(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0069502
(43) 공개일자 2013년06월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/30 (2013.01) *G06F 9/24* (2006.01)
(21) 출원번호 10-2012-0146376
(22) 출원일자 2012년12월14일
심사청구일자 없음
(30) 우선권주장
11306683.1 2011년12월16일
유럽특허청(EPO)(EP)

(71) 출원인
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 잔 다르크 뤼 1-5
(72) 발명자
스떼예르, 장-마리
프랑스 쎄에스 176 16 - 35 576 쎄쏭 쎄비네 자크 데 샹 블랑 아브뉘 데 샹 블랑 975 떼끄니꼴로르 에르 에 데 프랑스
루스띠드, 디디에
프랑스 쎄에스 176 16 - 35 576 쎄쏭 쎄비네 자크 데 샹 블랑 아브뉘 데 샹 블랑 975 떼끄니꼴로르 에르 에 데 프랑스
(74) 대리인
백만기, 양영준, 전경석

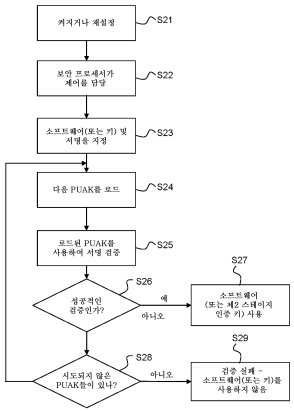
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **서명 검증을 위한 장치 및 방법**

(57) 요 약

수신기(100)는, 보안 프로세서(103)와, 소프트웨어 코드 또는 제2 스테이지 인증 키(107) 및 소프트웨어 또는 제2 스테이지 키를 위한 서명(108)을 저장하는 제1 메모리(106)를 포함한다. 수신기는 또한 복수의 검증 키(PUAKs)를 저장한다. 수신기가 켜지거나 재설정될 때(S21), 소프트웨어 또는 제2 스테이지 키(107) 및 서명(108)은 제1 메모리(106)로부터 로드된다(S23). 보안 프로세서(103)는 그 다음 PUAK를 로드하고(S24) 그것을 사용하여 서명(108)을 검증한다(S25). 성공적인 검증의 경우에, 소프트웨어 코드 또는 제2 스테이지 키가 사용되고(S27), 검증 방법은 종료되며; 그 다음 수신기에서 CA 특정 기능들을 활성화하는 것이 가능하다. 그러나, 검증에 성공하지 못한 경우, 시도되지 않은 PUAK들이 존재하는지가 검증된다(S28). 시도되지 않은 서명이 존재하지 않는 경우, 검증은 실패이고(S29) 소프트웨어는 검증될 수 없으며; 검증 방법은 종료된다. 시도되지 않은 서명이 존재하는 경우, 다음 PUAK가 로드된다(S25). 다시 말해, PUAK들이 반복적으로 또는 병렬로 시도된다.

대 표 도 - 도2



특허청구의 범위

청구항 1

디지털 데이터(107)를 위한 디지털 서명(108)을 검증하기 위한 장치(100)로서,

제1 인증 키(PUAK A)를 저장하도록 구성된 제1 메모리(105);

상기 디지털 데이터(107)를 저장하도록 구성된 제2 메모리(106) - 상기 디지털 데이터는 상기 장치(100)를 위한 부팅 코드 또는 디지털 데이터를 더 인증하는데 사용될 제2 스테이지 인증 키를 포함함 - ; 및

상기 장치(100)의 작동 시작(power up)이나 재설정 시에, 상기 디지털 데이터(107)와 상기 디지털 서명(108)을 수신하고, 상기 제1 검증 키(PUAK A)로 상기 디지털 서명(108)을 처리하여 상기 디지털 서명(108)을 검증하도록 구성된 프로세서(103)

를 포함하고,

상기 제1 메모리(105)는 또한 제2 검증 키(PUAK B)를 저장하도록 더 구성되고, 상기 제1 검증 키 및 상기 제2 검증 키는 제1 서명인 엔티티 및 제2 서명인 엔티티의 서명 키들에 각각 대응하고,

상기 프로세서(103)는 상기 제2 인증 키(PUAK B)로 상기 디지털 데이터(107)를 처리하여 상기 디지털 서명(108)을 검증하도록 또한 구성되는 것을 특징으로 하는 디지털 서명 검증 장치.

