(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년07월30일
(11) 등록번호 10-0973203
(24) 등록일자 2010년07월26일

(51) Int. Cl.
H04N 7/16 (2006.01) *G06F 9/22* (2006.01)
(21) 출원번호 10-2005-7005479
(22) 출원일자(국제출원일자) 2003년10월02일
심사청구일자 2008년09월02일
(85) 번역문제출일자 2005년03월30일
(65) 공개번호 10-2005-0083699
(43) 공개일자 2005년08월26일
(86) 국제출원번호 PCT/FR2003/050073
(87) 국제공개번호 WO 2004/032328
국제공개일자 2004년04월15일
(30) 우선권주장
02/12325 2002년10월04일 프랑스(FR)
(56) 선행기술조사문헌
JP09231068 A
JP14140298 A
EP0770957 A
WO0200064178 A1
전체 청구항 수 : 총 3 항

(73) 특허권자
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 루 잔다르크 1-5
(72) 발명자
차우, 헤르베
프랑스, 에프-77420 참프스 수르 마른, 아베뉴 앙페르, 31
사르파티, 장-끌로드
프랑스, 에프-93800 에피네이 수르 센, 플레이스 도베루셀, 2-4
(74) 대리인
김학수, 문경진

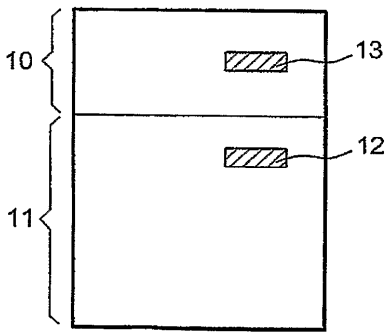
심사관 : 조남신

(54) 내장된 소프트웨어 및 이를 인증하는 방법

(57) 요 약

본 발명은 단말기에서 다운로딩된 소프트웨어를 인증하는 방법에 관한 것으로서, 상기 단말기에 내장된 소프트웨어를 사용하여 상기 다운로딩된 소프트웨어를 증명서에 의해 인증하는 단계와; 상기 다운로딩된 소프트웨어의 실행시, 상기 다운로딩된 소프트웨어와 연관된 인증 소프트웨어 모듈을 이용하여 상기 내장된 소프트웨어를 증명서에 의해 인증하는 단계를 포함한다.

대 표 도 - 도2



특허청구의 범위

청구항 1

단말기내에 다운로딩된 소프트웨어 인증 방법으로서,

제 1 증명서에 의해, 상기 단말기 내의 제 1 내장된 소프트웨어를 이용하여 상기 다운로딩된 소프트웨어를 인증하는 단계;

상기 다운로딩된 소프트웨어의 실행 동안, 상기 다운로딩된 소프트웨어와 연관된 검증 소프트웨어 모듈을 이용하여 상기 제 1 내장된 소프트웨어를 인증하는 단계를 포함하되,

상기 제 1 내장된 소프트웨어는 제 2 증명서를 이용하여 인증되고, 상기 제 1 내장된 소프트웨어는 인증 라이브러리 및 제 1 증명서를 사용하여 상기 다운로딩된 소프트웨어를 인증하고, 상기 제 1 내장된 소프트웨어 및 인증 라이브러리는 쓰기-방지된 메모리의 제 1 부분을 형성하고, 상기 다운로딩된 소프트웨어 및 제 1 증명서는 로딩가능한 메모리의 제 2 부분을 형성하며, 그리고

상기 쓰기-방지된 메모리의 제 1 부분은 상기 제 2 증명서를 추가로 포함하고, 상기 로딩가능한 메모리의 제 2 부분은 상기 검증 소프트웨어를 포함하고, 일단 상기 다운로딩된 소프트웨어가 인증된다면, 상기 검증 소프트웨어는 상기 인증 라이브러리 및 상기 제 2 증명서를 이용하여 상기 제 1 내장된 소프트웨어를 인증하는, 소프트웨어 인증 방법.

청구항 2

제 1 항에 있어서,

상기 다운로딩된 소프트웨어를 인증하는 단계와 상기 제 1 내장된 소프트웨어를 인증하는 단계는 상기 단말기의 초기화시 발생하는, 소프트웨어 인증 방법.

