 높음을 나타낸다. 그 결과, 인증이 승인되지 않는다.

[0066] 인증 서버에 의한 인증이 승인된 후에만, 인증 서버가 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록할 수 있다.

[0067] 도 1 내지 도 3에 도시된 전술한 정보 등록 방법들은, 표준 정보가 송신 중에 조작되었는지의 여부를 인증 서버가 유효하게 식별할 수 있게 하며, 이는 사용자가 비즈니스 서비스를 사용하는 동안 불법 조작자에 의한 영향을 받지 않음을 보장한다.

[0068] 전술한 정보 등록 방법들은, 단말이 비즈니스 애플리케이션을 통해 비즈니스 서비스를 획득하는 임의의 상황에 적용될 수 있다. 또한, 전술한 인증 서버는 서비스 제공자의 백엔드 서비스 시스템의 인증 기능을 갖는 서버일 수 있다. 예시적인 응용 상황에서, 지불 서비스, 송신 서비스 등의 비즈니스 서비스를 비교적 높은 보안 수준 요건으로 제공할 수 있는 서비스 제공자는, 일반적으로, 비교적 높은 보안 수준 요건으로 비즈니스 서비스에 의해 요구되는 아이덴티티 인증 지원을 실현하도록 인터넷 파이낸스 인증 연합(IFAA)이라고 하는 네트워크 아이덴티티 인증 아키텍처를 사용한다. 다시 말하면, IFAA는 전술한 등록 프로세스를 구현하기 위한 인증 서버를 제공한다.

[0069] 이러한 상황에서, 상이한 장비 제조사들은, 또한, 이러한 제조사들에 의해 제조된 단말에서의 아이덴티티 인증에 의해 요구되는 인터페이스 또는 서비스를 제공하도록 IFAA에 의해 제공되는 아이덴티티 인증 아키텍처를 사용한다.

[0070] 전술한 본 출원의 등록 방법들을 명확하게 설명하도록, IFAA에 의해 제공되는 아이덴티티 인증 아키텍처에서의 등록에 대한 상세한 설명을 일례로 제공한다.

[0071] 도 4는, 본 실시형태에 따라 단말과 IFAA 인증 서버 간의 등록의 예시적인 적용 방법을 도시하며, 여기서 비즈니스 애플리케이션과 보안 정보 애플리케이션은 단말에서 실행된다. 비즈니스 애플리케이션은, 서비스 제공자의 비즈니스 서비스 액세스 포트로서, 단말의 사용자들에게 다양한 비즈니스 서비스를 제공할 수 있는 한편, 보안 정보 애플리케이션은 비즈니스 애플리케이션에 의해 요구되는 보안 정보(본 실시 형태에서는 표준 정보)를 제공하는 데 사용된다. 도 4에 도시된 프로세스는 하기 단계들을 포함한다:

[0072] S401: 비즈니스 애플리케이션이 표준 정보를 등록하기 위한 요청을 IFAA 인증 서버에 송신하는 단계.

[0073] 사용자가 비즈니스 애플리케이션의 비즈니스 서비스를 처음으로 사용하는 경우, 사용자의 생체 정보를 IFAA 인증 서버에 표준 정보로서 등록할 필요가 있다. 이때, 비즈니스 애플리케이션은 표준 정보를 등록하기 위한 요청을 IFAA 인증 서버에 송신한다.

[0074] S402: IFAA 인증 서버는 도전 코드와 인증서를 포함하는 서명된 데이터 팩을 비즈니스 애플리케이션으로 피드백하는 단계.

[0075] 여기서, 도전 코드는 재생 공격을 방지할 수 있고, 인증서는 IFAA 인증 서버의 고유한 아이덴티티를 나타내는 데 사용된다. 서명된 데이터 팩은 전술한 등록 방법에서의 제1 인증 정보라고 간주할 수 있다.

[0076] 또한, 이 단계에서, IFAA 인증 서버는 IFAA S 키 정보를 사용하여 전술한 데이터 팩에 서명하고, IFAA S 키 정보는 IFAA 인증 서버 자체에 의해 생성된다는 점에 주목해야 한다. 반면, IFAA 인증 서버의 고유한 인증서는 BIOM(Biometric Manage) 키 정보에 의해 서명되고, BIOM 키 정보는 비즈니스 서비스를 제공하는 서비스 공급자의 유형을 나타내는 데 사용된다.

[0077] S403: 비즈니스 애플리케이션이 표준 정보 획득 요청을 생성하고, 표준 정보 획득 요청과 서명된 데이터 팩을 IFAA 서비스를 통해 보안 정보 애플리케이션에 송신한다.

[0078] 여기서, IFAA 서비스는 단말에 배치된 IFAA 아이덴티티 인증 아키텍처에 의해 제공되는 서비스이다. 예시적인 응용 상황의 한 방법에 있어서, 비즈니스 애플리케이션은 IFAA SDK(IFAA 아이덴티티 인증 아키텍처에 기초한 통신 툴)를 통해 IFAA 서비스를 호출할 수 있으며, 이것은 본원에서 특정하게 한정되지 않는다.

[0079] S404: 보안 정보 애플리케이션이 서명된 데이터 팩을 인증하고, 인증이 승인된 후, 표준 정보에 서명하는 단계.

[0080] 보안 정보 애플리케이션은, 먼저, 서명된 데이터 팩을 복호화할 필요가 있으며(예를 들어, IFAA 키 정보를 사용하여 복호화를 수행할 수 있으나, 본원에서 특정하게 한정되지는 않음), 복호화 후에, 인증 데이터 팩의 인증서를 사용하여 이것이 IFAA 등록 표준 정보(BIOM 키 정보가 인증서의 복호화 및 인증에 사용될 수 있음)인지 여부를 인증한다는 점에 주목해야 한다.

[0081] 인증이 승인된 후, 보안 정보 애플리케이션은, 사용자에 의해 입력되는 생체 정보를 표준 정보로서 획득하고, DA(장치 인증기) 키 정보를 사용하여 표준 정보에 서명하며, 여기서, DA 키 정보는 단말의 아이덴티티를 나타내는 데 사용된다(일례로, DA 키 정보는 보안 정보 애플리케이션의 아이덴티티를 나타낼 수 있는 한편, 보안 정보 애플리케이션은 장비 제조사에 의해 단말에 배치된다. 따라서, DA 키 정보도 단말의 아이덴티티를 나타낸다).

[0082] S405: 서명된 표준 정보에 따라 표준 정보의 아이덴티티 키 정보를 결정하는 단계.

[0083] 본 실시형태에서, 표준 정보의 아이덴티티 키 정보는, 통상적으로 비즈니스 애플리케이션에서 사용자에 의해 사용되는 계정 정보와 연관되어 표준 정보가 속하는 사용자를 나타낸다. 예시적인 응용에 있어서, 표준 정보의 아이덴티티 키 정보를 생성하기 위해, IFAA 서비스는, 키스토어(KeyStore)(REE 환경에서의 보안 저장 표준 호출 인터페이스)를 통해 키마스터(KeyMaster)(보안 저장 모듈)를 호출할 수 있고, 키마스터는 아이덴티티 키 정보를 생성한다.

[0084] 송신 중에 아이덴티티 키 정보의 보안을 보장하기 위해, 보안 정보 애플리케이션이 DA 키 정보를 사용하여 아이덴티티 키 정보에 서명할 수 있다는 점에 주목해야 한다.

[0085] S406: 보안 정보 애플리케이션이, 단말 인증서, 서명된 표준 정보, 및 서명된 아이덴티티 키 정보를 비즈니스 애플리케이션으로 다시 리턴하는 단계.

[0086] S407: 단말 인증서, 서명된 표준 정보, 및 서명된 아이덴티티 키 정보를 IFAA 서비스를 통해 IFAA 인증 서버에

송신하는 단계.

[0087] 단말 인증서는, IFAA 아이덴티티 인증 아키텍처에 참여하는 장비 제조사에 의해 제조된 장비에 있어서 이러한 장비 제조사에 의해 제공되는 인증기 인증서라고도 한다는 점에 주목해야 한다. 다시 말하면, 단말 인증서는, 단말이 IFAA 아이덴티티 인증 아키텍처를 사용하는지의 여부를 나타낼 수 있다.