청구항 2

제1항에 있어서, 상기 제1 메모리(105)는 복수의 검증 키(PUAK)를 저장하도록 구성되는 디지털 서명 검증 장치.

청구항 3

제2항에 있어서, 상기 프로세서(103)는, 상기 디지털 서명(108)이 성공적으로 검증될 때까지 또는 저장된 모든 검증 키를 사용해도 성공하지 못할 때까지, 상기 디지털 서명(108) 및 상기 저장된 검증 키들(PUAK) 각각을 사용하여 상기 디지털 서명(108)을 검증하도록 구성되는 디지털 서명 검증 장치.

청구항 4

제1항에 있어서, 상기 프로세서(103)는, 상기 디지털 서명(108)이 상기 제1 인증 키(PUAK A)를 사용하여 성공적으로 검증되지 못한 경우, 상기 제2 인증 키(PUAK B)로 상기 디지털 서명(108)를 처리하여 상기 디지털 서명(108)을 검증하도록 구성되는 디지털 서명 검증 장치.

청구항 5

제1항에 있어서, 상기 프로세서(103)는 제1 검증 키(PUAK A)와 제2 검증 키(PUAK B)를 병렬로 사용하여 상기 서명을 검증하도록 구성되는 디지털 서명 검증 장치.

청구항 6

제1항에 있어서, 상기 부팅 코드는 내장되어 있는 디지털 서명 검증 장치.

청구항 7

제6항에 있어서, 상기 장치(100)는, 상기 디지털 서명(108)이 성공적으로 인증되는 경우에, 상기 부팅 코드를 실행하도록 구성된 제2 프로세서(104)를 더 포함하는 디지털 서명 검증 장치.

청구항 8

제1항에 있어서, 상기 프로세서는, 상기 디지털 데이터(107)의 성공적인 검증 시에, 현재 CA 시스템을 식별하고 CA 특정 기능들을 활성화하도록 더 구성되는 디지털 서명 검증 장치.

청구항 9

제1항에 있어서, 상기 제1 메모리(105)는 기록할 수 없는(non-writable) 것인 디지털 서명 검증 장치.

청구항 10

장치(100)를 위한 부팅 코드 또는 추가의 디지털 데이터를 인증하는데 사용될 제2 스테이지 인증 키를 포함하는, 디지털 데이터(107)를 위한 디지털 서명(108)을 검증하기 위한 방법으로서,

상기 장치(100)의 작동 시작이나 재설정 시에, 프로세서(103)에서,

상기 디지털 데이터(107)와 상기 디지털 서명(108)을 수신하는 단계(S23); 및

검증 키(PUAK)를 획득하는 단계(S24) 및 획득된 검증 키(PUAK)로 상기 디지털 서명(108)을 처리하여 상기 디지털 서명(108)을 검증하는 단계(S25)에 의해, 상기 디지털 서명을 복수 회 검증하는 단계

를 포함하고,

상이한 검증 키(PUAK)가 획득되고 상기 복수 회 각각에 대해 사용되는 디지털 서명 검증 방법.

청구항 11

제10항에 있어서, 상기 획득하는 단계(S24)와 상기 검증하는 단계(S25)는 병렬로 수행되는 디지털 서명 검증 방법.

청구항 12

제10항에 있어서, 상기 획득하는 단계(S24)와 상기 검증하는 단계(S25)는, 상기 디지털 서명(108)이 성공적으로 검증될 때까지 또는 상기 프로세서(103)가 사용가능한 모든 검증 키(PUAK)로 시도해도 성공하지 못할 때까지 반복적으로 수행되는 디지털 서명 검증 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 보안에 관한 것으로, 특히, 디지털 서명의 검증에 관한 것이다.

배 경 기 술

[0002] 이 섹션은, 아래 설명 및/또는 청구되는 본 발명의 다양한 측면과 관련될 수 있는, 본 발명의 기술 분야의 다양한 측면을 독자에게 소개하기 위한 것이다. 이러한 논의는, 본 발명의 다양한 측면에 대한 이해를 더 용이하게 하기 위해 배경 정보를 독자에게 제공하는데 도움이 될 것으로 믿어진다. 따라서, 이러한 진술들은 상기의 견지에서 읽혀져야 하고, 종래 기술에 대한 인정이 아니라는 것이 이해되어야 한다.

