(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년10월10일
(11) 등록번호 10-1663700
(24) 등록일자 2016년09월30일

(51) 국제특허분류(Int. Cl.)
G06Q 40/02 (2012.01)
(21) 출원번호 10-2014-0179728
(22) 출원일자 2014년12월12일
심사청구일자 2014년12월12일
(65) 공개번호 10-2016-0072384
(43) 공개일자 2016년06월23일
(56) 선행기술조사문헌
KR1020100080031 A*
KR1020070037782 A*
KR1020120024082 A*
KR1020080039046 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국정보통신주식회사
서울특별시 중구 세종대로 39 (남대문로4가)
(72) 발명자
박용현
경기도 고양시 덕양구 푸른마을로120번길 34
1004동 1503호 (고양동,푸른마을10단지아파트)
(74) 대리인
특허법인아주

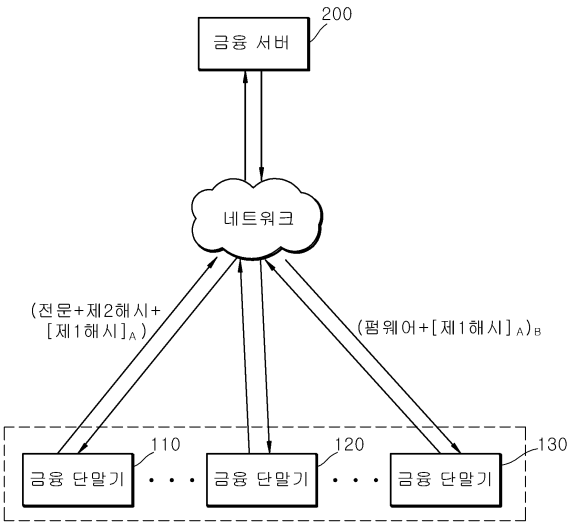
전체 청구항 수 : 총 6 항 심사관 : 송원선

(54) 발명의 명칭 **금융 시스템, 금융 시스템의 펌웨어 무결성 체크 방법**

(57) 요 약

본 발명은 금융 시스템, 금융 시스템의 펌웨어 무결성 체크 방법에 관한 것으로, 금융 서버로부터 펌웨어와 인증값이 결합되어 암호화된 정보를 전송받아 복호한 후 상기 복호화된 펌웨어를 이용해 무결성 체크를 위한 정보를 생성하여 상기 금융 서버에 전송하는 금융 단말기, 및 상기 금융 단말기를 업그레이드시키기 위하여, 펌웨어와 인증값이 결합된 정보를 암호화하여 상기 금융 단말기에 전송하고, 상기 금융 단말기로부터 전송받은 무결성 체크를 위한 정보를 이용하여 펌웨어에 대한 무결성 체크를 수행하는 금융 서버를 포함한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

금융 서버로부터 펌웨어와 인증값이 결합되어 암호화된 정보를 전송받아 복호한 후 상기 복호화된 펌웨어를 이용해 무결성 체크를 위한 정보를 생성하여 상기 금융 서버에 전송하는 금융 단말기; 및

상기 금융 단말기를 업그레이드시키기 위하여, 펌웨어와 인증값이 결합된 정보를 암호화하여 상기 금융 단말기에 전송하고, 상기 금융 단말기로부터 전송받은 무결성 체크를 위한 정보를 이용하여 펌웨어에 대한 무결성 체크를 수행하는 금융 서버;를 포함하되,

상기 금융 서버는,

상기 금융 단말기의 펌웨어에 대한 제1 해시를 생성하고, 상기 제1 해시를 제1 개인키(A)를 이용해 암호화하고, 상기 제1 해시($[제1해시]_A$)와 상기 펌웨어를 모두 제2 개인키(B)를 이용하여 이중 암호화($(펌웨어 + [제1해시]_A)_B$)하고, 상기 이중 암호화된 펌웨어($(펌웨어 + [제1해시]_A)_B$)를 상기 금융 단말기에 전송하는 것을 특징으로 하는 금융 시스템.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

금융 서버가 금융 단말기를 업그레이드시키기 위한 펌웨어와 인증값이 결합된 정보를 암호화하여 금융 단말기에 전송하는 단계;

상기 금융 단말기가 상기 펌웨어와 인증값이 결합되어 암호화된 정보를 전송받아 복호한 후 상기 복호화된 펌웨어를 이용해 무결성 체크를 위한 정보를 생성하여 상기 금융 서버에 전송하는 단계; 및

상기 금융 서버가 상기 금융 단말기로부터 전송받은 무결성 체크를 위한 정보를 이용하여 무결성 체크를 수행하는 단계;를 포함하되,

상기 펌웨어와 인증값이 결합된 정보를 암호화하여 금융 단말기에 전송하는 단계에서, 상기 금융 서버는, 상기 펌웨어에 대한 제1 해시를 생성하고, 상기 제1 해시를 제1 개인키(A)를 이용해 암호화하고, 상기 암호화된 제1 해시($[제1해시]_A$)와 상기 펌웨어를 모두 제2 개인키(B)를 이용하여 이중 암호화($(펌웨어 + [제1해시]_A)_B$)하고, 상기 이중 암호화된 펌웨어($(펌웨어 + [제1해시]_A)_B$)를 상기 금융 단말기에 전송하는 것을 특징으로 하는 금융 시스템의 무결성 체크 방법.

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

제 1항에 있어서,

상기 금융 단말기는, 상기 금융 서버로부터 이중 암호화된 펌웨어($(펌웨어 + [제1해시]_A)_B$)를 전송 받아 이를 상기 제2 개인키(B)에 대응하는 공개키를 이용해 복호화하여 펌웨어 및 암호화된 제1 해시($[제1해시]_A$)로 분리하여 내부 메모리에 저장하고, 상기 펌웨어가 복호화되면, 상기 금융 서버의 해시 생성 알고리즘과 동일한 알고리즘을 이용하여, 상기 복호화된 펌웨어의 제2 해시를 자체적으로 생성하여 내부 메모리에 저장하고, 상기 제1 개인키(A)에 대응되는 공개키를 보유하고 있지 않을 경우, 상기 제1 해시($[제1해시]_A$)를 복호화하지 않은 상태로 저장하며, 상기 금융 단말기에 설치된 펌웨어에 대하여 자체적으로 생성한 제2 해시, 상기 제1 해시($[제1해시]_A$), 및 전문이 포함된 무결성 체크를 위한 정보를 생성하여, 상기 무결성 체크를 위한 정보(전문 + 제2 해시 + 인증값($[제1해시]_A$))를 상기 금융 서버에 전송하는 것을 특징으로 하는 금융 시스템.