[0088] 본 실시형태에 따른 방법에서, 전술한 도전 코드와 IFAA 인증 서버의 고유한 인증서도 IFAA 인증 서버로 동시에 리턴될 수 있다. 이처럼, IFAA 인증 서버는 도전 코드와 IFAA 인증 서버의 고유한 인증서를 또한 인증할 수 있다.

[0089] S408: IFAA 인증 서버가 수신된 정보를 인증하고, 인증이 승인된 후, 표준 정보 및 표준 정보의 아이덴티티 키 정보를 등록하는 단계.

[0090] IFAA 인증 서버는 단말 인증서를 먼저 인증한다는 점에 주목해야 한다. 예를 들어, IFAA 인증 서버는, IFAA 키 정보를 사용하여 수신된 정보를 복호화하고 단말 인증서의 유효성을 인증할 수 있다. 인증이 승인된 후, IFAA 인증 서버는 DA 키 정보를 사용하여 아이덴티티 키 정보를 복호화하고 인증한다. 양측이 승인되면, 송신 중에 표준 정보가 조작되지 않았다고 간주할 수 있으며, IFAA 인증 서버는 표준 정보 및 표준 정보의 아이덴티티 키 정보를 등록한다.

[0091] S409: 등록 결과를 비즈니스 애플리케이션으로 피드백하는 단계.

[0092] 전술한 실시형태들에 있어서, 예시적인 응용 상황에서, 다양한 키 정보를 사용하여 표준 정보가 송신 중에 조작되었는지의 여부를 정확하게 결정할 수 있음을 알 수 있다.

[0093] 전술한 내용은 표준 정보 등록 방법을 설명한다. 표준 정보가 등록된 후, 사용자는 해당 비즈니스 서비스를 사용할 수 있다. 사용자가 비즈니스 서비스를 사용하는 경우, 사용자의 보안 정보를 제공해야 한다. 대응하여, 인증 서버는 비즈니스 서비스를 사용하는 동안 사용자에 의해 제공되는 보안 정보에 따라 인증을 수행할 수 있다. 따라서, 본 출원의 일 실시형태에서는, 정보 인증 방법을 또한 제공하며, 도 5에 도시된 바와 같이, 그 방법은 하기 단계들을 포함한다:

[0094] S501: 인증될 정보에 대한 검증 요청을 인증 서버에 송신하는 단계.

[0095] 사용자가 비즈니스 애플리케이션에서 비즈니스 서비스(예를 들어, 지문 지불 서비스)를 사용하는 경우, 사용자는 미리 등록된 표준 정보와의 비교를 위해 자신의 보안 정보(예를 들어, 지문 정보)를 제공해야 하는 경우가 종종 있다. 이때, 비즈니스 애플리케이션은, 사용자의 보안 정보를, 인증될 정보로서 획득하고, 후속하여 인증 및 검증을 위해 인증 서버에 송신한다.

[0096] 상술한 상황에서, 비즈니스 애플리케이션은 인증될 정보에 대한 검증 요청을 인증 서버에 송신한다.

[0097] S502: 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하는 단계.

[0098] 전술한 등록 방법과 유사하게, 제1 인증 정보는 인증 서버의 아이덴티티를 나타내므로, 여기서 반복하지는 않는다.

[0099] S503: 제1 인증 정보에 따라 인증될 정보 획득 요청을 생성하고, 인증될 정보 획득 요청을 보안 정보 애플리케이션에 송신하고, 보안 정보 애플리케이션에 의해 제공되는 인증될 정보 및 인증될 정보의 인증될 아이덴티티 식별자를 획득하는 단계.

[0100] 유사하게, 보안 정보 애플리케이션은, 제1 인증 정보에 따라 인증될 당사자의 아이덴티티를 결정한다. 인증될 당사자의 아이덴티티가 유효한 것으로 결정되고 인증이 승인된 후, 보안 정보 애플리케이션은, 또한, 사용자에 의해 제공되는 인증될 정보 및 인증될 정보의 인증될 아이덴티티 식별자를 비즈니스 애플리케이션으로 다시 리턴한다.

[0101] 전술한 등록 방법과는 달리, 인증될 정보에 서명하는 데 제2 인증 정보를 사용할 필요가 없다.

[0102] S504: 인증될 정보, 인증될 아이덴티티 식별자, 및 제1 인증 정보를 인증 서버에 송신하여, 인증 서버가 제1 인증 정보, 인증될 아이덴티티 식별자, 및 인증될 정보를 인증하고, 인증 결과를 생성하고, 인증 결과를 비즈니스 애플리케이션으로 피드백하게 하는 단계.

[0103] 위 내용으로부터, 제1 인증 정보와 인증될 아이덴티티 식별자를 통해, 인증될 정보가 송신 중에 조작되었는지의

여부를 식별할 수 있다. 인증이 승인된 후, 인증 서버는 인증될 정보에 대한 인증을 수행할 수 있다.

[0104] 본 출원의 일 실시형태에서는, 정보 인증 방법을 또한 제공하며, 도 6에 도시된 바와 같이, 방법은 하기 단계들을 포함한다:

[0105] S601: 비즈니스 애플리케이션에 의해 송신되며 제1 인증 정보를 반송하는 인증될 정보 획득 요청을 수신하는 단계.

[0106] S602: 제1 인증 정보를 반송하는 표준 정보 획득 요청에 따라, 인증될 정보 및 인증될 정보의 아이덴티티 식별자를 비즈니스 애플리케이션을 통해 인증 서버에 송신하여, 인증 서버가 제1 인증 정보, 인증될 아이덴티티 식별자, 및 인증될 정보를 인증하고, 인증 결과를 생성하고, 인증 결과를 비즈니스 애플리케이션으로 피드백하게 하는 단계.

[0107] 위 단계(S602)에 관하여, 제1 인증 정보를 반송하는 표준 정보 획득 요청에 따라, 인증될 정보 및 인증될 정보의 아이덴티티 식별자를 비즈니스 애플케이션으로 다시 송신하는 것은, 표준 정보 획득 요청에 반송되는 제1 인증 정보를 인증하고, 인증이 승인된 후, 사용자에 의해 입력되는 인증될 정보를 수신하고, 인증될 정보가 속하는 표준 정보를 식별하고, 표준 정보에 일치하는 아이덴티티 표준을 인증될 정보의 인증될 아이덴티티 식별자라고 결정하고, 인증될 정보와 인증될 정보의 인증될 아이덴티티 식별자를 비즈니스 애플리케이션으로 다시 리턴하는 것을 포함한다.

[0108] 본 출원의 일 실시형태에서는, 정도 인증 방법을 또한 제공하며, 도 7에 도시된 바와 같이, 방법은 하기 단계들을 포함한다:

[0109] S701: 인증 서버에 의해, 비즈니스 애플리케이션에 의해 송신되는 인증될 정보에 대한 검증 요청을 수신하는 단계;

[0110] S702: 검증 요청에 따라, 제1 인증 정보를 생성하고 제1 인증 정보를 비즈니스 애플리케이션으로 피드백하는 단계;

[0111] S703: 비즈니스 애플리케이션에 의해 송신되는, 인증될 정보, 인증될 정보의 아이덴티티 식별자, 및 제1 인증 정보를 수신하는 단계;

[0112] S704: 제1 인증 정보, 아이덴티티 식별자, 및 인증될 정보를 각각 인증하여 인증 결과를 생성하고 인증 결과를 비즈니스 애플리케이션으로 피드백하는 단계.

[0113] 위 단계(S704)에 관하여, 인증 서버는 비즈니스 애플리케이션에 의해 송신되는 정보를 각각 인증한다는 점에 주목해야 한다. 일례로, 제1 인증 정보, 아이덴티티 식별자, 및 인증될 정보를 각각 인증하는 것은, 제1 인증 정보에 관하여, 인증 서버의 제1복호화 키를 사용하여 제1 인증 정보를 복호화하고 복호화된 인증서를 인증하는 것을 포함하고, 아이덴티티 식별자에 관하여, 등록된 표준 정보의 아이덴티티 식별자에 따라, 아이덴티티 식별자가 등록된 표준 정보의 아이덴티티 식별자와 일치하는지의 여부를 결정하고, 인증을 위해 인증될 정보를 등록된 표준 정보와 비교하는 것을 포함한다.