[0003] 디지털 콘텐츠, 이를테면, 예컨대, 프리미엄 가치 디지털 텔레비전 프로그램들을 보호하기 위해, 소위 조건부 액세스(Conditional Access; CA) 기술을 사용하는 것이 본 발명의 기술 분야에서 잘 알려져 있다. 이러한 기술은 디지털 콘텐츠를 암호화하고 나중에 해독하기 위해, 또한 무단 사용(unauthorized use)으로부터 단말기들을 보호하기 위해 상이한 암호화 프로토콜들을 사용한다.

[0004] CA 기술은, CA 제공자가 사용자에게, 직접적으로 또는 간접적으로, 제공한 일부 종류의 (보통 이동식(removable)) 보안 요소를 사용하여, 수신기들, 예를 들어, 텔레비전 세트들 및 소위 셋-톱 박스들(STBs)에서 구현된다. 이러한 보안 요소의 바람직한 구현은, 본 발명의 기술 분야에서 잘 알려진, 스마트카드이다.

[0005] 보통은 CA 보호된 디지털 콘텐츠에 액세스하기 위해 비용을 지불할 필요가 있으나, 저작권 침해자들(pirates)은 비용을 지불하지 않고 CA 보호된 디지털 콘텐츠에 액세스하기 위해 CA 시스템을 '해킹'하려고 시도한다는 것은 매우 흔한 일이라는 것이 인식될 것이다. 스마트카드가 점점 더 안전해 짐에 따라 - 즉, 해킹하기가 점점 더 어려워짐에 따라 - 저작권 침해자들은 직접적으로 수신기들을 공격하려는 경향이 있다.

[0006] 물론, 수신기 제조자들은, 지원된 CA 제공자가 필요로 하고 지정하는 특정 보안 특징들을 구현하고, 특별히 구현한 CA 전용 버전의 메인 IC를 사용하여, 그들의 수신기들의 보안을 개선하기 위해 노력하고 있다

[0007] ● 128 비트 대칭 키로서 구현될 수 있는 SRK(Secret Root Key), 및

[0008] ● 유리하게 비대칭 1024 또는 2048 비트 RSA 키로서 구현될 수 있는 PUAK(Public Authentication Key).

[0009] 칩 제공자들이 구현하는 이러한 보안 특징들은 제공된 특정한 CA의 보안 요구사항들을 만족해야 한다. 제1 CA 제공자 A는 제2 CA 제공자 B와는 상이한 보안 요구사항들을 가질 가능성이 높다. 이는, A를 위해 맞춰지는(customized) 컴포넌트들은 B를 위해 작동하지 않거나 허용되지 않을 수 있다는 것을 의미할 수 있고; 게다가, CA 제공자들은 보통 다른 CA 제공자들에게 그들의 솔루션을 전달하지 않는다.

[0010] 또한, CA 제공자들은 종종 상업적 경쟁자들(commercial rivals)인 만큼, 그들은 보안 요구사항들의 공통 집합에 동의하기 어려울 수 있다. 이러한 상업적 경쟁은 따라서 CA 제공자로 하여금 그들의 보안 요구사항들을 개선하고 이를 비밀로 유지하도록 독려한다.

[0011] 이러한 이유로, 특정 CA 제공자들은, 칩 제공자 '표준' 보안 특징(chip providers 'standard' security features) 대신 사용하기 위해, 칩 제공자를 위한 사유 보안 블록(proprietary security block)을 제공한다.

[0012] 따라서 상이한 CA 제공자들은 상이한 보안 특징들을 제공한다는 것을 알 수 있다.

[0013] CA 제공자들의 클라이언트들, 이를테면, 유료 TV 오퍼레이터들(pay TV operators)은 복수의 CA 제공자로부터의 제품들을 사용할 수 있다는 것에 관심을 갖는다는 것 또한 인식될 것이다. 그러나 지금까지는 오퍼레이터가 CA 제공자를 선택하면, 다음의 이유로 새로운 것으로 전환하기가 어렵다.

[0014] ● 설치된 수신기를 변경하는데 비용이 많이 들고; 과거(old) 및 새로운(new) 수신기들 모두 동일한 방식으로 작동할 수 있도록 보장되어야 한다.

[0015] ● 감소된 보안에 대한 위험을 감수하지 않고 필요로 된 보안 특징들을 가능하게 하는 플랫폼을 새로운 CA 제공자에게 제공하기는 어렵다.