청구항 3

컴퓨터 시스템으로서,

프로세서; 및

쓰기-방지된 메모리인 제 1 부분과, 로딩가능한 메모리인 제 2 부분을 포함하는 메모리를 포함하되,

상기 제 1 부분은 제 1 내장된 소프트웨어, 인증 라이브러리, 및 제 2 증명서를 포함하고,

상기 제 2 부분은 다운로딩된 응용 소프트웨어, 제 1 증명서, 및 검증 소프트웨어를 포함하고,

상기 프로세서에 의해 실행되는 경우, 상기 제 1 증명서에 의해, 상기 제 1 내장된 소프트웨어를 이용하여 상기 다운로딩된 응용 소프트웨어를 인증하고,

상기 다운로딩된 응용 소프트웨어의 실행 동안 상기 검증 소프트웨어 모듈을 사용하여 상기 1 내장된 소프트웨어를 인증하고, 상기 제 1 내장된 소프트웨어는 제 2 증명서를 이용하여 인증되도록, 구성된 내장된 소프트웨어 명령어를 추가로 포함하되,

상기 제 1 내장된 소프트웨어는 상기 인증 라이브러리 및 제 1 증명서를 이용하여 상기 다운로딩된 응용 소프트웨어를 인증하고,

일단 상기 다운로딩된 응용 소프트웨어가 인증된다면, 상기 검증 소프트웨어는 상기 인증 라이브러리 및 제 2 증명서를 이용하여 상기 제 1 내장된 소프트웨어를 인증하는, 컴퓨터 시스템.

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 내장된 소프트웨어(integrated software)와 이 내장된 소프트웨어를 인증하는 방법에 관한 것으로서, 상세하게는 디지털 텔레비전 디코더 분야에 관한 것이다.

배 경 기 술

[0002] 종래 기술의 장치에 있어서, 내장된 소프트웨어의 무결성 검사는 통상적으로 외부 툴을 사용하여 이 내장된 소프트웨어를 대표하는 이 소프트웨어의 기준 서명(reference signature)을 계산하고 이 소프트웨어에 상기 기준 서명을 삽입함으로써 수행된다. 소프트웨어 초기화 시기 동안, 해당 소프트웨어는 자기 자신의 서명을 계산하고 이 자기 자신의 서명을 상기 기준 서명과 비교한다. 만약 이 서명들이 상이하다면, 해당 소프트웨어는 방어 절차(defense procedure)에 대해 특정된 소프트웨어 루틴을 실행하며, 상이하지 않다면 정상적으로 계속된다.

[0003] 이러한 소프트웨어의 인증의 경우, 상기 인증의 소스를 체크하는 것이 바람직하다. 기존 해법은, 무결성 검사 원리를 적용하는 단계 및 이를 비대칭 암호 알고리즘과 결합하는 단계로 구성된다. 즉, 기준 서명은 비밀키(private key)를 사용하여 암호화되고 그 결과물은 해당 소프트웨어에 증명서(certificate)의 형태로 내장된다. 체크 시기 동안, 이 기준 서명은 해당 소프트웨어에 포함되어 있는 공개키(public key)를 사용하여 해독된 후 기준 서명과 비교된다.

[0004] 종래 기술의 첫번째 자료로서, 표제가 "Digital Video Broadcasting(DVB) Multimedia Home Platform(MHP) Specification 1.0"인 ETSI standard TS 101 812 V1-1-1 (2000-07)에서 특히 섹션 12.2와 12.7은, 단말기로 다운로딩된 소프트웨어를 상기 단말기에 내장된 소프트웨어를 이용하여 상기 다운로딩된 소프트웨어의 증명서에 의한 인증을 수행함으로써 인증하는 방법의 구현에 대해 기술하고 있다.

[0005] 종래 기술의 두번째 자료로서, US 6,167,521은 시스템으로 새 소프트웨어를 다운로딩하는 방법을 기술하고 있는데, 이 기술의 목적은, 구체적으로 각각의 소프트웨어 소유자들이 서로 믿지 않고 있을 때, 이 시스템에 이미 설치되어 있는 소프트웨어를 이 새로 다운로딩된 소프트웨어가 공격하는 것을 방지하려는 것, 또는 반대로, 이미 설치되어 있는 소프트웨어가 새로운 소프트웨어를 공격하는 것을 방지하려는 것이다.

[0006] 더 구체적으로 말하자면, 소프트웨어 인증을 수행하기 위하여, 도 1에 도시된 바와 같이, 다운로딩되었을 수 있는 제 2 부분(11)의 응용 소프트웨어를 이 제 2 부분(11) 안에 위치하는 증명서(12)를 사용하여 인증하기 위하여, 고정된 즉 쓰기-방지된 제 1 부분(10) 내의 메모리 안에 포함된 소프트웨어를 사용하는 것이 알려져 있다.

[0007] 따라서, 디코더 분야에서, 고객이 새로운 응용 소프트웨어를 가진 서비스 제공자를 찾고 있을 때, 서비스 제공자는 이러한 응용 소프트웨어를 검증하기 위한 소프트웨어 및 상기 응용 소프트웨어와 연관될 증명서를 고객에게 제공한다.