[0114] 예시적인 응용 상황에서, 인증 서버는, 인증 프로세스 동안 인증 서버에 의한 임의의 정보의 인증이 승인되지 않으면 실패 통지를 피드백할 수 있고, 인증 서버에 의한 모든 정보의 인증이 승인될 때에만 성공 통지를 피드백할 수 있다. 일례로, 인증 결과를 생성하고 인증 결과를 비즈니스 애플리케이션으로 피드백하는 것은, 제1 인증 정보에 관하여, 인증이 승인되면 인증될 정보와 인증될 아이덴티티 식별자를 인증하고, 인증이 승인되지 않으면 인증 실패 통지를 리턴하고, 아이덴티티 식별자에 관하여, 인증이 승인되면 인증될 정보를 인증하고, 인증이 승인되지 않으면 인증 실패 통지를 리턴하고, 인증될 정보에 관하여, 인증이 승인되면 성공 통지를 리턴하고, 인증이 승인되지 않으면 인증 실패 통지를 리턴한다.

[0115] 전술한 등록 프로세스에 대응하여, 본 출원의 전술한 인증 방법들을 명확하게 설명하도록, 일례로 IFAA에 의해 제공되는 아이덴티티 인증 아키텍처에서의 인증을 상세히 설명한다.

[0116] 도 8은 본 실시형태에서의 단말과 IFAA 인증 서버 간의 인증의 예시적인 적용 방법을 도시한다. 도시된 프로세스는 하기 단계들을 포함한다:

[0117] S801: 비즈니스 애플리케이션이 인증될 정보 검증 요청을 IFAA 인증 서버에 송신하는 단계;

[0118] S802: IFAA 인증 서버가 도전 코드와 인증서를 포함하는 서명된 데이터 팩을 비즈니스 애플리케이션으로 피드백

하는 단계;

[0119] S803: 비즈니스 애플리케이션이, 인증될 정보 획득 요청을 생성하고, 인증될 정보 획득 요청과 서명된 데이터 팩을 IFAA 서비스를 통해 보안 정보 애플리케이션에 송신하는 단계;

[0120] S804: 보안 정보 애플리케이션이, 서명된 데이터 팩을 인증하고, 인증이 승인된 후, 등록 프로세스에서 인증될 정보에 의해 사용되는 아이덴티티 키 정보에 서명하는 단계;

[0121] S805: 보안 정보 애플리케이션이 서명된 인증될 정보를 비즈니스 애플리케이션으로 다시 리턴하는 단계;

[0122] S806: 서명된 인증될 정보를 IFAA 서비스를 통해 IFAA 인증 서버에 송신하는 단계;

[0123] S807: 수신된 서명된 인증될 정보에 관하여, IFAA 인증 서버가, 등록된 아이덴티티 키 정보를 사용하여 서명된 인증될 정보를 인증하고, 인증이 승인된 후, 인증을 위해 인증될 정보를 등록된 표준 정보와 비교하는 단계;

[0124] S808: 인증 결과를 비즈니스 애플리케이션으로 다시 리턴하는 단계.

[0125] 정보 송신 방법을 본 출원의 다양한 실시형태에 의해 전술하였다. 마찬가지로, 본 출원의 실시형태들은 또한 정보 등록 장치를 제공한다. 도 9에 도시된 바와 같이, 장치는, 표준 정보 등록 요청을 인증 서버에 송신하도록 구성된 등록 요청 모듈(901); 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하도록 구성된 수신 모듈(902); 표준 정보 획득 요청을 생성하고, 표준 정보 획득 요청 및 제1 인증 정보를 보안 정보 애플리케이션에 송신하고, 보안 정보 애플리케이션이 제1 인증 정보의 인증을 승인한 후 보안 정보 애플리케이션에 의해 리턴되는, 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 획득하고, 여기서, 서명된 표준 정보는 제2 인증 정보를 사용하여 보안 정보 애플리케이션에 의해 서명된 것이도록 구성된 획득 모듈(903); 및 서명된 표준 정보, 표준 정보의 아이덴티티 식별자, 및 제1 인증 정보를 인증 서버에 송신하여, 인증 서버가 제1 인증 정보의 인증을 승인하고 서명된 표준 정보에 따라 제2 인증 정보의 인증을 승인한 후에 인증 서버가 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록하게 하도록 구성된 송신 모듈(904)을 포함한다.

[0126] 수신 모듈(902)은, 인증 서버에 의해 송신되고 인증 서버의 고유한 제1암호화 키를 사용하여 서명된 인증서를 수신하고 서명된 인증서를 제1 인증 정보로서 사용하도록 구성된다.

[0127] 도 10에 도시된 바와 같이, 본 출원의 실시형태들은 또한 정보 등록 장치를 제공하며, 이 장치는, 비즈니스 애플리케이션에 의해 송신되는 제1 인증 정보와 표준 정보 획득 요청을 구성된 수신 모듈(1001), 및 서명 모듈(1002)을 포함하고, 서명 모듈은, 제1 인증 정보를 인증하고, 인증이 승인된 후, 제2 인증 정보를 사용하여 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 비즈니스 애플리케이션으로 다시 리턴하여, 비즈니스 애플리케이션이 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 인증 서버에 송신하게 하고, 인증 서버가 제1 인증 정보의 인증을 승인하고 서명된 표준 정보에 따라 제2 인증 정보의 인증을 승인한 후에 인증 서버가 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록하게 하도록 구성된다.

[0128] 서명 모듈(1002)은, 사용자에 의해 입력되는 표준 정보를 수신하고, 제2 인증 정보를 사용하여 표준 정보에 서명하고, 표준 정보에 대하여 표준 정보의 아이덴티티 식별자를 결정하고, 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 비즈니스 애플리케이션으로 다시 리턴하도록 구성된다.

[0129] 표준 정보의 아이덴티티 식별자는 표준 정보의 아이덴티티 키 정보를 포함하고, 아이덴티티 키 정보는 사용자의 계정 정보에 연관된 것이라는 점에 주목해야 한다.

[0130] 제1 인증 정보가 인증 서버의 서명된 인증서를 포함하는 상황에서, 서명 모듈(1002)은, 인증 서버의 제1암호화 키에 일치하는 제1복호화 키를 사용하여 서명된 인증서를 복호화 및 인증한다.

[0131] 제2 인증 정보는 인증 서버와 미리 합의된 제2키 정보를 포함하고, 제2키 정보는 제2암호화 키 및 제2복호화 키를 포함한다. 서명 모듈(1002)은, 인증 서버와 미리 합의된 제2암호화 키를 사용하여 표준 정보에 서명하도록 구성된다.

[0132] 도 11에 도시된 바와 같이, 본 출원의 실시형태들은 정보 등록 장치를 또한 제공하며, 이 장치는, 비즈니스 애플리케이션에 의해 송신되는 표준 정보를 등록하기 위한 요청을 수신하도록 구성된 등록 요청 수신 모듈(1101); 표준 정보를 등록하기 위한 요청에 따라, 제1 인증 정보를 생성하여 비즈니스 애플리케이션으로 피드백하도록 구성된 피드백 모듈(1102); 비즈니스 애플리케이션에 의해 송신되는, 서명된 표준 정보, 표준 정보의 아이덴티티 식별자, 제1 인증 정보를 수신하도록 구성된 등록 정보 수신 모듈(1103)로서, 서명된 표준 정보는 보안 정보 애플리케이션에 의해 제2 인증 정보를 사용하여 서명되고 비즈니스 애플리케이션에 송신되는 것인, 상기 등록

정보 수신 모듈; 제1 인증 정보를 인증하고, 서명된 표준 정보에 따라 제2 인증 정보를 인증하도록 구성된 인증 모듈(1104); 및 제1 인증 정보와 제2 인증 정보의 인증이 모두 승인된 후에 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록하도록 구성된 등록 모듈(1105)을 포함한다.