[0016] 이러한 이유로, 유료 TV 오퍼레이터들은 CA 제공자들로부터 가능한 독립적일 수 있기를 원하므로, 동일한 수신기 하드웨어가 상이한 CA 시스템들과 사용될 수 있어, 상이한 보안 요구사항들이 독립적으로 지원된다.

[0017] 수신기가 복수의 CA 제공자와 호환되기 위한 요구사항은, 각각의 CA 제공자의 보안 기능들, 즉, 보안 블록이 칩 제조자가 제공한 칩에 통합되는 경우 만족될 수 있다.

[0018] SW 인증 체인(SW Authentication chain):

[0019] 예컨대, 작동 시작(power up) 시에, 수신기에 내장된 소프트웨어(또는 제2 스테이지 인증 키)가 유효하다는 검증에 의해, 단지 인증된 소프트웨어만 수신기에 설치되도록 보장하기 위해, 유리하게 CA 제공자가 보유하는 PRAK(Private Asymmetric Key)를 사용하여 소프트웨어(또는 제2 스테이지 인증 키)에 디지털적으로 서명하는 것이 알려져 있다. 본 발명의 기술 분야에서 잘 알려진 바와 같이, 작동 시작 시에, 수신기는 PRAK에 대응하는 그의 PUAK(Public Authentication Key)를 사용하여, 수신기에 내장된 소프트웨어(또는 제2 스테이지 인증 키)의 서명을 검증한다.

[0020] CA 제공자를 위한 PUAK는 CA 제공자의 보안 요구사항들을 충족하기 위한 칩의 사용자 지정(customization)의 일부이다.

[0021] 지금까지는, 단일 CA 제공자의 PUAK는 칩에 저장된다. 이것은, 또 다른 CA 제공자의 다른 모든 보안 특징들이 칩에 구현된 경우에도, 칩이 복수의 CA 시스템과 호환되는 것이 불가능하다는 것을 의미한다.

[0022] 따라서 당업자는 수신기가 복수의 PUAK를 저장 및 사용하는 것을 허용하는 솔루션이 필요하다는 것을 인식할 것이다. 본 발명은 이러한 솔루션을 제공한다.

발명의 내용

[0023] 제1 측면에서, 본 발명은 디지털 데이터를 위한 디지털 서명을 검증하기 위한 장치에 관한 것이다. 장치는, 제1 인증 키를 저장하도록 구성된 제1 메모리; 디지털 데이터를 저장하도록 구성된 제2 메모리 - 디지털 데이터는 장치를 위한 부팅 코드(boot code) 또는 디지털 데이터를 더 인증하는데 사용될 제2 스테이지 인증 키를 포함함 - ; 및 장치의 작동 시작이나 재설정 시에, 디지털 데이터와 디지털 서명을 수신하고, 제1 검증 키로 디지털 서명을 처리하여 디지털 서명을 검증하도록 구성된 프로세서를 포함한다. 제1 메모리는 제2 검증 키를 저장하도록 더 구성되고, 제1 검증 키 및 제2 검증 키는 각각 제1 서명인 엔티티(signatory entity) 및 제2 서명인 엔티티의 서명 키들에 대응하고; 프로세서는 제2 인증 키로 디지털 데이터를 처리하여 디지털 서명을 검증하도록 더

구성된다.

[0024] 바람직한 제1 실시예에서, 제1 메모리는 복수의 검증 키를 저장하도록 구성된다. 프로세서는, 디지털 서명이 성공적으로 검증될 때까지 또는 저장된 모든 검증 키를 사용해도 성공하지 못할 때까지, 디지털 서명 및 저장된 검증 키들 각각을 사용하여 디지털 서명을 검증하도록 구성되는 것이 유리하다.

[0025] 바람직한 제2 실시예에서, 프로세서는, 디지털 서명이 제1 인증 키를 사용하여 성공적으로 검증되지 못한 경우, 제2 인증 키로 디지털 서명을 처리하여 디지털 서명을 검증하도록 구성된다.

[0026] 바람직한 제3 실시예에서, 프로세서는 제1 검증 키 및 제2 검증 키를 병렬로 사용하여 서명을 검증하도록 구성된다.

[0027] 바람직한 제4 실시예에서, 부팅 코드(boot code)는 내장되어 있다. 장치는, 디지털 서명이 성공적으로 인증되는 경우에, 부팅 코드를 실행하도록 구성된 제2 프로세서를 더 포함하는 것이 유리하다.

