(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년10월06일
(11) 등록번호 10-1070978
(24) 등록일자 2011년09월29일

(51) Int. Cl.
H04L 9/32 (2006.01) *G08B 13/14* (2006.01)
H04L 12/22 (2006.01)
(21) 출원번호 10-2005-7002837
(22) 출원일자(국제출원일자) 2003년08월21일
심사청구일자 2008년08월20일
(85) 번역문제출일자 2005년02월18일
(65) 공개번호 10-2005-0058376
(43) 공개일자 2005년06월16일
(86) 국제출원번호 PCT/EP2003/050386
(87) 국제공개번호 WO 2004/019296
국제공개일자 2004년03월04일
(30) 우선권주장
0210430 2002년08월21일 프랑스(FR)
(56) 선행기술조사문헌
US06032257 A1*
WO1998004967 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 잔 다르크 뤼 1-5
(72) 발명자
체브리오, 실베인
프랑스 에프-35000 르네스 스퀘어 드 로이 아터 9
디일, 에릭
프랑스 에프-35340 리프레 라 버자디에르
퍼론, 테디
프랑스 에프-35000 르네스 뤼 데 라 세인트 13
(74) 대리인
주성민, 전경석, 백만기

전체 청구항 수 : 총 18 항 심사관 : 이형일

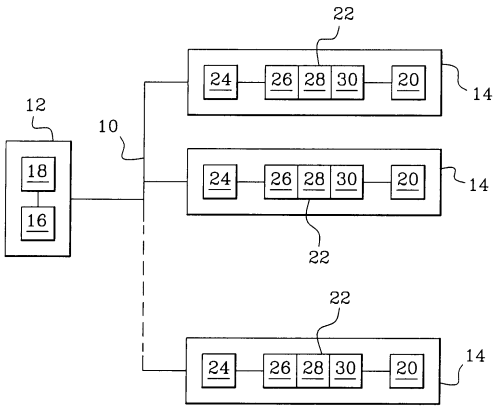
(54) 보안 전자 도난방지 디바이스, 그러한 디바이스를 포함하는도난방지 시스템 및 전자 디바이스 정합 방법

(57) 요 약

본 발명은 적어도 하나의 워치독 디바이스(12)를 포함하는 소정 네트워크(10)에 접속하기 위한 전자 디바이스(14)에 관한 것이다. 전자 디바이스는, 상기 워치독 디바이스의 존재할 때 동작을 인증하는 구성 수단(26)- 여기서, 이들 구성 수단은 전자 디바이스의 저장 수단(20)에 워치독 디바이스 공개 식별자(V)의 기록에 근거함 -, 그러한 워치독 디바이스를 포함하는 임의의 네트워크에 전자 디바이스가 접속될 때 적어도 하나의 워치독 디바이스를 식별하는 수단(28), 및 식별된 워치독 디바이스가 구성된 워치독 디바이스(12)에 대응하지 않거나 상기 네트워크가 워치독 디바이스를 포함하지 않는다면 전자 디바이스(14)를 디스에이블링하기 위한 수단을 포함한다.

본 발명은 또한 도난 방지 시스템 및 디바이스를 결합하는 방법에 관한 것이다.

대 표 도 - 도1



특허청구의 범위

청구항 1

적어도 하나의 워치독(watchdog) 디바이스(12)를 포함하는 소정의 네트워크(10)와 접속하는 전자 디바이스(14)로서,

저장 수단(20)과,

상기 워치독 디바이스(12)가 존재할 때 전자 디바이스의 동작을 인가하는 구성 수단(26)과,

워치독 디바이스를 포함하는 임의의 네트워크에 상기 전자 디바이스가 접속될 때 적어도 하나의 워치독 디바이스를 식별하는 수단(28)과,

식별된 상기 워치독 디바이스가 전자 디바이스용으로 구성된 워치독 디바이스(12)에 대응하지 않거나 또는 상기 네트워크가 워치독 디바이스를 포함하지 않으면, 상기 전자 디바이스(14)를 디스에이블하는 수단(30)

을 포함하고,

상기 구성 수단(26)은, 상기 워치독 디바이스(12)로부터 공개 식별자(V)의 수신시 상기 전자 디바이스용으로 구성된 상기 워치독 디바이스(12)의 공개 식별자(V)를 상기 저장 수단(20)에 기록하도록 구성된, 전자 디바이스.