[0133] 일례로, 피드백 모듈(1102)은, 표준 정보를 등록하기 위한 요청에 따라, 인증 서버의 고유한 인증서를 인보크하고, 인증 서버의 고유한 제1암호화 키를 사용하여 제1 인증 정보로서의 인증서에 서명하여 이를 비즈니스 애플리케이션으로 피드백하도록 구성된다.

[0134] 인증 모듈(1104)은 제1복호화 키를 사용하여 제1 인증 정보를 복호화 및 인증하도록 구성된다.

[0135] 제2 인증 정보는 인증 서버 및 보안 정보 애플리케이션에 의해 미리 합의된 제2키 정보를 포함하고, 제2키 정보는 제2암호화 키 및 제2복호화 키를 포함하고, 서명된 표준 정보는, 제2암호화 키를 사용하여 보안 정보 애플리케이션에 의해 서명된 것이다. 이러한 상황에서, 인증 모듈(1104)은, 미리 합의된 제2키 정보에 따라, 보안 정보 애플리케이션과 미리 합의된 제2복호화 키를 사용하여 서명된 표준 정보를 복호화하여 제2 인증 정보를 인증하도록 구성된다.

[0136] 도 12에 도시된 바와 같이, 본 출원의 실시형태들은 정보 인증 장치를 또한 제공하며, 이 장치는, 인증될 정보에 대한 검증 요청을 인증 서버에 송신하도록 구성된 등록 요청 모듈(1201); 인증 서버에 의해 피드백되는 제1 인증 정보를 수신하도록 구성된 수신 모듈(1202); 인증될 정보 획득 요청을 생성하고, 인증될 정보 획득 요청 및 제1 인증 정보를 보안 정보 애플리케이션에 송신하고, 보안 정보 애플리케이션이 제1 인증 정보의 인증을 승인한 후에 보안 정보 애플리케이션에 의해 리턴되는, 인증될 정보 및 인증될 정보의 인증될 아이덴티티 식별자를 획득하도록 구성된 획득 모듈(1203); 인증될 정보, 인증될 아이덴티티 식별자, 및 제1 인증 정보를 인증 서버에 송신하여, 인증 서버가 제1 인증 정보, 인증될 아이덴티티 식별자, 및 인증될 정보를 인증하고, 인증 결과를 생성하고, 인증 결과를 비즈니스 애플리케이션으로 피드백하게 하도록 구성된 송신 모듈(1204)을 포함한다.

[0137] 도 13에 도시된 바와 같이, 본 출원의 실시형태들은 정보 인증 장치를 또한 제공하며, 이 장치는, 비즈니스 애플리케이션에 의해 송신되고 제1 인증 정보를 반송하는 인증될 정보 획득 요청을 수신하도록 구성된 수신 모듈(1301); 및 제1 인증 정보를 인증하고, 인증이 승인된 후, 인증될 정보 및 인증될 정보의 아이덴티티 식별자를 비즈니스 애플리케이션을 통해 인증 서버에 송신하여, 인증 서버가 제1 인증 정보, 인증될 아이덴티티 식별자, 및 인증될 정보를 인증하고, 인증 결과를 생성하고, 인증 결과를 비즈니스 애플리케이션으로 피드백하게 하도록 구성된 서명 모듈(1302)을 포함한다.

[0138] 일례로, 서명 모듈(1302)은, 표준 정보 획득 요청에 반송되는 제1 인증 정보를 인증하고, 인증이 승인된 후, 인증될 정보가 속하는 표준 정보를 식별하고, 표준 정보에 일치하는 아이덴티티 표준을 인증될 정보의 인증될 아이덴티티 식별자라고 결정하고, 인증될 정보 및 인증될 정보의 인증될 아이덴티티 식별자를 비즈니스 애플리케이션으로 다시 리턴하도록 구성된다.

[0139] 도 14에 도시된 바와 같이, 본 개시 내용의 실시형태들은 정보 인증 장치를 또한 제공하며, 이 장치는, 비즈니스 애플리케이션에 의해 송신되는 인증될 정보에 대한 검증 요청을 수신하도록 구성된 인증 요청 수신 모듈(1401); 검증 요청에 따라, 제1 인증 정보를 생성하여 비즈니스 애플리케이션으로 피드백하도록 구성된 피드백 모듈(1402); 비즈니스 애플리케이션에 의해 송신되는, 인증될 정보, 인증될 정보의 인증될 아이덴티티 식별자, 및 제1 인증 정보를 수신하도록 구성된 인증 정보 수신 모듈(1403); 및 제1 인증 정보, 인증될 아이덴티티 식별자, 및 인증될 정보를 각각 인증하여 인증 결과를 생성하고 인증 결과를 비즈니스 애플리케이션으로 피드백하도록 구성된 인증 모듈(1404)을 포함한다.

[0140] 인증 모듈(1404)은, 제1 인증 정보에 관하여, 정보 인증 장치의 제1복호화 키를 사용하여 제1 인증 정보를 복호화하고 복호화된 인증서를 인증하고, 인증될 아이덴티티 식별자에 관하여, 등록된 표준 정보의 아이덴티티 식별자에 따라, 인증될 아이덴티티 식별자가 등록된 표준 정보의 아이덴티티 식별자와 일치하는지의 여부를 결정하고, 인증을 위해 인증될 정보를 등록된 표준 정보와 비교하도록 구성된다.

[0141] 인증 모듈(1404)은, 제1 인증 정보에 관하여, 인증이 승인되면 인증될 정보 및 인증될 아이덴티티 식별자를 인증하고, 인증이 승인되지 않으면 인증 실패 통지를 리턴하고, 아이덴티티 식별자에 관하여, 인증이 승인되면 인증될 정보를 인증하고 인증이 승인되지 않으면 인증 실패 통지를 리턴하고, 인증될 정보에 관하여, 인증이 승인되면 성공 통지를 리턴하고 인증이 승인되지 않으면 인증 실패 통지를 리턴하도록 구성된다.

[0142] 통상적인 구성에서, 계산 장치는, 하나 이상의 중앙 처리 유닛(CPU), 입력/출력 인터페이스, 네트워크 인터페이

스, 및 메모리를 포함한다.

[0143] 메모리는, 휘발성 메모리, 랜덤 액세스 메모리(RAM), 및/또는 비휘발성 메모리, 예를 들어, 판독 전용 메모리(ROM) 또는 플래시 RAM과 같은 컴퓨터 판독가능 매체를 포함할 수 있다. 메모리는 컴퓨터 판독가능 매체의 일례이다.

[0144] 컴퓨터 판독가능 매체는, 임의의 방법 또는 기술을 통해 정보 저장을 구현할 수 있는 영구 매체, 휘발성 매체, 이동형 매체, 및 고정형 매체를 포함한다. 정보는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 다른 데이터일 수 있다. 컴퓨터의 저장 매체의 예로는, 상 변화 RAM(PRAM), 정적 RAM(SRAM), 동적 RAM(DRAM), 다른 유형의 RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, DVD 또는 다른 광학 메모리, 카세트, 카세트와 디스크 메모리 또는 다른 자기 메모리 장치 또는 연산 장치에 액세스 가능한 정보를 저장하는 데 사용될 수 있는 다른 임의의 비전송 매체를 포함할 수 있지만, 이에 한정되지는 않는다. 본 출원의 정의에 따르면, 컴퓨터 판독가능 매체는 변조된 데이터 신호 및 캐리어와 같은 일시적 매체를 포함하지 않는다.