[0028] 바람직한 제5 실시예에서, 프로세서는, 디지털 데이터의 성공적인 검증 시, 현재 CA 시스템을 식별하고 CA 특정 기능들을 활성화하도록 더 구성된다.

[0029] 바람직한 제6 실시예에서, 제1 메모리는 기록할 수 없는 것(non-writable)이다.

[0030] 제2 측면에서, 본 발명은, 장치를 위한 부팅 코드 또는 디지털 데이터를 더 인증하는데 사용될 제2 스테이지는 인증 키를 포함하는 디지털 데이터를 위한 디지털 서명을 검증하기 위한 방법에 관한 것이다. 장치의 작동 시작이나 재설정 시, 프로세서는 디지털 데이터와 디지털 서명을 수신하고; 검증 키를 획득하고, 획득된 검증 키로 디지털 서명을 처리하여 디지털 서명을 검증하여, 복수 회(a plurality of times) 디지털 서명을 검증한다. 상이한 검증 키가 획득되어, 복수 회 각각에 사용된다.

[0031] 바람직한 제1 실시예에 있어서, 획득 단계와 검증 단계는 병렬로 수행된다.

[0032] 바람직한 제2 실시예에서, 획득 단계와 검증 단계는, 디지털 서명이 성공적으로 검증될 때까지 또는 프로세서가 사용가능한 모든 검증 키로 시도해도 성공하지 못할 때까지 반복적으로 수행된다.

도면의 간단한 설명

[0033] 이제, 첨부 도면을 참조하여, 본 발명의 바람직한 특징들이 비-한정 예로서 설명될 것이다.

도 1은 본 발명의 바람직한 실시예에 따른 수신기를 도시한다.

도 2는 본 발명의 바람직한 실시예에 따른 소프트웨어 또는 제2 스테이지 인증 키 서명의 검증을 위한 방법을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0034] 본 발명의 주된 독창적인 아이디어는, 복수의 CA 제공자로부터 기원한 서명들을 검증할 수 있기 위해, 복수의 인증 키(PUAK)를 저장하는 조건부 액세스(Conditional Access; CA) 시스템에 수신기를 제공하는 것이다. 수신기는 바람직하게는 셋-톱 박스(STB)이지만, 텔레비전 세트와 같은 임의의 다른 적절한 디바이스일 수 있다.

[0035] 도 1은 본 발명의 바람직한 실시예에 따른 수신기를 도시한다. 수신기(100)는 보안된 칩(secured chip; 102) 및 제1 (바람직하게는 비-휘발성) 메모리(106)를 포함한다. 도면에는 단지 본 발명에 필요한 특징들만 도시된다는 것이 인식될 것이다.

[0036] 제1 메모리(106)는, 바람직한 실시예에서 소프트웨어(이하에서 예로서 사용됨)이고, 유리하게는 수신기가 켜지거나 재설정될 때 사용되는 소위 부팅 코드인 디지털 데이터(107), 및 소프트웨어를 위한 디지털 서명(108)을 저장한다. 소프트웨어(107) 및 서명(108)은 단일 파일의 일부인 것이 바람직하다. 디지털 데이터(107)는 또한 제2 스테이지는 인증 키일 수 있다.

[0037] 효율성을 이유로, 보안된 칩(102)은 바람직하게는 보안 프로세서(103)와 메인 프로세서(104)를 포함한다. 보안 프로세서(103)는, 이하에서 설명되는 바와 같이, 소프트웨어 서명(108)을 검증하도록 구성된다. 보안된 칩(102)은 제2 메모리(105), 바람직하게는 기록할 수 없는, 즉 복수의 인증 키(PUAKs)를 보유하는 ROM(read only memory)을 더 포함한다. 도 1에는, 단지 2개의 PUAK: PUAK A 및 PUAK B가 있다. 그러나 적어도 보안된 칩을 사용할 수 있는 CA 제공자들만큼 많은 PUAK를 저장하는 것이 유리하다는 것이 이해될 것이다 - 일부 CA 제공자

들은 그들의 소프트웨어에 대해 복수의 서명을 제공하기 위해 복수의 키를 사용할 수 있다.