청구항 2

제1항에 있어서,

상기 식별 수단(28)은 상기 워치독 디바이스의 공개 식별자(V)를 판정하도록 임의의 워치독 디바이스에 문의하는 수단을 포함하는 전자 디바이스.

청구항 3

제1항에 있어서,

상기 식별 수단(28)은, 상기 전자 디바이스용으로 구성된 워치독 디바이스(12)를 인증하는 수단을 포함하는 전자 디바이스.

청구항 4

제3항에 있어서,

상기 인증 수단은 제로 인식 챌린지/응답 프로토콜을 구현하는 전자 디바이스.

청구항 5

제1항에 있어서,

상기 전자 디바이스는, 버진(virgin) 상태(32), 적어도 하나의 워치독 디바이스가 존재할 때 동작하는 구성 상태(34), 블록(blocked) 상태(36)를 포함하는 어셈블리의 요소들중 하나로부터 선택된 상태에 있으며,

상기 구성 상태(34)는 상기 구성 수단(26)의 활성화 후에 획득되며,

상기 블록 상태(36)는 상기 디스에이블 수단(30)의 활성화 후에 획득되는 전자 디바이스.

청구항 6

제5항에 있어서,

상기 전자 디바이스가 구성 상태(34)에 있을 때에만 동작하는 전자 디바이스.

청구항 7

도난방지 시스템으로서,

적어도 하나의 네트워크(10),

상기 네트워크에 접속되고 공개 식별자(V)를 포함하는 적어도 하나의 워치독 디바이스(12), 및

상기 네트워크에 접속되도록 의도되는 적어도 하나의 전자 디바이스(14)를 포함하고,

상기 전자 디바이스(14)는,

저장 수단(20),

상기 워치독 디바이스(12)가 존재할 때 상기 전자 디바이스의 동작을 인가하는 구성 수단(26) - 상기 구성 수단은 상기 워치독 디바이스(12)로부터 공개 식별자(V)의 수신시 상기 전자 디바이스용으로 구성되는 워치독 디바이스의 공개 식별자를 기록하도록 구성됨 -,

상기 전자 디바이스가 워치독 디바이스를 포함하는 임의의 네트워크에 접속되는 경우 적어도 하나의 워치독 디바이스를 식별하는 수단(28), 및

식별된 상기 워치독 디바이스가 전자 디바이스용으로 구성된 워치독 디바이스에 대응하지 않거나 또는 상기 네트워크가 워치독 디바이스를 포함하지 않으면, 상기 전자 디바이스를 디스에이블하는 수단(30)을

포함하는 도난방지 시스템.

청구항 8

제7항에 있어서,

상기 워치독 디바이스(12)는, 상기 공개 식별자(V)가 생성되는, 비밀 식별자(S)를 저장하는 보안 수단(16)을 포함하는 도난방지 시스템.

청구항 9

제7항에 있어서,

상기 네트워크(10)는, 전기 네트워크, 디지털 전송 네트워크, 및 원격통신 네트워크를 포함하는 그룹의 요소들 중 하나로부터 선택되는 도난방지 시스템.

청구항 10

제1 디바이스(12) 및 제2 디바이스(14)를 결합하는 방법으로서,

상기 제2 디바이스(14)는 제1 워치독 디바이스(12)에 접속된 네트워크(10)에 접속되도록 설계되고,

상기 워치독 디바이스(12)가 존재할 때에만 상기 제2 디바이스의 동작을 허가하도록 상기 제2 디바이스(14)를 구성하는 단계(38)를 포함하고,

상기 제2 디바이스(14)를 구성하는 단계(38)는, 상기 워치독 디바이스(12)의 공개 식별자(V)를 상기 제2 디바이스(14)의 저장 수단(20)에 기록하는 단계를 포함하는 방법.

청구항 11

제10항에 있어서,

상기 제2 디바이스(14)는, 버진 상태(32), 적어도 하나의 워치독 디바이스(12)가 존재하는 경우에 동작하는 구성 상태(34), 및 블록 상태(36)로 구성된 어셈블리의 요소들중 하나로부터 선택되는 상태에 있으며,

상기 구성 단계(38)는, 상기 제2 디바이스(14)의 상태를 상기 버진 상태(32)로부터 상기 구성 상태(34)로 변경하는 단계를 포함하는 방법.

청구항 12

제11항에 있어서,

상기 제2 디바이스가 상기 제2 디바이스용으로 구성되지 않은 워치독 디바이스에 접속될 때 상기 제2 디바이스(14)를 디스에이블하는 단계(40)를 포함하고,

상기 디스에이블 단계는, 상기 제2 디바이스(14)의 상태를 상기 구성 상태(34)로부터 상기 블록 상태(36)로 변

경하는 단계를 포함하는 방법.