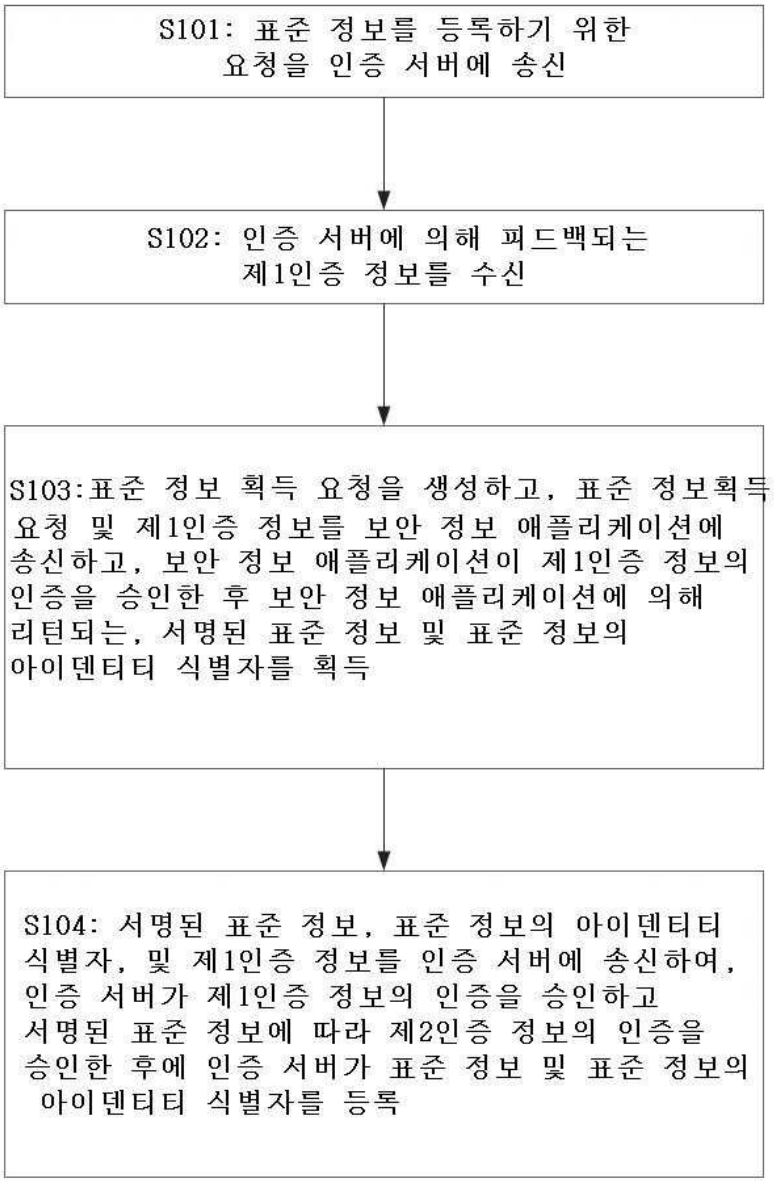
[0145] 또한, "포함하는"(including), "포함하는"(comprising), 또는 다른 임의의 변형 용어들은, 일련의 요소를 포함하는 프로세스, 방법, 상품, 또는 장치가, 이러한 요소들을 포함할 뿐만 아니라, 특정하게 열거되는 다른 요소들도 포함하거나 프로세스, 방법, 상품, 또는 장치에 대하여 고유한 요소들을 더 포함하는 것처럼 비배타적 포함을 나타내고자 하는 것이다. 추가 제한이 없는 경우, "하나를 포함하는"이라는 문구에 의해 정의되는 요소들은, 해당 요소들을 포함하는 프로세스, 방법, 상품, 또는 장치가 동일한 추가 요소를 더 포함하는 것을 배제하지 않는다.

[0146] 통상의 기술자는 본 출원의 실시형태들이 방법, 시스템, 또는 컴퓨터 프로그램 제품으로서 제공될 수 있음을 이해해야 한다. 따라서, 본원은, 완전한 하드웨어 실시형태, 완전한 소프트웨어 실시형태, 또는 소프트웨어와 하드웨어를 결합한 실시형태로서 구현될 수 있다. 또한, 본원은, 컴퓨터 사용가능 프로그램 코드를 포함하는 하나 이상의 컴퓨터 사용가능 저장 매체(자기 디스크 메모리, CD-ROM, 광학 메모리 등을 포함하지만, 이에 한정되지는 않음)에 구현된 컴퓨터 프로그램 제품의 형태일 수 있다.

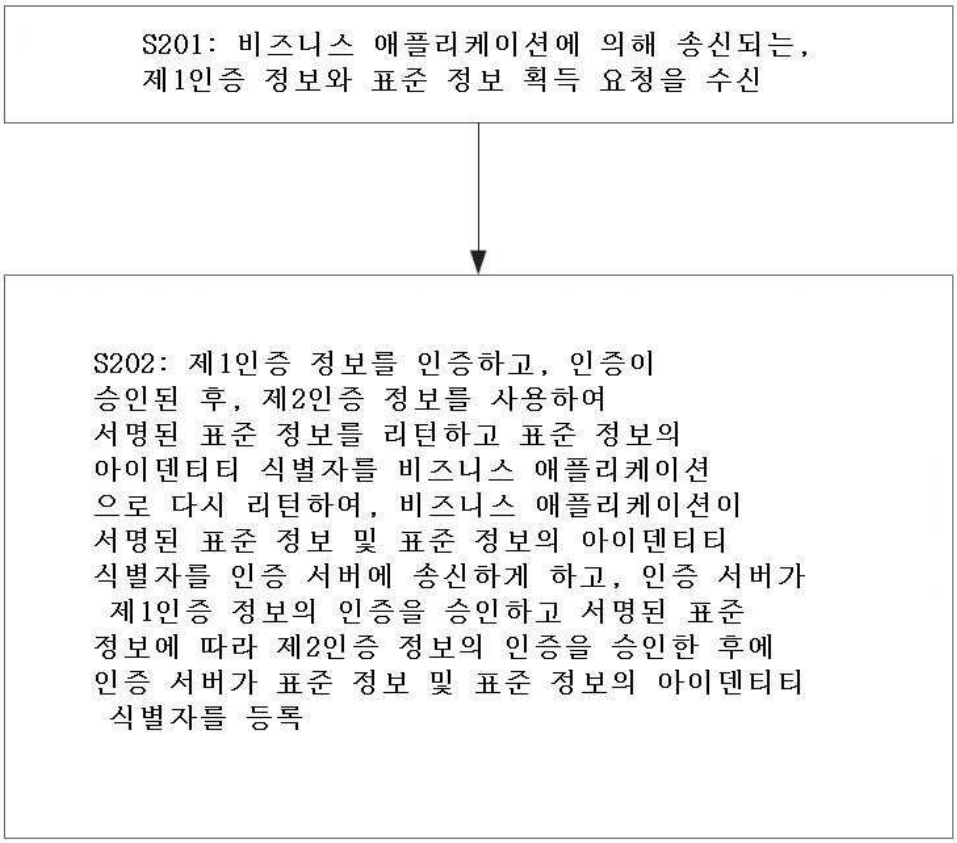
[0147] 본 출원의 실시형태만을 상술하였지만, 이는 본원을 한정하는 데 사용되지 않는다. 통상의 기술자라면, 본원은 다양한 변형예 및 변경예를 가질 수 있다. 본 출원의 사상과 및 원리 내에서 이루어지는 임의의 수정, 균등한 대체, 또는 개선은 본 출원의 청구범위에 의해 포함된다.