청구항 18

제 17항에 있어서,

상기 금융 서버는,

상기 금융 단말기로부터 무결성 체크를 위한 정보(전문 + 제2 해시 + 인증값($[제1해시]_A$))를 전송 받은 후, 상기 무결성 체크를 위한 정보에 포함된 제2 해시와 상기 제1 해시를 비교하여 제1 해시와 제2 해시가 동일한 경

우에는 상기 금융 단말기에 전송된 펌웨어에 대한 무결성이 보장된 것으로 판단하고, 상기 제1 해시와 제2 해시가 동일하지 않은 경우에는 상기 금융 단말기에 전송된 펌웨어에 대한 무결성이 훼손된 것으로 판단하여 무결성 훼손 알림을 출력하는 것을 특징으로 하는 금융 시스템.

청구항 19

제 9항에 있어서,

상기 금융 단말기가 무결성 체크를 위한 정보를 생성하여 상기 금융 서버에 전송하는 단계에서,

상기 금융 단말기는, 상기 금융 서버로부터 이중 암호화된 펌웨어((펌웨어 + $[제1해시]_A)_B$)를 전송 받아 이를 상기 제2 개인키(B)에 대응하는 공개키를 이용해 복호화하여 펌웨어 및 암호화된 제1 해시($[제1해시]_A$)로 분리하여 내부 메모리에 저장하고, 상기 펌웨어가 복호화되면, 상기 금융 서버의 해시 생성 알고리즘과 동일한 알고리즘을 이용하여, 상기 복호화된 펌웨어의 제2 해시를 자체적으로 생성하여 내부 메모리에 저장하고, 상기 제1 개인키(A)에 대응되는 공개키를 보유하고 있지 않을 경우, 상기 제1 해시($[제1해시]_A$)를 복호화하지 않은 상태로 저장하며, 상기 금융 단말기에 설치된 펌웨어에 대하여 자체적으로 생성한 제2 해시, 상기 제1 해시($[제1해시]_A$), 및 전문이 포함된 무결성 체크를 위한 정보를 생성하여, 상기 무결성 체크를 위한 정보(전문 + 제2 해시 + 인증값($[제1해시]_A$))를 상기 금융 서버에 전송하는 것을 특징으로 하는 금융 시스템의 무결성 체크 방법.

청구항 20

제 19항에 있어서,

상기 금융 서버는, 무결성 체크를 수행하기 위하여, 상기 금융 단말기로부터 무결성 체크를 위한 정보(전문 + 제2 해시 + 인증값($[제1해시]_A$))를 전송 받은 후, 상기 무결성 체크를 위한 정보에 포함된 제2 해시와 상기 제1 해시를 비교하여 제1 해시와 제2 해시가 동일한 경우에는 상기 금융 단말기에 전송된 펌웨어에 대한 무결성이 보장된 것으로 판단하고, 상기 제1 해시와 제2 해시가 동일하지 않은 경우에는 상기 금융 단말기에 전송된 펌웨어에 대한 무결성이 훼손된 것으로 판단하여 무결성 훼손 알림을 출력하는 것을 특징으로 하는 금융 시스템의 무결성 체크 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 금융 시스템, 금융 시스템의 펌웨어 무결성 체크 방법에 관한 것으로, 보다 상세하게는 금융 서버와 금융 단말기 간에 펌웨어 정보를 이용해서 무결성을 체크할 수 있도록 하는 금융 시스템, 금융 시스템의 펌웨어 무결성 체크 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 금융 단말기(또는 금융자동화기기)는 고객이 금융기관에서 발급받은 카드나 통장 등을 사용하여 언제 어디서나 신용카드의 사용 및 거래 등의 금융거래, 입출금 거래, 계좌이체, 및 조회업무 등의 금융 업무를 수행할 수 있도록 하는 무인단말기를 의미한다.

[0003] 또한 금융 서버는 상기 금융 단말기와 유선(또는 무선) 네트워크로 연결되어 있으며, 상기 금융 단말기의 결제요청 정보를 수신하여 그 결제요청을 승인하는 기능, 및 상기 금융 단말기와 통신하여 상기 금융 단말기의 펌웨어(Firmware)를 업그레이드 시키는 기능을 수행한다.

[0004] 그런데 종래에는 상기 금융 서버로부터 상기 금융 단말기의 펌웨어를 업그레이드하거나 평상시(예 : 결제요청 정보를 금융 서버로 전송할 때, 및 일정 주기가 되었을 때 등) 무결성 체크를 위한 작업을 수행하지 않았다. 따

라서 상기 펌웨어가 해커에 노출되어 변경되더라도 무결성을 확인할 수 없는 문제점이 있었다.

[0005] 본 발명의 배경기술은 대한민국 공개특허 특2001-0086870호(2001.09.15.공개, 통합금융자동화 장치 및, 인터넷을 이용한 점외 금융자동화기기 시스템 운영방법)에 개시되어 있다. 상기 배경기술은 금융자동화기기의 소프트웨어 업그레이드에 대해서 개시되어 있으나 무결성 보장에 관련된 기술은 개시되어 있지 않다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 상기와 같은 문제점을 해결하기 위해 창작된 것으로서, 금융 서버와 금융 단말기 간에 펌웨어 정보를 이용해서 무결성을 체크할 수 있도록 하는 금융 시스템, 금융 시스템의 펌웨어 무결성 체크 방법을 제공하는데 그 목적이 있다.

과제의 해결 수단

[0007] 본 발명의 일 측면에 따른 금융 시스템은, 금융 서버로부터 펌웨어와 인증값이 결합되어 암호화된 정보를 전송받아 복호한 후 상기 복호화된 펌웨어를 이용해 무결성 체크를 위한 정보를 생성하여 상기 금융 서버에 전송하는 금융 단말기; 및 상기 금융 단말기를 업그레이드시키기 위하여, 펌웨어와 인증값이 결합된 정보를 암호화하여 상기 금융 단말기에 전송하고, 상기 금융 단말기로부터 전송받은 무결성 체크를 위한 정보를 이용하여 펌웨어에 대한 무결성 체크를 수행하는 금융 서버;를 포함하는 것을 특징으로 한다.