[0038] 보안 프로세서(103)는 서명(108)의 검증을 위해 어떤 PUAK를 사용해야 하는지를 알지 못하므로, 지금까지 설명한 바와 같이, 수신기(100)는 복수의 CA 제공자와 호환되기에 충분하지 않다.

[0039] 도 2는 본 발명의 바람직한 실시예에 따른 소프트웨어 서명(108)의 검증을 위한 방법을 도시한다.

[0040] 단계 S21에서, 수신기는 켜지거나 재설정되고, 이는, 제1 메모리(106)에 저장된 인증될 소프트웨어(107)를 가리키도록 수신기에게 요구한다. 이 시점에 수신기는 어떤 엔티티가 소프트웨어 서명(108)을 제공하는지 알지 못하고 결과적으로 어떤 PUAK를 사용할지를 알지 못한다는 것이 인식될 것이다.

[0041] 보안 프로세서(103)은 보안된 칩(102)의 제어를 담당한다(단계 S22). 소프트웨어(107) 및 서명(108)은 그 다음 제1 메모리(106)로부터 보안된 칩(102)으로 로드된다(단계 S23).

[0042] 보안 프로세서(103)는 그 다음 제2 메모리(105)로부터 PUAK를 로드하고(단계 S24), 그것을 사용하여 서명(108)을 검증한다(단계 S25).

[0043] 단계 S26에서 검증이 성공적이면("Y") 그 다음 단계 S27에서 소프트웨어 코드가 사용되고; 검증 방법은 종료된다.

[0044] 이에 반해, 단계 S26에서 검증에 성공하지 못한 경우("N") 그 다음 더 많은 PUAK들, 즉, 서명(108)의 검증을 위해 사용되지 않은 PUAK들이 존재하는지가 검증된다.

[0045] 단계 S28에서 더 이상 서명이 존재하지 않는 경우("N") 검증은 실패이고(단계 S29), 검증될 수 없으므로 그 소프트웨어는 사용되어서는 안 되고, 검증 방법은 종료된다. 단계 S28에서 시도되지 않은 서명이 존재하는 경우("Y") 단계 S25에서 제2 메모리로부터 다음 PUAK가 로드된다.

[0046] 검증 방법이 종료될 때, 보안 프로세서(103)는 보안된 칩의 통제권을 다시 메인 프로세서(104)에게 넘겨줄 수 있다. 데이터가 제2 스테이지 인증 키인 경우에, 보안된 칩은 인증된 제2 스테이지 인증 키를 사용하여 제2 스테이지 인증을 수행할 수 있다.

[0047] 환언하면, 방법은 연속적으로(반복적으로) 소프트웨어 서명을 검증하기 위해 저장된 PUAK 키들을 시도한다. PUAK가 서명을 검증하는 경우, 소프트웨어는 성공적으로 검증되고; 어떠한 PUAK도 서명을 검증하지 못하는 경우, 소프트웨어는 성공적으로 검증되지 않는다.

[0048] 당업자는 적어도 두 개의 PUAK를 병렬로 시도할 수도 있다는 것을 인식할 것이고; 주된 포인트는 하나의 PUAK가 소프트웨어 서명을 성공적으로 검증한 경우에 소프트웨어가 성공적으로 검증된다는 점이다.

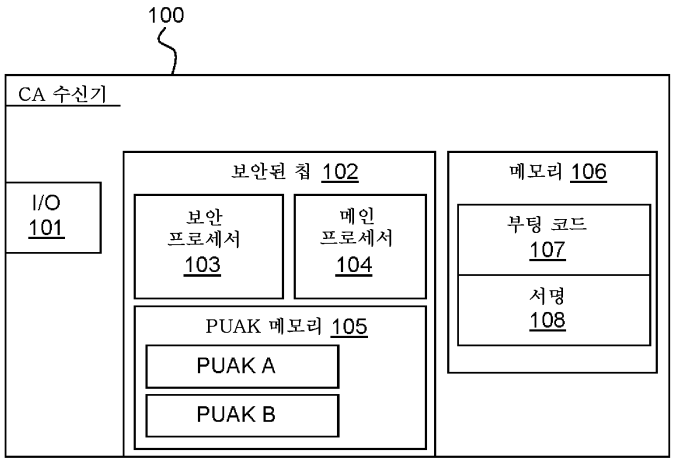
[0049] 따라서, 소프트웨어 서명이 임의의 복수의 서명인에 의해 제공되었을 때, 본 발명은, 소프트웨어 서명을 검증하기 위한 수신기를 위한 방식을 제공할 수 있다는 것이 인식될 것이다. 이는, 사용할 키를 아는 방식이 존재하지 않는다고 믿어졌던 이전의 시스템에서는 가능하지 않았다는 것이 인식될 것이다. 본 발명은 따라서 중요하지만 지금까지 해결되지 않았던 기술적 문제에 대한 급진적인 새롭고 놀라운 솔루션을 제공한다. 또한, 본 발명은 사용되는 CA 시스템을 식별하는 것 또한 가능하게 할 수 있어, 수신기(100)에서 CA 특정 기능들의 활성화를 가능하게 한다.