도면

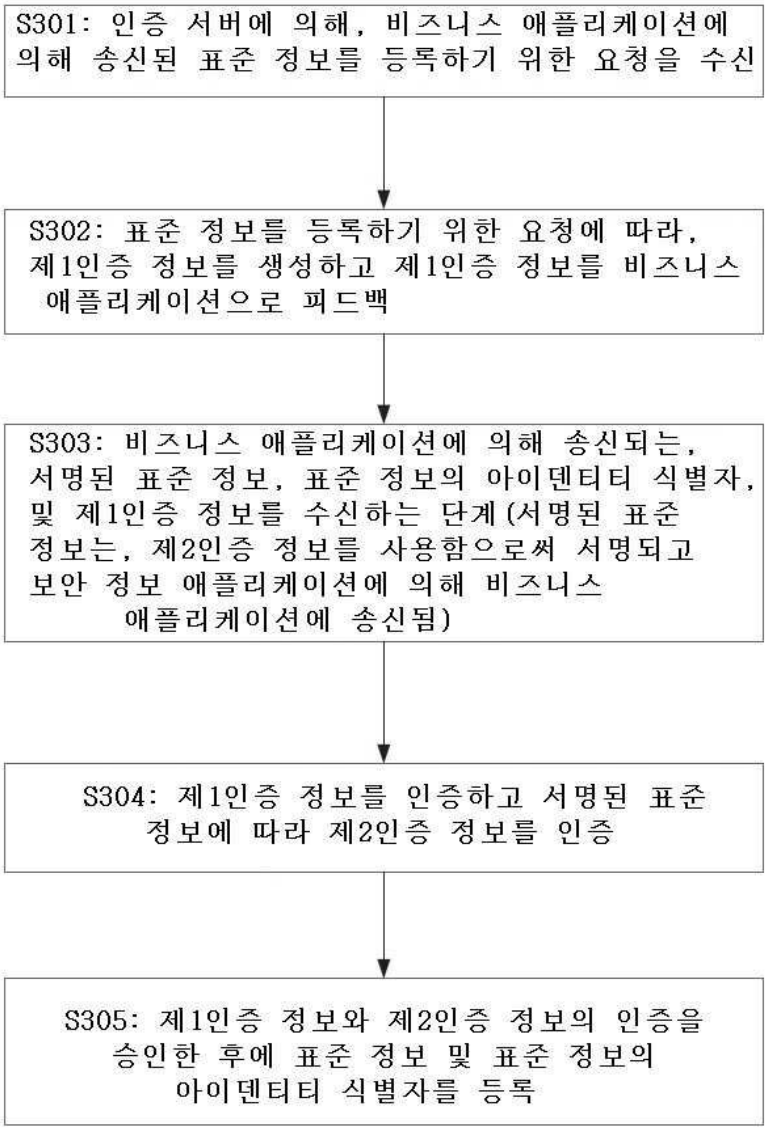
도면1


S101: 표준 정보를 등록하기 위한 요청을 인증 서버에 송신
S102: 인증 서버에 의해 피드백되는 제1인증 정보를 수신
S103:표준 정보 획득 요청을 생성하고, 표준 정보획득 요청 및 제1인증 정보를 보안 정보 애플리케이션에 송신하고, 보안 정보 애플리케이션이 제1인증 정보의 인증을 승인한 후 보안 정보 애플리케이션에 의해 리턴되는, 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 획득
S104: 서명된 표준 정보, 표준 정보의 아이덴티티 식별자, 및 제1인증 정보를 인증 서버에 송신하여, 인증 서버가 제1인증 정보의 인증을 승인하고 서명된 표준 정보에 따라 제2인증 정보의 인증을 승인한 후에 인증 서버가 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록

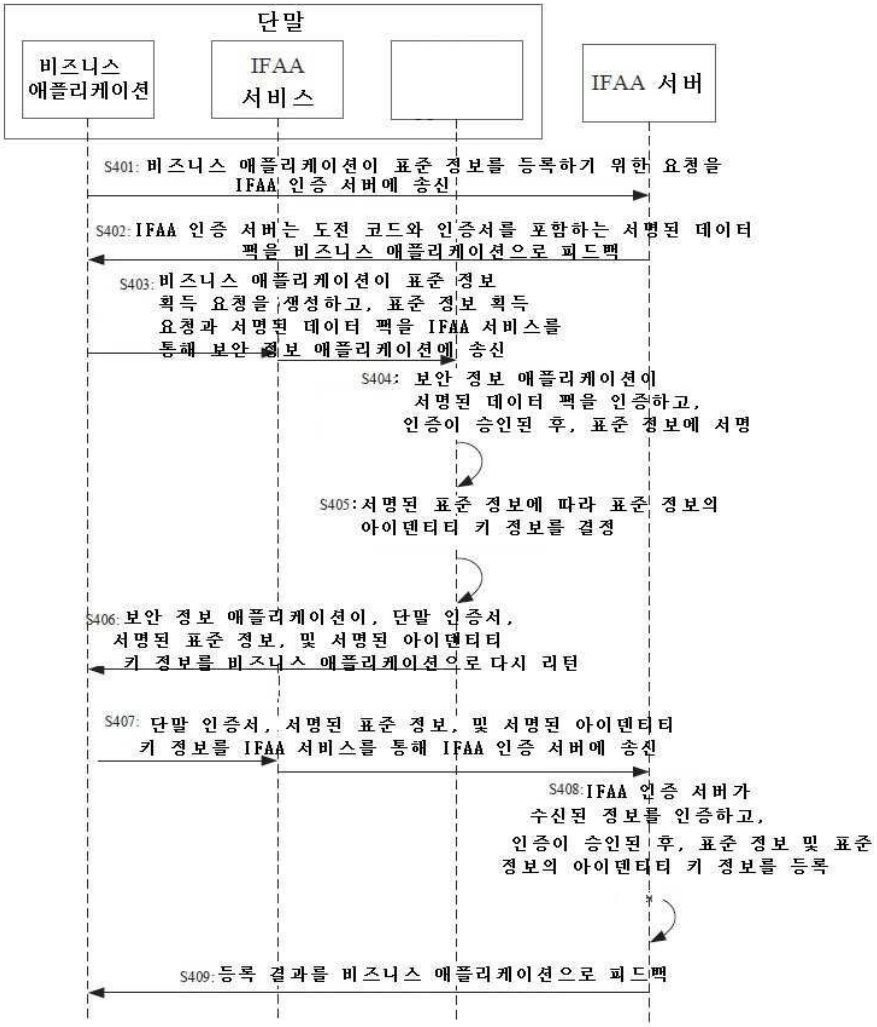
도면2


S201: 비즈니스 애플리케이션에 의해 송신되는, 제1인증 정보와 표준 정보 획득 요청을 수신
S202: 제1인증 정보를 인증하고, 인증이 승인된 후, 제2인증 정보를 사용하여 서명된 표준 정보를 리턴하고 표준 정보의 아이덴티티 식별자를 비즈니스 애플리케이션으로 다시 리턴하여, 비즈니스 애플리케이션이 서명된 표준 정보 및 표준 정보의 아이덴티티 식별자를 인증 서버에 송신하게 하고, 인증 서버가 제1인증 정보의 인증을 승인하고 서명된 표준 정보에 따라 제2인증 정보의 인증을 승인한 후에 인증 서버가 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록