[0008] 본 발명에 있어서, 상기 금융 서버는, 상기 펌웨어에 대하여 생성한 제1 해시를 제1 개인키를 이용하여 암호화하여 상기 인증값을 생성하는 것을 특징으로 한다.

[0009] 본 발명에 있어서, 상기 금융 단말기는, 상기 금융 서버로부터 전송받은 인증값, 및 상기 펌웨어에 대하여 자체적으로 생성한 제2 해시를 포함하여 상기 무결성 체크를 위한 정보로 생성하는 것을 특징으로 한다.

[0010] 본 발명에 있어서, 상기 금융 서버는, 상기 펌웨어에 대한 무결성이 훼손된 경우, 상기 금융 서버 자신 및 금융 단말기 중 적어도 하나를 통해 무결성 훼손을 알리는 것을 특징으로 한다.

[0011] 본 발명에 있어서, 상기 금융 서버는, 상기 펌웨어와 인증값이 결합된 정보를 제2 개인키를 이용해 암호화하는 것을 특징으로 한다.

[0012] 본 발명에 있어서, 상기 금융 서버는, 상기 금융 단말기로부터 전송받은 인증값에 포함된 제1 해시와 상기 금융 단말기가 자체적으로 생성한 제2 해시를 비교하여 무결정 체크를 수행하고, 상기 비교를 통해 상기 제1 해시와 제2 해시가 동일한 경우에 상기 펌웨어에 대한 무결성을 보장하는 것을 특징으로 한다.

[0013] 본 발명에 있어서, 상기 금융 단말기는, 미리 설정된 이벤트 발생 시마다 상기 무결성 체크를 위한 정보를 생성하여 상기 금융 서버로 전송하는 것을 특징으로 한다.

[0014] 본 발명에 있어서, 상기 이벤트는, 펌웨어 업그레이드, 결제요청 정보를 금융 서버로 전송, 및 미리 설정된 주기가 되었을 때 중 적어도 하나를 포함하는 것을 특징으로 한다.

[0015] 본 발명의 다른 측면에 따른 금융 시스템의 무결성 체크 방법은, 금융 서버가 금융 단말기를 업그레이드시키기 위한 펌웨어와 인증값이 결합된 정보를 암호화하여 금융 단말기에 전송하는 단계; 상기 금융 단말기가 상기 펌웨어와 인증값이 결합되어 암호화된 정보를 전송받아 복호한 후 상기 복호화된 펌웨어를 이용해 무결성 체크를 위한 정보를 생성하여 상기 금융 서버에 전송하는 단계; 및 상기 금융 서버가 상기 금융 단말기로부터 전송받은 무결성 체크를 위한 정보를 이용하여 무결성 체크를 수행하는 단계;를 포함하는 것을 특징으로 한다.

[0016] 본 발명에 있어서, 상기 인증값은, 상기 금융 서버가 상기 펌웨어에 대하여 생성한 제1 해시를 제1 개인키를 이용하여 암호화한 정보인 것을 특징으로 한다.

[0017] 본 발명에 있어서, 상기 무결성 체크를 위한 정보는, 상기 금융 서버로부터 전송받은 인증값, 및 상기 금융 단

말기가 상기 펌웨어에 대하여 자체적으로 생성한 제2 해시를 포함하는 정보인 것을 특징으로 한다.

[0018] 본 발명에 있어서, 상기 무결성 체크를 수행하는 단계 이후에, 상기 무결성이 훼손된 경우, 상기 금융 서버는, 상기 금융 서버 자신 및 금융 단말기 중 적어도 하나를 통해 무결성 훼손을 알리는 단계;를 더 포함하는 것을 특징으로 한다.

[0019] 본 발명에 있어서, 상기 인증값은 상기 펌웨어에 대한 제1 해시를 제1 개인키를 이용해 암호화한 정보이고, 상기 펌웨어와 인증값이 결합된 정보는 제2 개인키를 이용해 암호화된 정보인 것을 특징으로 한다.

[0020] 본 발명에 있어서, 상기 무결성 체크를 수행하는 단계에서, 상기 금융 서버는, 상기 금융 단말기로부터 전송받은 인증값에 포함된 제1 해시와 상기 금융 단말기가 자체적으로 생성한 제2 해시를 비교하고, 상기 비교를 통해 상기 제1 해시와 제2 해시가 동일한 경우에 무결성을 보장하는 것을 특징으로 한다.

[0021] 본 발명에 있어서, 상기 무결성 체크를 위한 정보를 생성하여 상기 금융 서버에 전송하는 단계에서, 상기 금융 단말기는 미리 설정된 이벤트 발생 시마다 상기 무결성 체크를 위한 정보를 생성하여 전송하는 것을 특징으로 한다.

[0022] 본 발명에 있어서, 상기 이벤트는, 펌웨어 업그레이드, 결제요청 정보를 금융 서버로 전송, 및 미리 설정된 주기가 되었을 때 중 적어도 하나를 포함하는 것을 특징으로 한다.

발명의 효과

[0023] 본 발명에 따른 금융 시스템, 금융 시스템의 펌웨어 무결성 체크 방법은, 금융 서버와 금융 단말기 간에 펌웨어 정보를 이용해서 금융 시스템의 펌웨어에 대한 무결성을 체크할 수 있도록 한다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 일 실시예에 따른 무결성 체크를 위한 금융 시스템의 구성을 개략적으로 보인 예시도.

도 2는 본 발명의 일 실시예에 따른 금융 시스템의 펌웨어 업그레이드 및 펌웨어의 무결성 체크를 위한 금융 서버 측의 동작을 설명하기 위한 흐름도.

도 3은 본 발명의 일 실시예에 따른 펌웨어의 무결성 체크를 위한 금융 단말기 측의 동작을 설명하기 위한 흐름도.

도 4는 본 발명의 일 실시예에 따라 펌웨어 업그레이드 후 및 평상시의 펌웨어 무결성 체크를 위한 금융 단말기 측의 동작을 설명하기 위한 흐름도.

도 5는 본 발명의 일 실시예에 따라 펌웨어 업그레이드 후 및 평상시의 펌웨어 무결성 체크를 위한 금융 서버 측의 동작을 설명하기 위한 흐름도.

발명을 실시하기 위한 구체적인 내용

[0025] 이하, 첨부된 도면을 참조하여 본 발명에 따른 금융 시스템, 금융 시스템의 펌웨어 무결성 체크 방법의 일 실시예를 설명한다.