[0050] 본 방법은, 소프트웨어 코드의 검증 또는 실제로 내부 메모리로부터 다운로드되는 디지털 데이터로 결코 한정되지 않는다는 것이 인식될 것이다.

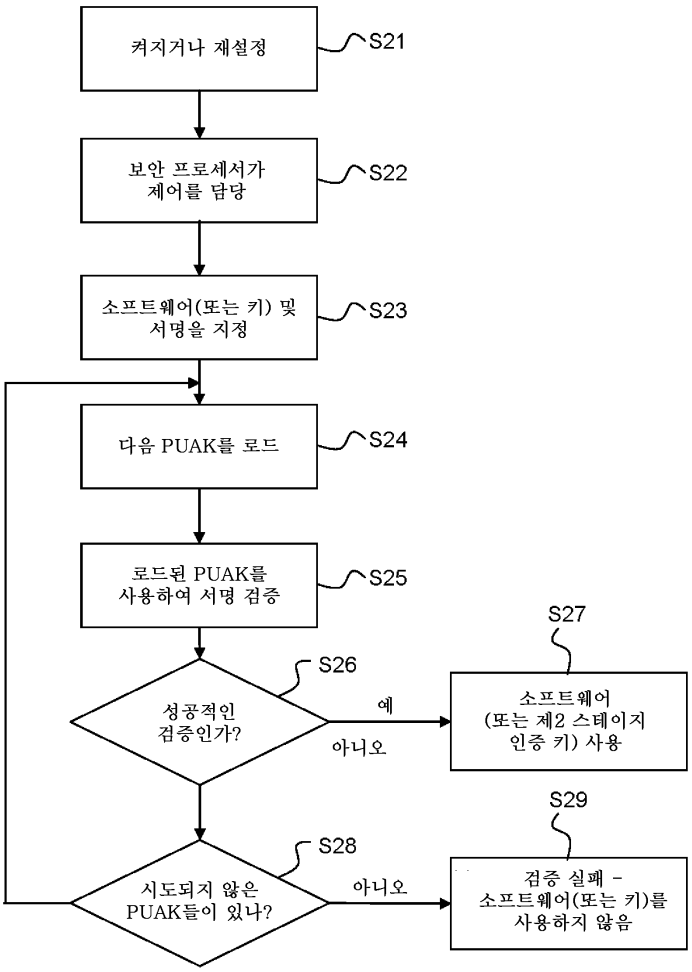
[0051] 설명 및 (적절한 곳에서) 청구항들 및 도면들에 개시된 각각의 특징은 독립적으로 또는 임의의 적절한 조합으로 제공될 수 있다. 하드웨어에서 구현되는 것으로 설명된 특징들은 또한 소프트웨어에서 구현될 수 있고, 그 반대일 수도 있다. 청구항들에 등장하는 도면 부호들은 단지 실례로서, 청구항들의 범주를 한정하는 효과는 없다.

도면

도면1


100
CA 수신기
I/O
101
보안된 칩 102
보안
프로세서
103
메인
프로세서
104
PUAK 메모리 105
PUAK A
PUAK B
메모리 106
부팅 코드
107
서명
108

도면2


켜지거나 재설정
S21
보안 프로세서가
제어를 담당
S22
소프트웨어(또는 키) 및
서명을 지정
S23
다음 PUAK를 로드
S24
로드된 PUAK를
사용하여 서명 검증
S25
S26
성공적인
검증인가?
예
아니오
S27
소프트웨어
(또는 제2 스테이지
인증 키) 사용
S28
시도되지 않은
PUAK들이 있나?
아니오
S29
검증 실패 -
소프트웨어(또는 키)를
사용하지 않음