청구항 13

제11항에 있어서,

상기 제2 디바이스(14)가 네트워크에 접속될 때 상기 네트워크에 접속된 워치독 디바이스를 식별하는 단계를 포함하는 방법.

청구항 14

제13항에 있어서,

상기 식별 단계는, 상기 제2 디바이스(14)와 상기 네트워크와의 접속에 의해 이루어진 이벤트 세트로부터의 트리거 이벤트들중 하나인, 상기 제2 디바이스와 정규 또는 랜덤 식별 프로그램의 기동에 의해 트리거되는 방법.

청구항 15

제13항에 있어서,

상기 식별 단계는 상기 워치독 디바이스를 인증하는 단계를 포함하는 방법.

청구항 16

제15항에 있어서,

상기 인증 단계는 제로 인식 챌린지/응답 프로토콜의 사용에 의해 실현되는 방법.

청구항 17

제16항에 있어서,

상기 워치독 디바이스(12)는, 공개 식별자(V)가 생성되는, 비밀 식별자(S)를 저장하는 보안 수단(16)을 포함하고,

상기 식별 단계는 상기 워치독 디바이스의 공개 식별자(V)를 판정하도록 상기 워치독 디바이스에 문의하는 단계를 포함하며,

상기 인증 단계는, 상기 워치독 디바이스(12)가 상기 제로 인식 챌린지/응답 프로토콜을 이용하여 상기 비밀 식별자(S)를 알고 있음을 상기 제2 디바이스(14)에 증명하는 일련의 단계를 포함하는 방법.

청구항 18

제13항에 있어서,

상기 식별 단계에서, 상기 네트워크가 상기 제2 디바이스(14)용으로 구성된 워치독 디바이스(12)를 포함하고, 상기 제2 디바이스가 블록 상태에 있다고 결정되면, 상기 제2 디바이스(14)의 상태를 상기 블록 상태(36)로부터 상기 구성 상태(34)로 변경하는 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 적어도 하나의 워치독(watchdog) 디바이스를 포함하는 네트워크에 접속하는 것을 의도로하는 전자 디바이스에 관한 것이다. 본 발명은 또한 워치독 디바이스가 접속되는 네트워크를 포함하는 도난방지 시스템에 관한 것이다. 마지막으로, 본 발명은 워치독 디바이스라 칭해지는 제1 디바이스와 제2 디바이스를 결합하는 방법에 관한 것이다.

배 경 기 술

[0002] 워치독 디바이스를 포함하는 네트워크에 접속하는 것을 의도로 하는 그러한 전자 디바이스는 종래에 이미 공개되어 있다. 이들은 도난의 경우에 전자 디바이스의 동작을 방지하도록 구성되어 있다.

[0003] 예를 들면, WO 98/04967호에는, 방지 시스템을 특징으로 하는 전자 디바이스는 자신의 동작을 인증하는 워치독 디바이스에 접속되는 경우에만 동작할 수 있다. 워치독 디바이스는, 관련 데이터베이스에서, 고유한 식별 코드에 의해 식별되는 전자 디바이스의 리스트를 관리하고 그 리스트에 기록된 디바이스용의 동작 인증 수단을 포함한다. 일반적으로, 워치독 디바이스는 고정, 숨김, 또는 심지어 원거리에 있어 도둑이 워치독에 접속된 전자 디바이스만을 훔칠 수 있다. 따라서, 도둑은 훔친 장치를 동작하게 하는 워치독 디바이스를 소유할 수 없어 이들 디바이스를 사용하거나 되팔수 없게 된다.

[0004] 그러한 시스템의 불리한 점은, 워치독 디바이스가 전자 디바이스가 동작하게하는 인증을 제어한다는 것이다. 더우기, 워치독 디바이스는 리스트 상의 모든 다른 디바이스의 동작에 대해 인증을 제어한다. 이러한 제어 시스템은 많은 전자 디바이스가 워치독 디바이스에 접속되는 곳에서는 성가실 수 있고 어려울 수 있다.

[0005] 발명의 개요

[0006] 본 발명은, 이러한 단점을 극복하고자 전자 디바이스들의 리스트 관리를 요구하지 않고 전자 디바이스에 관련된 워치독 디바이스에 의해 도난으로부터 보호받을 수 있는 전자 디바이스를 제공한다.