[0026] 이 과정에서 도면에 도시된 선들의 두께나 구성요소의 크기 등은 설명의 명료성과 편의상 과장되게 도시되어 있을 수 있다. 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례에 따라 달라질 수 있다. 그러므로 이러한 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0027] 도 1은 본 발명의 일 실시예에 따른 무결성 체크를 위한 금융 시스템의 구성을 개략적으로 보인 예시도이다.

[0028] 도 1에 도시된 바와 같이, 본 실시예에 따른 무결성 체크를 위한 금융 시스템은, 적어도 하나 이상의 금융 단말기(예 : 카드 리더기)(110 ~ 130), 상기 금융 단말기(110 ~ 130)와 네트워크로 연결되어 무결성 보장된 펌웨어 업그레이드를 수행하는 금융 서버(200)를 포함한다.

[0029] 여기서 무결성 보장은 오직 허가된 금융 단말기(110 ~ 130)에게만 정보가 개방되고, 또한 상기 금융 단말기(110

~ 130)에 의해서만 정보가 전달되고 수신될 수 있음을 보장하는 것이다. 즉, 상기 무결성은 결점이 없다는 뜻으로, 상기 금융 서버(200)로부터 전송되는 데이터(즉, 펌웨어)에 변경이 없었다는 것을 보증하고, 또한 상기 금융 단말기(110 ~ 130)에 설치된 펌웨어에 변경이 없었다는 것을 보증하는 것이다.

[0030] 가령 상기 금융 서버(200)가 전송한 데이터(즉, 펌웨어)가 상기 금융 단말기(110 ~ 130)에 전송되는 도중에 중간에서 해커의 해킹이나 다른 이유로 변경(또는 일부 삭제, 일부 추가 등)될 경우에 이를 상기 금융 서버(200)나 상기 금융 단말기(110 ~ 130)에 알려주어 대응할 수 있게 하는 것이다. 또한 상기 업그레이드 시 뿐만 아니라, 평상시(예 : 결제요청 정보를 금융 서버로 전송할 때, 및 일정 주기가 되었을 때 등)에도 무결성 체크를 위한 작업을 지속적으로 수행함으로써, 상기 금융 단말기(110 ~ 130)에 설치된 펌웨어에 대한 무결성을 금융 서버(200)가 지속적으로 체크할 수 있도록 하는 것이다.

[0031] 한편 상기 금융 서버(200)는 업그레이드할 상기 금융 단말기(130)의 펌웨어에 대한 해시(hash)(이하 제1 해시)를 생성하여, 미리 설정된 임의의 암호화 알고리즘을 통해, 상기 제1 해시를 미리 설정된 제1 개인키(A)(즉, 해시 암호화를 위한 개인키)를 이용해 암호화하고(예 : $[제1해시]_A$), 상기 펌웨어와 상기 제1 개인키로 암호화된 제1 해시($[제1해시]_A$) 모두를 제2 개인키(B)(즉, 배포용 개인키)를 이용해 다시 암호화하여(예 : $(펌웨어 + [제1해시]_A)_B$) 상기 금융 단말기(130)에 전송한다.

[0032] 본 실시예에서 상기 제1 개인키(A)(즉, 해시 암호화를 위한 개인키)로 암호화된 제1 해시(예 : $[제1해시]_A$)는 무결성 체크를 위한 일종의 인증값으로 사용된다.

[0033] 상기 금융 단말기(130)는 상기 금융 서버(200)로부터 암호화된 펌웨어(예 : $(펌웨어 + [제1해시]_A)_B$)가 수신되면, 미리 설정된 공개키(즉, 배포용 개인키(B)에 대응하는 배포용 공개키)를 이용하여 상기 제2 개인키(B)로 암호화된 펌웨어(예 : $(펌웨어 + [제1해시]_A)_B$)를 복호화한다. 그리고 상기 금융 단말기(130)는 상기 복호화된 펌웨어에 대한 해시(이하, 제2 해시)를 자체적으로 생성할 수 있다.

[0034] 한편 본 실시예에서는 상기 금융 단말기(130)의 기능을 수행하기 위한 내부 구성을 구체적으로 기재하지 않았으나, 상기 금융 단말기(130)는 적어도 내부 제어부(미도시), 및 내부 메모리(미도시)를 포함하여 구성될 수 있다.

[0035] 여기서 상기 내부 메모리(미도시)는 별도의 메모리(예 : 플래시 메모리, 시큐어 메모리 등)를 추가로 포함할 수 있으며, 복호화 알고리즘, 암호화 알고리즘, 해시 생성 알고리즘, 해시(hash), 공개키, 및 개인키 중 적어도 하나 이상이 상기 별도의 메모리에 각기 저장될 수 있다.

[0036] 참고로 여기서 개인키란 암호화/복호화를 위해 비밀 메시지(예 : 펌웨어, 결제요청정보, 승인정보 등)를 교환하는 당사자(예 : 금융 서버, 금융 단말기)만이 알고 있는 키(Key)이고, 공개키란 상기 개인키와 함께 결합되어 암호화 및 복호화를 수행하기 위한 키이다.

[0037] 좀 더 구체적으로, 상기 금융 단말기(130)는 상기 제2 개인키(B)에 대응되는 공개키를 이용하여 상기 제2 개인키(B)로 암호화된 펌웨어를 복호화한다. 아울러 상기 금융 단말기(110 ~ 130)가 상기 제1 개인키(A)에 대응되는 공개키를 보유하고 있을 경우, 상기 제1 개인키(A)로 암호화된 제1 해시(예 : $[제1해시]_A$)를 복호화할 수 있다. 물론 상기 금융 단말기(110 ~ 130)가 상기 제1 개인키(A)에 대응되는 공개키를 보유하고 있지 않을 경우, 상기 제1 해시(예 : $[제1해시]_A$)를 복호화하지 않은 상태로 저장할 수 있다.

[0038] 그리고 상기 금융 단말기(110 ~ 130)는, 미리 설정된 임의의 해시 생성 알고리즘을 이용해서, 상기 복호화된 펌웨어에 대한 해시(즉, 제2 해시)를 자체적으로 생성한다.