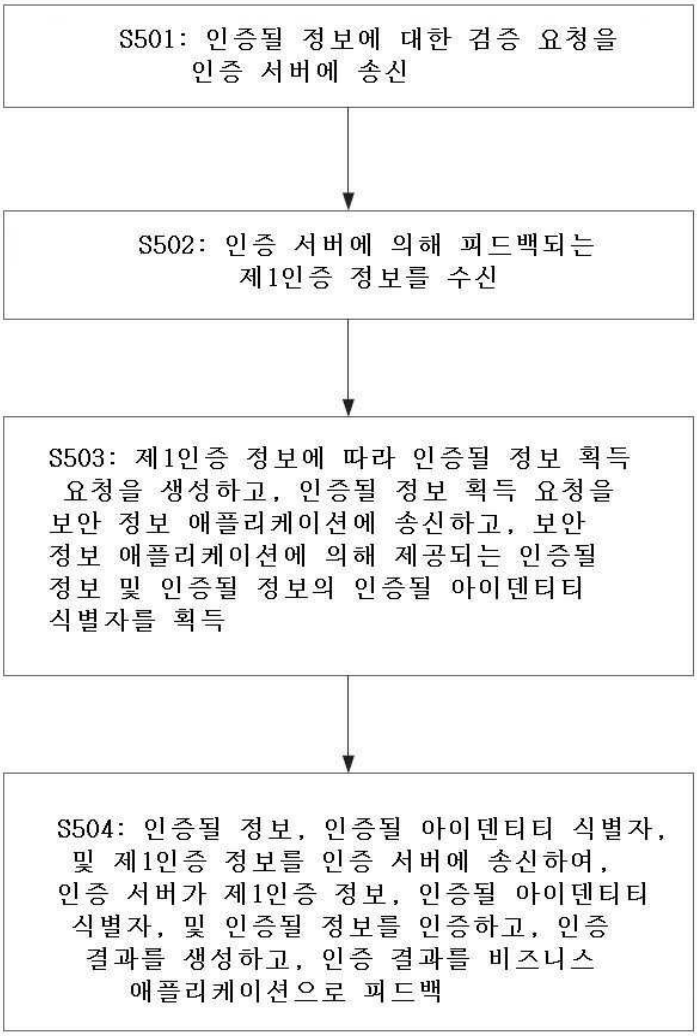
도면3


S301: 인증 서버에 의해, 비즈니스 애플리케이션에 의해 송신된 표준 정보를 등록하기 위한 요청을 수신
S302: 표준 정보를 등록하기 위한 요청에 따라, 제1인증 정보를 생성하고 제1인증 정보를 비즈니스 애플리케이션으로 피드백
S303: 비즈니스 애플리케이션에 의해 송신되는, 서명된 표준 정보, 표준 정보의 아이덴티티 식별자, 및 제1인증 정보를 수신하는 단계(서명된 표준 정보는, 제2인증 정보를 사용함으로써 서명되고 보안 정보 애플리케이션에 의해 비즈니스 애플리케이션에 송신됨)
S304: 제1인증 정보를 인증하고 서명된 표준 정보에 따라 제2인증 정보를 인증
S305: 제1인증 정보와 제2인증 정보의 인증을 승인한 후에 표준 정보 및 표준 정보의 아이덴티티 식별자를 등록

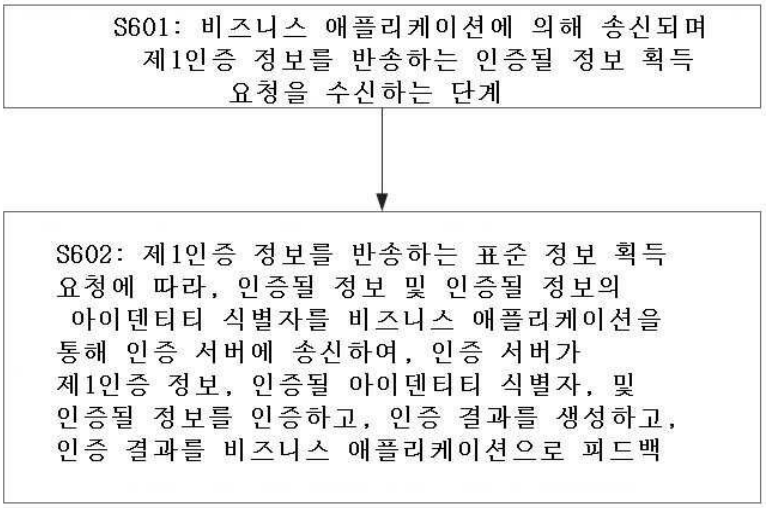
도면4


단말
비즈니스 애플리케이션
IFAA 서비스
IFAA 서버
S401: 비즈니스 애플리케이션이 표준 정보를 등록하기 위한 요청을 IFAA 인증 서버에 송신
S402: IFAA 인증 서버는 도전 코드와 인증서를 포함하는 서명된 데이터 팩을 비즈니스 애플리케이션으로 피드백
S403: 비즈니스 애플리케이션이 표준 정보 획득 요청을 생성하고, 표준 정보 획득 요청과 서명된 데이터 팩을 IFAA 서비스를 통해 보안 정보 애플리케이션에 송신
S404: 보안 정보 애플리케이션이 서명된 데이터 팩을 인증하고, 인증이 승인된 후, 표준 정보에 서명
S405: 서명된 표준 정보에 따라 표준 정보의 아이덴티티 키 정보를 결정
S406: 보안 정보 애플리케이션이, 단말 인증서, 서명된 표준 정보, 및 서명된 아이덴티티 키 정보를 비즈니스 애플리케이션으로 다시 리턴
S407: 단말 인증서, 서명된 표준 정보, 및 서명된 아이덴티티 키 정보를 IFAA 서비스를 통해 IFAA 인증 서버에 송신
S408: IFAA 인증 서버가 수신된 정보를 인증하고, 인증이 승인된 후, 표준 정보 및 표준 정보의 아이덴티티 키 정보를 등록
S409: 등록 결과를 비즈니스 애플리케이션으로 피드백

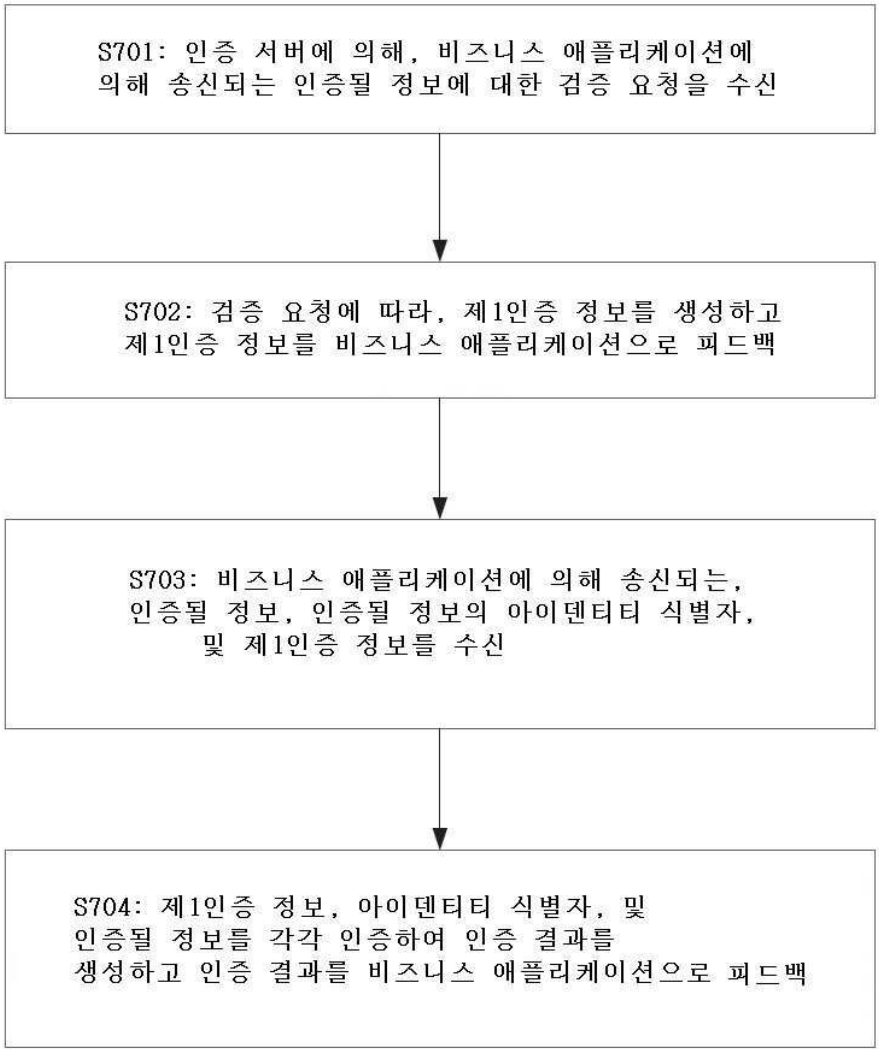
도면5


S501: 인증될 정보에 대한 검증 요청을 인증 서버에 송신
S502: 인증 서버에 의해 피드백되는 제1인증 정보를 수신
S503: 제1인증 정보에 따라 인증될 정보 획득 요청을 생성하고, 인증될 정보 획득 요청을 보안 정보 애플리케이션에 송신하고, 보안 정보 애플리케이션에 의해 제공되는 인증될 정보 및 인증될 정보의 인증될 아이덴티티 식별자를 획득
S504: 인증될 정보, 인증될 아이덴티티 식별자, 및 제1인증 정보를 인증 서버에 송신하여, 인증 서버가 제1인증 정보, 인증될 아이덴티티 식별자, 및 인증될 정보를 인증하고, 인증 결과를 생성하고, 인증 결과를 비즈니스 애플리케이션으로 피드백