[0007] 이를 위해, 본 발명은

[0008] 적어도 하나의 워치독 디바이스를 포함하는 네트워크에 접속되는 전자 디바이스를 제공한다. 이 전자 디바이스는, 저장 수단과, 워치독 디바이스가 존재할 때 전자 디바이스의 동작을 인가하는 구성 수단과, 워치독 디바이스를 포함하는 임의의 네트워크에 전자 디바이스가 접속될 때 적어도 하나의 워치독 디바이스를 식별하는 수단과, 식별된 워치독 디바이스가 전자 디바이스용으로 구성된 워치독 디바이스에 대응하지 않으면 또는 네트워크가 워치독 디바이스를 포함하지 않으면, 전자 디바이스를 디스에이블하는 수단을 포함한다. 전자 디바이스의 구성 수단은 전자 디바이스용으로 구성된 워치독 디바이스의 공개 식별자를 전자 디바이스의 저장 수단에 기록하는데 적절하다.

[0009] 또한, 본 발명에 따른 전자 디바이스는, 다음에 따르는 특성들중 하나 이상을 특징으로 한다.

[0010] - 식별 수단은 워치독 디바이스의 공개 식별자를 판정하도록 임의의 워치독 디바이스에 문의하는 수단을 포함한다.

[0011] - 식별 수단은 전자 디바이스용으로 구성된 워치독 디바이스를 인증하는 수단을 포함한다.

[0012] - 인증 수단은 제로 인식 챌린지/응답 프로토콜을 구현한다.

[0013] - 전자 디바이스는, 버진 상태, 적어도 하나의 워치독 디바이스가 존재할 때 동작하는 구성 상태, 및 블록 상태를 포함하는 어셈블리의 요소들중 하나로부터 선택된 상태에 있으며, 구성 상태는 구성 수단의 활성화 후에 획득되며, 블록 상태는 디스에이블 수단의 활성화 후에 획득된다.

[0014] - 전자 디바이스가 구성 상태(34)에 있을 때에만 동작한다.

[0015] 또한, 본 발명은 적어도 하나의 네트워크, 및 네트워크에 접속되고 공개 식별자를 포함하는 적어도 하나의 워치독 디바이스를 포함하는 도난방지 시스템에 관한 것으로서, 상술한 바와 같은 적어도 하나의 전자 디바이스를 포함한다.

[0016] 게다가, 본 발명에 따른 도난방지 시스템은 다음에 같은 특성들중 하나 이상을 특징으로 할 수 있다.

[0017] - 워치독 디바이스는, 공개 식별자가 생성되는, 비밀 식별자를 저장하는 보안 수단을 포함한다.

[0018] - 네트워크는, 전기 네트워크, 디지털 전송 네트워크, 및 원격통신 네트워크를 포함하는 상기 그룹의 요소들중 하나로부터 선택된다.

[0019] 마지막으로, 본 발명은 제1 디바이스 및 제2 디바이스를 결합하는 방법을 제공하며, 여기서 제2 디바이스는 제1 워치독 디바이스에 접속된 네트워크에 접속되도록 설계된다. 이 방법은, 제2 워치독 디바이스를 구성하여 워치독 디바이스가 존재할 때에만 디바이스의 동작을 허가하는 단계를 포함한다. 제2 디바이스를 구성하는 단계는 워치독 디바이스의 공개 식별자를 저장 수단에 기록하는 단계를 포함한다.

[0020] 게다가, 본 발명에 따른 결합 방법은 다음과 같은 특성들중 하나 이상을 특징으로 한다.

[0021] - 제2 디바이스는, 버진 상태, 적어도 하나의 워치독 디바이스가 존재하는 경우에 동작하는 구성 상태, 및 블록 상태로 구성된 어셈블리의 요소들중 하나로부터 선택되는 상태에 있으며, 구성 단계는 제2 디바이스의 상태를

버진 상태로부터 구성 상태로 변경하는 단계를 포함한다.

[0022] - 이 방법은, 제2 디바이스가 디바이스용으로 구성되지 않은 워치독 디바이스에 접속될 때 제2 디바이스를 디스에이블하는 단계를 포함하고, 디스에이블 단계는, 제2 디바이스의 상태를 구성 상태로부터 블록 상태로 변경하는 단계를 포함한다.

[0023] - 이 방법은, 제2 디바이스가 네트워크에 접속될 때 네트워크에 접속된 워치독 디바이스를 식별하는 단계를 포함한다.