[0039] 만약, 상기 금융 단말기(110 ~ 130)가 상기 제1 개인키(A)에 대응되는 공개키를 이용해 상기 제1 해시(예 : $[제1해시]_A$)를 복호화 했을 경우, 상기 금융 단말기(110 ~ 130)는 자체적으로 생성한 제2 해시와 상기 복호화된 제1 해시를 비교하여 두 해시 값(즉, 제1 해시, 제2 해시)이 동일한 경우에 상기 복호된 펌웨어에 대한 무결성이 보장된 것으로 판단한다. 상기와 같이 금융 단말기(110 ~ 130) 자체적으로 무결성 체크를 수행하여 상기 금융 서버(200)로부터 전송받은 펌웨어의 무결성이 보장되면, 상기 금융 단말기(110 ~ 130)는 상기 무결성이 보장된 펌웨어를 이용해 업그레이드를 수행한다.

[0040] 그러나 상기 금융 단말기(110 ~ 130)가 상기 제1 개인키(A)에 대응되는 공개키를 보유하고 있지 않을 경우, 상

기 제1 개인키(A)로 암호화된 해시(예 : $[제1해시]_A$)(즉, 인증값)를 내부 메모리(미도시)에 저장해 두기만 하고, 자체적인 무결성 체크를 수행하지는 않는다. 상기와 같이 자체적인 무결성 체크를 수행하지 않을 경우, 상기 금융 단말기(110 ~ 130)는 상기 펌웨어가 복호화되면 상기 복호화된 펌웨어를 이용해 곧바로 업그레이드를 수행한다.

[0041] 그리고 상기 금융 단말기(110 ~ 130)는 상기 펌웨어 업그레이드 후, 및 평상시(예 : 결제요청 정보를 금융 서버로 전송할 때, 및 일정 주기가 되었을 때 등) 상기 금융 단말기(110 ~ 1130)에 설치된 펌웨어에 대하여 자체적으로 생성한 제2 해시, 상기 인증값(즉, 제1 개인키(A)로 암호화된 제1 해시($[제1해시]_A$)), 및 전문(예 : 결제정보, 금융단말기 상태/동작정보 등의 데이터)을 포함하여 상기 금융 서버(200)로 전송한다.

[0042] 상기 금융 서버(200)로 전송되는 정보(전문 + 제2 해시 + 인증값($[제1해시]_A$))은 상기 제2 개인키(B)에 대응하는 공개키로 암호화되어 전송될 수도 있다.

[0043] 이후 상기 금융 서버(200)는 상기 금융 단말기(110 ~ 130)로부터 전송받은 정보(전문 + 제2 해시 + 인증값($[제1해시]_A$)) 중 상기 제2 해시와 상기 제1 해시를 비교하여 두 해시 값(즉, 제1 해시, 제2 해시)이 동일한 경우에 상기 금융 단말기(110 ~ 130)에 전송된(또는 설치된) 펌웨어에 대한 무결성이 보장된 것으로 판단한다.

[0044] 도 2는 본 발명의 일 실시예에 따른 금융 시스템의 펌웨어 업그레이드 및 펌웨어의 무결성 체크를 위한 금융 서버 측의 동작을 설명하기 위한 흐름도이다.

[0045] 도 2에 도시된 바와 같이, 금융 서버(200)는 미리 설정된 특정 금융 단말기(110 ~ 130)에 대하여 업그레이드할 펌웨어가 준비될 경우(S101의 예), 상기 특정 금융 단말기(110 ~ 130)에 업그레이드할 펌웨어를 전송한다.

[0046] 이때 상기 펌웨어가 전송되는 도중에 해커에 의해 상기 펌웨어가 변경되는 것을 방지하기 위하여, 즉 무결성을 보장(또는 펌웨어 인증)하기 위한 작업을 수행한다. 즉, 상기 금융 서버(200)는 상기 업그레이드할 금융 단말기(110 ~ 130)의 펌웨어에 대한 해시(즉, 제1 해시)를 생성한다(S102).

[0047] 상기 해시는 미리 설정된 특정 해시 생성 알고리즘을 이용하여 생성된다.

[0048] 상기 해시 값으로는 원래의 펌웨어를 알 수 없으며, 입력 값(즉, 펌웨어)이 조금만 바뀌어도 출력 해시 값이 매우 크게 달라지고, 입력 값의 크기에 상관없이 아주 작은 크기의 출력 해시 값을 생성하므로 상기 펌웨어의 무결성을 증명하는데 높은 안정성을 제공한다.

[0049] 상기 금융 서버(200)는 상기 업그레이드할 펌웨어에 대하여 생성한 해시(즉, 제1 해시)를 제1 개인키(A)(예 : 해시 암호화를 위한 개인키)를 이용해 암호화한다(S103). 이때 상기 금융 단말기(130)는 상기 제1 개인키(A)에 대응하는 배포용 공개키를 미리 보유할 수도 있다.

[0050] 그리고 상기 금융 서버(200)는 상기 제1 개인키(A)를 이용해 암호화된 해시(즉, 제1 해시)($[제1해시]_A$)와 상기 특정 금융 단말기(110 ~ 130)에 업그레이드할 펌웨어를 모두 포함하여 제2 개인키(B)(즉, 배포용 개인키)를 이용하여 암호화(즉, 이중 암호화)(예 : (펌웨어 + $[제1해시]_A)_B$)한다(S104).

[0051] 그리고 상기 금융 서버(200)는 상기 이중 암호화된 펌웨어(예 : 펌웨어 + $[제1해시]_A)_B$)를 미리 설정된 특정 금융 단말기(110 ~ 130)에 전송한다(S105).

[0052] 상기와 같이 본 실시예는 이중 암호화를 통해 상기 전송할 펌웨어에 대한 기밀성을 보장하면서, 아울러 상기 업그레이드할 펌웨어에 대해서 해시(즉, 제1 해시)를 이용해 무결성을 보장할 수 있도록 한다. 물론 상기 펌웨어의 무결성 보장을 위한 해시(즉, 제1 해시) 자체에 대해서도 기밀성과 무결성을 보장할 수 있도록 하는 효과가 있다.

[0053] 도 3은 본 발명의 일 실시예에 따른 펌웨어의 무결성 체크를 위한 금융 단말기 측의 동작을 설명하기 위한 흐름도이다.

[0054] 도 3에 도시된 바와 같이, 금융 단말기(110 ~ 130)는 상기 금융 서버(200)로부터 이중으로 암호화된 펌웨어(예 : (펌웨어 + $[제1해시]_A)_B$)를 전송 받는다(S201).

[0055] 이에 따라 상기 금융 단말기(110 ~ 130)는 상기 제2 개인키(B)로 암호화된 펌웨어(예 : (펌웨어 + $[제1해시]_A)_B$)를 상기 제2 개인키(B)에 대응하는 공개키를 이용해 복호화하여 펌웨어 및 암호화된 제1 해시($[제1해시]_A$)로

분리한다(S202).