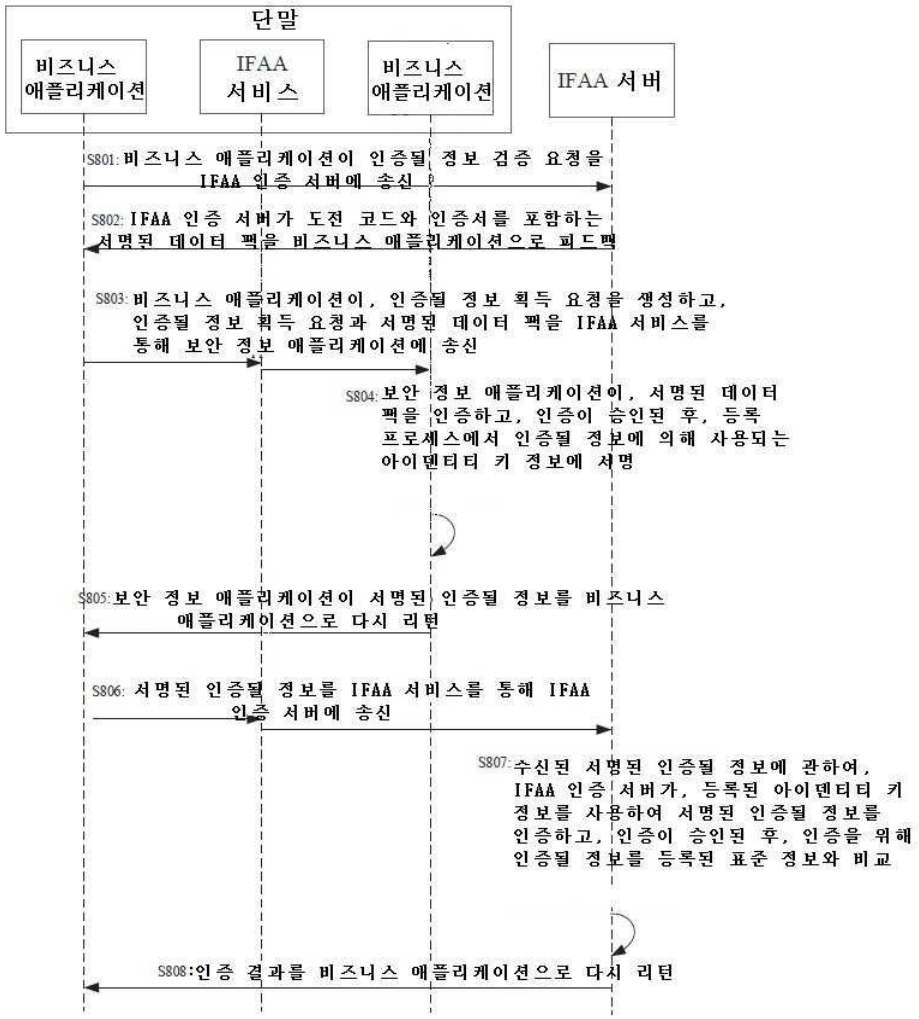
도면6


S601: 비즈니스 애플리케이션에 의해 송신되며 제1인증 정보를 반송하는 인증될 정보 획득 요청을 수신하는 단계
S602: 제1인증 정보를 반송하는 표준 정보 획득 요청에 따라, 인증될 정보 및 인증될 정보의 아이덴티티 식별자를 비즈니스 애플리케이션을 통해 인증 서버에 송신하여, 인증 서버가 제1인증 정보, 인증될 아이덴티티 식별자, 및 인증될 정보를 인증하고, 인증 결과를 생성하고, 인증 결과를 비즈니스 애플리케이션으로 피드백

도면7


S701: 인증 서버에 의해, 비즈니스 애플리케이션에 의해 송신되는 인증될 정보에 대한 검증 요청을 수신
S702: 검증 요청에 따라, 제1인증 정보를 생성하고 제1인증 정보를 비즈니스 애플리케이션으로 피드백
S703: 비즈니스 애플리케이션에 의해 송신되는, 인증될 정보, 인증될 정보의 아이덴티티 식별자, 및 제1인증 정보를 수신
S704: 제1인증 정보, 아이덴티티 식별자, 및 인증될 정보를 각각 인증하여 인증 결과를 생성하고 인증 결과를 비즈니스 애플리케이션으로 피드백

도면8

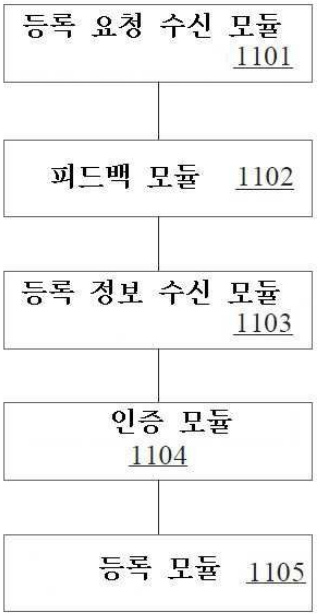

단말
비즈니스 애플리케이션
IFAA 서비스
비즈니스 애플리케이션
IFAA 서버
S801: 비즈니스 애플리케이션이 인증될 정보 검증 요청을 IFAA 인증 서버에 송신
S802: IFAA 인증 서버가 도전 코드와 인증서를 포함하는 서명된 데이터 팩을 비즈니스 애플리케이션으로 피드백
S803: 비즈니스 애플리케이션이, 인증될 정보 획득 요청을 생성하고, 인증될 정보 획득 요청과 서명된 데이터 팩을 IFAA 서비스를 통해 보안 정보 애플리케이션에 송신
S804: 보안 정보 애플리케이션이, 서명된 데이터 팩을 인증하고, 인증이 승인된 후, 등록 프로세스에서 인증될 정보에 의해 사용되는 아이덴티티 키 정보에 서명
S805: 보안 정보 애플리케이션이 서명된 인증될 정보를 비즈니스 애플리케이션으로 다시 리턴
S806: 서명된 인증될 정보를 IFAA 서비스를 통해 IFAA 인증 서버에 송신
S807: 수신된 서명된 인증될 정보에 관하여, IFAA 인증 서버가, 등록된 아이덴티티 키 정보를 사용하여 서명된 인증될 정보를 인증하고, 인증이 승인된 후, 인증을 위해 인증될 정보를 등록된 표준 정보와 비교
S808: 인증 결과를 비즈니스 애플리케이션으로 다시 리턴

도면9

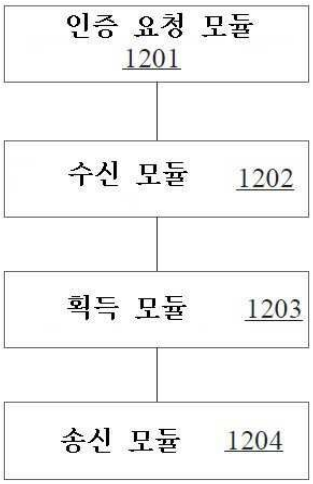

등록 요청 모듈 901
수신 모듈 902
획득 모듈 903
송신 모듈 904

도면10

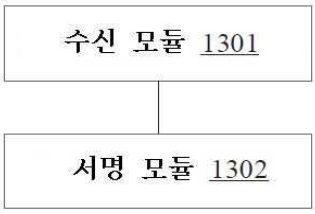
도면11



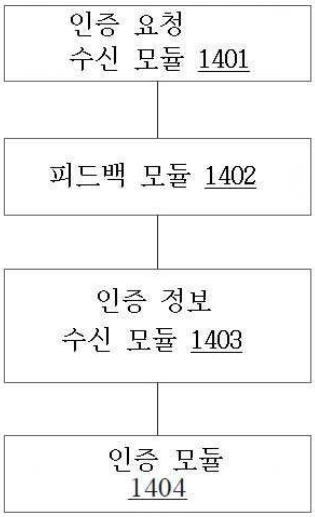
도면12



도면13


수신 모듈 1301
서명 모듈 1302

도면14


인증 요청
수신 모듈 1401
피드백 모듈 1402
인증 정보
수신 모듈 1403
인증 모듈
1404