[0008] 그러나, 상기 해법에 있어서는, 제 1 소프트웨어의 제공자로 하여금 인증 절차가 실제로 수행되었는지를 체크하기 위한 방법이 존재하지 않는다.

발명의 상세한 설명

[0009] 본 발명의 목적은 상기 제공자로 하여금 이러한 인증이 실제로 수행되었는지를 체크함으로써 자기의 권리가 실제로 고객에 의해 존중되었는지를 체크할 수 있게 하려는 것이다.

[0010] 따라서 본 발명은 단말기에서 다운로딩된 소프트웨어를 인증하는 방법을 제안한다. 상기 방법은 상기 단말기에 내장된 소프트웨어를 사용하여 상기 다운로딩된 소프트웨어를 증명서에 의해 인증하는 단계를 포함한다. 또한 상기 방법은, 상기 다운로딩된 소프트웨의 실행시, 상기 다운로딩된 소프트웨어와 연관된 인증 소프트웨어 모듈을 이용하여 상기 제 1 내장된 소프트웨어를 증명서에 의해 인증하는 단계를 포함하는 것을 특징으로 한다.

[0011] 유리하게, 상기 제 1 내장된 소프트웨어는 인증 라이브러리와 제 1 증명서를 이용하여 상기 다운로딩된 소프트웨어를 인증한다. 여기서 상기 제 1 내장된 소프트웨어와 상기 인증 라이브러리는 쓰기-방지된 메모리의 제 1

부분을 형성하고, 상기 다운로딩된 소프트웨어와 상기 제 1 증명서는 로딩가능한 메모리의 제 2 부분을 형성한다.

[0012] 유리하게, 상기 제 1 부분은 또한 제 2 증명서를 포함하며, 상기 제 2 부분은 또한 검증 소프트웨어를 포함하고, 일단 상기 다운로딩된 소프트웨어가 인증되면, 상기 검증 소프트웨어는 상기 제 1 소프트웨어를 상기 인증 라이브러리와 상기 제 2 증명서를 이용하여 인증한다.

[0013] 유리하게, 이들 두개의 연속적인 인증은 초기화시 수행된다. 제 2 부분은 다운로딩될 수 있다.

[0014] 또한 본 발명은 내장된 소프트웨어에 관한 것으로서, 상기 내장된 소프트웨어는 제 1 소프트웨어와 인증 라이브러리에 의해 형성된 제 1 쓰기-방지된 메모리 부분과, 응용 소프트웨어와 제 1 증명서를 포함하는 제 2 부분을 포함한다. 상기 내장된 소프트웨어에 있어서, 상기 제 1 부분은 또한 제 2 증명서를 포함하고, 상기 제 2 부분은 또한 검증 소프트웨어를 포함한다는 것을 특징으로 한다.

[0015] 이 소프트웨어는 예컨대 디지털 텔레비전 디코더, PC(퍼스널 컴퓨터) 타입의단말기, 또는 임의의 다른 통합 디바이스에서 사용될 수 있다.

실 시 예

[0020] 본 발명의 방법에 있어서, 도 1에서 예시된 종래 기술의 방법에서와 마찬가지로, 쓰기-방지된 메모리의 제 1 부분(10)에 포함되어 있는 제 1 소프트웨어는, 예컨대 초기화 시기에, 제 2 기록가능 부분(11)에 위치하는 응용 소프트웨어인 제 2 소프트웨어를, 상기 제 1 부분에 위치하는 인증 라이브러리와 이 제 2 부분(11)에 위치하는 증명서(12)를 사용하여 인증한다.

[0021] 용어 "증명서(certificate)"가 매우 구체적인 의미를 가지기 때문에(사람 또는 네트워크 엔터티에 대해 신뢰할 수 있는 제 3 자에 의해 발행된 전자적인 식별정보, 각각의 증명서는 증명 권한의 비밀서명키로 서명되어 있다) 그리고 인증 기술에 있어서 너무나 제한적이기 때문에, 본 상세한 설명에서 사용되는 용어 "증명서"는 더 일반적으로, 용어 '서명', 'CRC' 또는 소프트웨어의 권한/무결성을 검증하기 위해 요구되는 임의의 다른 데이터도 역시 포괄하는 의미를 가진다.

[0022] 본 발명의 방법에 있어서, 제 1 부분(10)은 또한 도 2에 예시된 바와 같이 제 2 증명서(13)를 포함한다. 제 2 부분(11)은 또한 검증 소프트웨어를 포함한다. 이 검증 소프트웨어는, 일단 응용 소프트웨어가 인증되면, 인증 라이브러리와 제 2 증명서를 이용하여 제 1 소프트웨어를 인증한다.