[0056] 상기 분리된 제1 해시([제1해시]$_A$)는 내부 특정 메모리(미도시)에 저장된다.

[0057] 상기와 같이 제2 개인키(B)로 암호화된 펌웨어가 복호화되면, 상기 금융 단말기(110 ~ 130)는, 미리 설정된 해시 생성 알고리즘(상기 금융 서버의 해시 생성 알고리즘과 동일한 알고리즘)을 이용하여, 상기 복호화된 펌웨어의 해시(즉, 제2 해시)를 자체적으로 생성한다. 그리고 상기 자체적으로 생성된 해시(즉, 제2 해시)를 내부의 특정 메모리(예 : 시큐어 메모리)(미도시)에 저장한다(S203).

[0058] 상기 금융 단말기(110 ~ 130)는 상기 제1 개인키(A)에 대응되는 공개키를 보유하고 있을 경우, 상기 제1 개인키(A)로 암호화된 제1 해시(예 : [제1해시]$_A$)를 복호화할 수 있다(S204).

[0059] 그러나 상기 금융 단말기(110 ~ 130)가 상기 제1 개인키(A)에 대응되는 공개키를 보유하고 있지 않을 경우, 상기 제1 해시(예 : [제1해시]$_A$)를 복호화하지 않은 상태로 저장할 수 있다. 즉, 상기 단계(S204)는 실시예에 따라서 생략될 수도 있다.

[0060] 만약, 상기 금융 단말기(110 ~ 130)가 상기 제1 개인키(A)에 대응되는 공개키를 이용해 상기 제1 해시(예 : [제1해시]$_A$)를 복호화 했을 경우, 상기 금융 단말기(110 ~ 130)는 자체적으로 생성한 제2 해시와 상기 복호화된 제1 해시를 비교한다(S205).

[0061] 그리고 상기 비교 결과에 따라, 두 해시 값(즉, 제1 해시, 제2 해시)이 동일한 경우(S206의 예), 상기 금융 단말기(110 ~ 130)는 상기 복호화된 펌웨어에 대한 무결성이 보장된 것으로 판단하여 상기 무결성이 보장된 펌웨어를 이용해 업그레이드를 수행한다(S207). 그러나 상기 제1 해시와 제2 해시가 동일하지 않은 경우(S206의 아니오), 상기 금융 단말기(110 ~ 130)는 상기 금융 서버(200)로부터 전송받은 펌웨어에 대한 무결성이 훼손된 것으로 판단하여 무결성 훼손 알림(예 : 금융 서버 및 금융 단말기에 경고 출력)을 출력하고 펌웨어 업그레이드를 중지한다(S208).

[0062] 하지만, 실시예에 따라 상기 단계(S204)가 생략될 경우, 그 이후의 모든 단계(S205 ~ S208)가 생략될 수 있으며, 이에 따라 상기 금융 단말기(110 ~ 130)는 펌웨어에 대한 자체적인 무결성 체크를 수행하지 않고, 상기 복호화된 펌웨어를 이용해 곧바로 펌웨어 업그레이드를 수행할 수도 있다.

[0063] 도 4는 본 발명의 일 실시예에 따라 펌웨어 업그레이드 후 및 평상시의 펌웨어 무결성 체크를 위한 금융 단말기 측의 동작을 설명하기 위한 흐름도이다.

[0064] 도 4에 도시된 바와 같이, 상기 금융 단말기(110 ~ 130)는 미리 설정된 이벤트 발생 시(즉, 상기 펌웨어 업그레이드 후, 및 평상시(예 : 결제요청 정보를 금융 서버로 전송할 때, 및 일정 주기가 되었을 때 등))(S301의 예), 상기 금융 단말기(110 ~ 1130)에 설치된 펌웨어에 대하여 자체적으로 생성한 제2 해시, 상기 인증값(즉, 제1 개인키(A)로 암호화된 제1 해시([제1해시]$_A$)), 및 전문(예 : 결제정보, 금융단말기 상태/동작정보 등의 데이터)이 포함된 정보(즉, 무결성 체크를 위한 정보)를 생성한다(S302).

[0065] 그리고 상기 금융 단말기(110 ~ 130)는 상기 생성된 정보(전문 + 제2 해시 + 인증값([제1해시]$_A$))를 상기 금융 서버(200)에 전송한다(S303).

[0066] 이때 상기 금융 서버(200)에 전송되는 정보(전문 + 제2 해시 + 인증값([제1해시]$_A$))는 상기 제2 개인키(B)에 대응하는 공개키로 암호화될 수도 있다.

[0067] 도 5는 본 발명의 일 실시예에 따라 펌웨어 업그레이드 후 및 평상시의 펌웨어 무결성 체크를 위한 금융 서버 측의 동작을 설명하기 위한 흐름도이다.

[0068] 도 5에 도시된 바와 같이, 상기 금융 서버(200)는 상기 금융 단말기(110 ~ 130)로부터 무결정 체크를 위한 정보(전문 + 제2 해시 + 인증값([제1해시]$_A$))를 전송 받은 후(S401), 상기 무결정 체크를 위한 정보에 포함된 제2 해시와 상기 제1 해시를 비교한다(S402).

[0069] 그리고 상기 비교 결과에 따라, 두 해시 값(즉, 제1 해시, 제2 해시)이 동일한 경우(S403의 예), 상기 금융 단말기(110 ~ 130)에 전송된(또는 설치된) 펌웨어에 대한 무결성이 보장된 것으로 판단한다(S404).

[0070] 그러나 상기 제1 해시와 제2 해시가 동일하지 않은 경우(S403의 아니오), 상기 금융 서버(200)는 상기 금융 단

말기(110 ~ 130)에 전송된(또는 설치된) 펌웨어에 대한 무결성이 훼손된 것으로 판단하여 무결성 훼손 알림(예 : 금융 서버 및 금융 단말기에 경고 출력)을 출력한다(S405).

[0071] 상기와 같이 본 실시예는 금융 단말기(110 ~ 130)의 펌웨어를 업그레이드하거나 평상시 금융 단말기(110 ~ 130)에 전송되거나 설치된 펌웨어에 대하여 무결성 체크를 수행할 수 있도록 한다.

[0072] 이상으로 본 발명은 도면에 도시된 실시예를 참고로 하여 설명되었으나, 이는 예시적인 것에 불과하며, 당해 기술이 속하는 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 기술적 보호범위는 아래의 특허청구범위에 의해서 정하여져야 할 것이다.

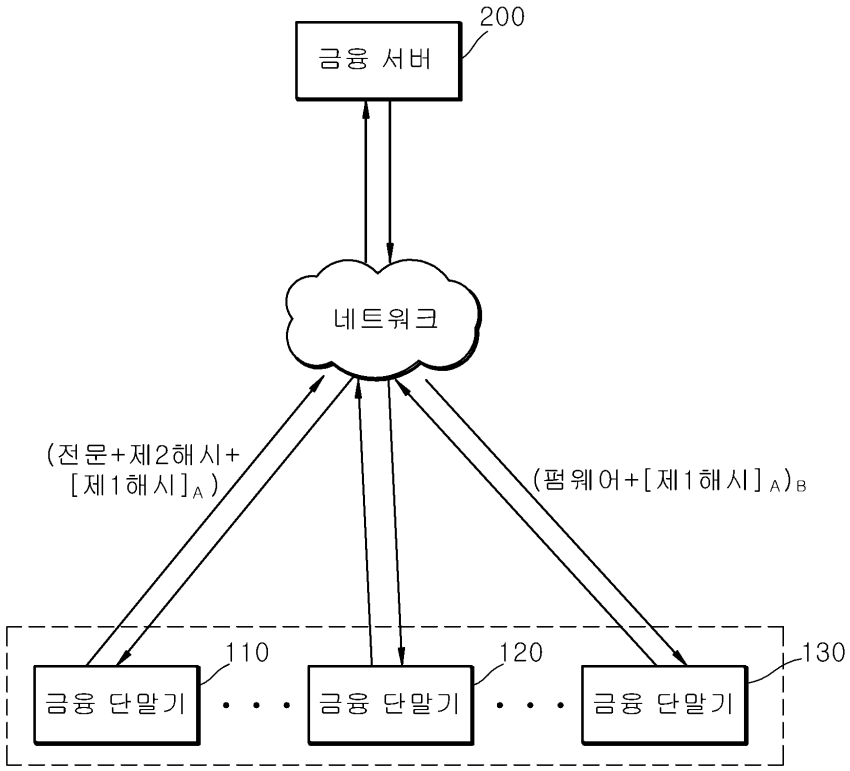
부호의 설명

[0073] 110 ~ 130 : 금융 단말기

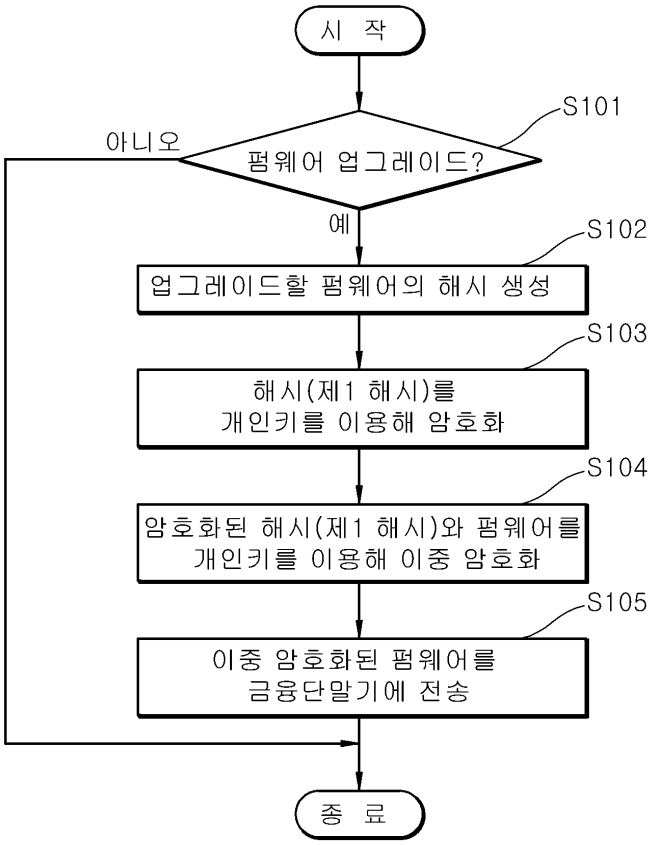
200 : 금융 서버

도면

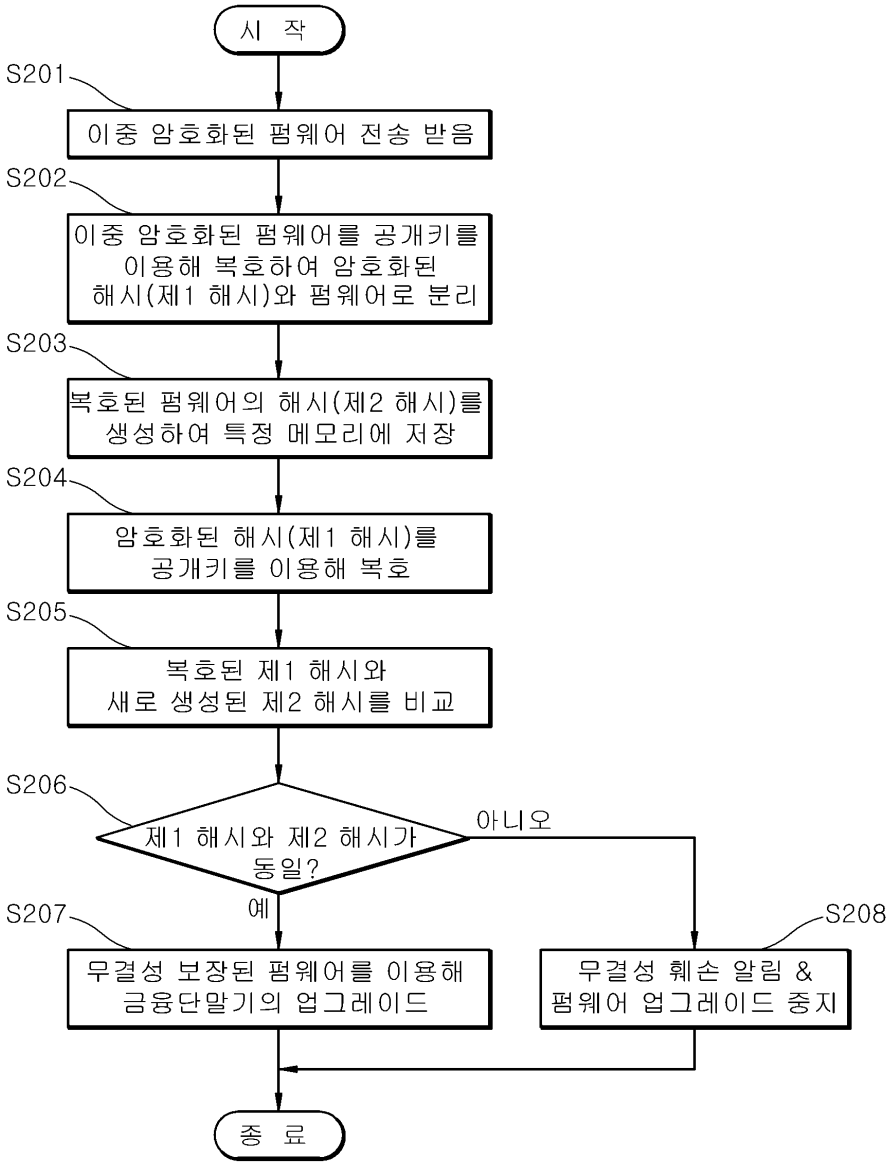
도면1



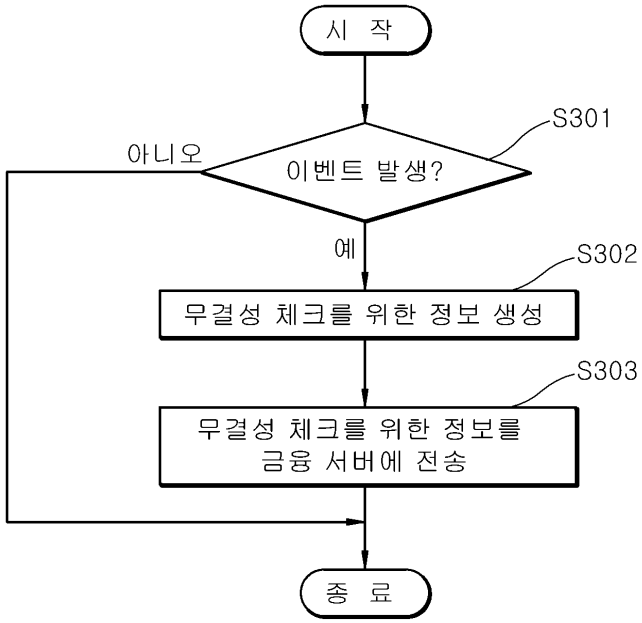
도면2


시 작
S101
펌웨어 업그레이드?
아니오
예
S102
업그레이드할 펌웨어의 해시 생성
S103
해시(제1 해시)를
개인키를 이용해 암호화
S104
암호화된 해시(제1 해시)와 펌웨어를
개인키를 이용해 이중 암호화
S105
이중 암호화된 펌웨어를
금융단말기에 전송
종 료