[0023] 이러한 방법은 제 1 소프트웨어의 공급자로 하여금 응용 소프트웨어를 사용하는 고객이 공급자의 권리를 실제로 존중하는지를 체크할 수 있게 한다.

[0024] 예시적인 실시예에서, 도 3에 도시된 증명서의 포맷은 아래와 같다:

[0025] • 헤더:

[0026] - CLP (Certificate Location Pattern: 증명서 위치 패턴) : 메모리에서 인증 증명서를 발견하기 위해 증명서의 위치를 제공하는 패턴(예컨대 8바이트),

[0027] - RFU (Reserved for Futere Use: 미사용부분) : 나중의 사용을 위해 유보된 것 (예컨대, 1 바이트),

[0028] - K : 사용될 키 번호 (예컨대, 1 바이트)

[0029] • 서명 (예컨대, 128 바이트): 도 4에 예시된 1024 비트의 메시지를 비밀키를 사용하여 RSA 암호화한 결과.

[0030] 1024-비트 서명은 RSA 암호화를 가능하게 하기 위하여 0에서 일 바이트로 시작하고, 나머지 20은 각각의 암호화 전에 상이한 방식으로 랜덤하게 채워진다.

[0031] 메시지의 시작으로부터 오프셋 H_CODE_OFFSET만큼 떨어진 곳에, 20 바이트에 대해 하시(hash) 코드 SHA1가 있다. 이 H_CODE의 앞에는 CHECK_PATTERN 패턴이 있는데, 이것의 기능은 무결성 체크 동안에 잘못된 해독(공개키 번호 또는 값, 알고리즘, 불일치한 증명서)과 잘못된 H_CODE 사이의 구별을 가능하게 하는 것이다.

산업상 이용 가능성

[0032] 상술한 바와 같이, 본 발명은 내장된 소프트웨어와 이 내장된 소프트웨어를 인증하는 방법 등에 이용가능하며,

상세하게는 디지털 텔레비전 디코더 분야에서 이용가능하다.

도면의 간단한 설명

[0016] 도 1는 종래 기술의 인증 방법을 예시하는 개략도.

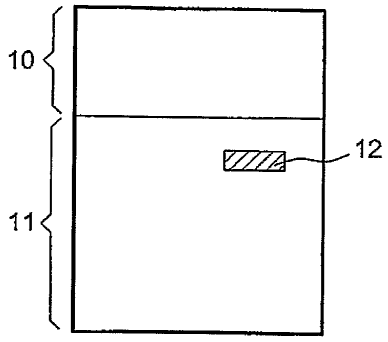
[0017] 도 2는 본 발명의 인증 방법을 예시하는 개략도.

[0018] 도 3은 증명서의 예를 도시하는 개략도.

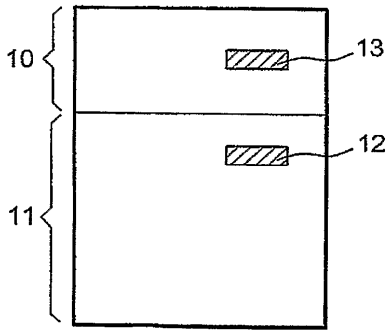
[0019] 도 4는 서명의 예를 도시하는 개략도.

도면

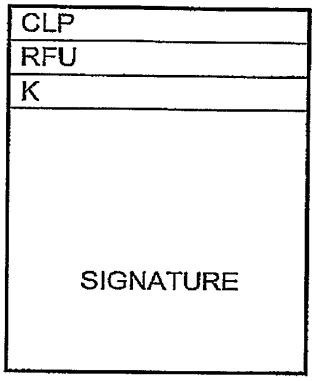
도면1



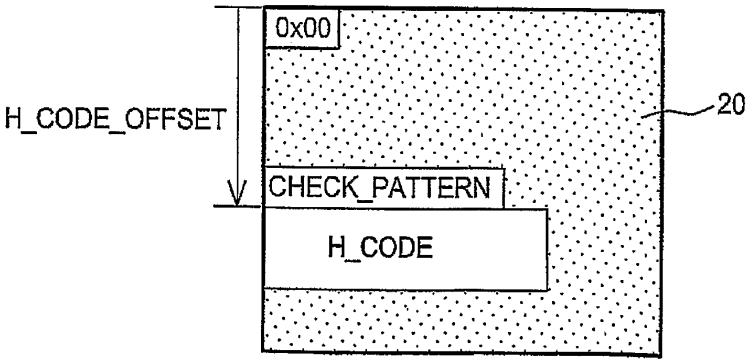
도면2



도면3


CLP
RFU
K
SIGNATURE

도면4


0x00
H_CODE_OFFSET
20
CHECK_PATTERN
H_CODE