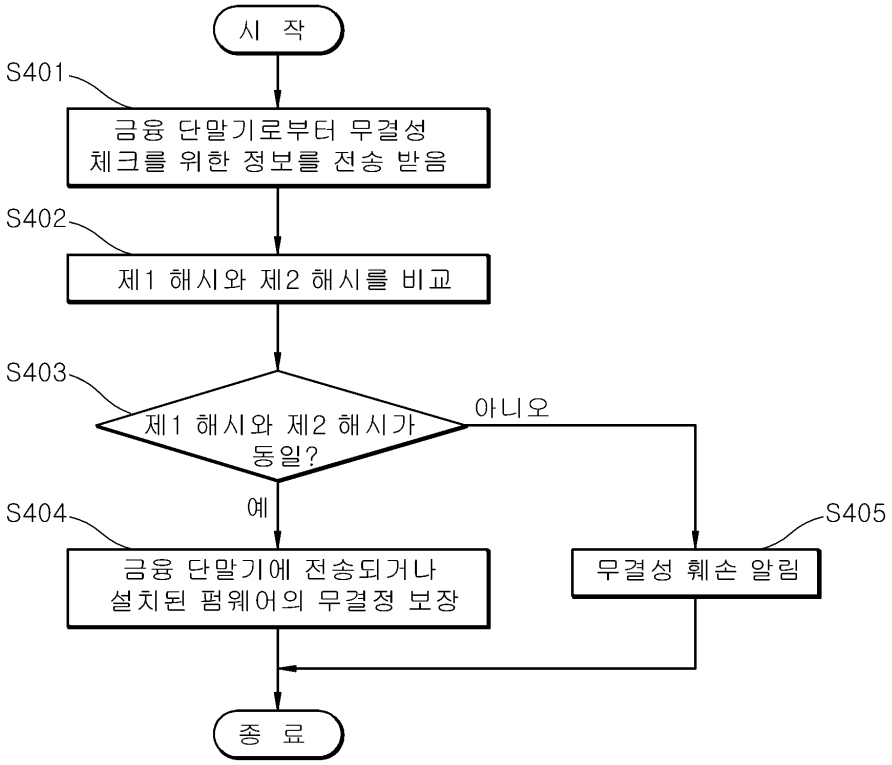
도면3


시 작
S201
이중 암호화된 펌웨어 전송 받음
S202
이중 암호화된 펌웨어를 공개키를 이용해 복호하여 암호화된 해시(제1 해시)와 펌웨어로 분리
S203
복호된 펌웨어의 해시(제2 해시)를 생성하여 특정 메모리에 저장
S204
암호화된 해시(제1 해시)를 공개키를 이용해 복호
S205
복호된 제1 해시와 새로 생성된 제2 해시를 비교
S206
제1 해시와 제2 해시가 동일?
아니오
예
S207
무결성 보장된 펌웨어를 이용해 금융단말기의 업그레이드
S208
무결성 훼손 알림 & 펌웨어 업그레이드 중지
종 료

도면4


시 작
S301
이벤트 발생?
아니오
예
S302
무결성 체크를 위한 정보 생성
S303
무결성 체크를 위한 정보를
금융 서버에 전송
종 료

도면5


시 작
S401
금융 단말기로부터 무결성
체크를 위한 정보를 전송 받음
S402
제1 해시와 제2 해시를 비교
S403
제1 해시와 제2 해시가
동일?
아니오
예
S404
금융 단말기에 전송되거나
설치된 펌웨어의 무결정 보장
S405
무결성 훼손 알림
종 료