[0024] - 식별 단계는, 제2 디바이스와 네트워크와의 접속에 의해 이루어진 이벤트 세트로부터의 트리거 이벤트들중 하나인, 제2 디바이스와 정규 또는 랜덤 식별 프로그램의 기동에 의해 트리거된다.

[0025] - 식별 단계는 워치독 디바이스를 인증하는 단계를 포함한다.

[0026] - 인증 단계는 제로 인식 챌린지/응답 프로토콜의 사용에 의해 실현된다.

[0027] - 워치독 디바이스는, 공개 식별자가 생성되는, 비밀 식별자를 저장하는 보안 수단을 포함하고, 식별 단계는 워치독 디바이스의 공개 식별자를 판정하도록 워치독 디바이스에 문의하는 단계를 포함하며, 인증 단계는, 워치독 디바이스가 제로 인식 챌린지/응답 프로토콜을 이용하여 비밀 식별자를 알고 있음을 전자 디바이스에 증명하는 일련의 단계를 포함한다.

[0028] - 식별 단계에서, 네트워크가 제2 디바이스용으로 구성된 워치독 디바이스를 포함하고 있는 반면 제2 디바이스가 블록 상태에 있다고 결정되면, 제2 디바이스의 상태를 블록 상태로부터 구성 상태로 변경한다.

발명의 상세한 설명

[0033] 도 1은 전자 전력 공급 네트워크, 디지털 전송 네트워크 또는 심지어 통신 네트워크 같은 로컬 네트워크(10)를 도시한다. 이것은 유선 또는 무선 네트워크일 수 있다. 워치독 디바이스(12) 및 전자 디바이스(14)는 이 로컬 네트워크(10)에 접속된다.

[0034] 워치독 디바이스(12)는 숨겨지거나 지지대에 고정될수 있어 훔치기가 어렵다. 이것은 보안 프로세서 같은 계산 수단(16) 및 네트워크 인터페이스(18)을 포함한다. 워치독 디바이스(12)는 (도면에는 도시되지 않은) 매우 큰 수의 비밀번호(S) 및 번호(V) - 이후 워치독 디바이스(12)의 공개 식별자로 칭함 - 를 메모리에 저장한다. S 및 V는 다음의 수학식을 입증한다.

[0035] $$S=\sqrt{V}\bmod n$$

[0036] 여기서, n은, 예를 들면, 비밀을 간직한 두개의 매우 큰 소수를 곱함으로써 비밀 인수분해한 정수이다.

[0037] $S=\sqrt{V}\bmod n$ 이면, $S^2=V \bmod n$을 증명하는 것은 쉽다.

[0038] 워치독 디바이스(12)는 또한 공개키(K)를 사용하여 제어 인증에 의해 계산된 공개 식별자(V)의 서명(SigV)를 저장한다.

[0039] V 및 n은 공개값, 즉, 워치독 디바이스(12)가 알고 있는 값이지만 전자 디바이스(14)에 또한 통신될 수 있다. 값(n)이 구성시에 전자 디바이스(14)에 저장되는 반면, 값(V)는 구성동안 전자 디바이스(14)에 전송된다.

[0040] 전자 디바이스(14)는, 예를 들면, 가전 제품, 오디오비주얼 디바이스, 컴퓨터 또는 도난에 대해 보호될 필요가 있고 네트워크(10)에 접속되기에 적당한 임의의 다른 디바이스이다. 각각의 전자 디바이스(14)는 비휘발성 메모리 같은 저장 수단(20), 프로세서와 같은 계산 수단(22) 및 워치독 디바이스(12)의 네트워크 인터페이스(18)와 유사한 네트워크 인터페이스(24)를 포함한다.

[0041] 계산 수단(22)은 각각의 전자 디바이스(14)를 구성하기 위한 수단(26), 워치독 디바이스를 식별하기 위한 수단(28) 및 각각의 전자 디바이스(14)를 디스에이블하기 위한 수단(30)을 포함한다. 이들 수단(26, 28 및 30)은 각 전자 디바이스(4)의 프로세서(22)에 전통적인 방법으로 프로그래밍된 소프트웨어 수단이 바람직하다.

[0042] 각 전자 디바이스(14)는 번호(n)과 서명(SigV)를 계산한 제어 인증에 의해 발행된 공개키(K)를 자신의 메모리(20)에 저장한다. 이 키는 서명(SigV)가 V의 값에 따라 증명되도록 한다.

[0043] 실시예에서, 본 발명은 각 디바이스(14)의 사용을 로컬 네트워크(10)로 국한하는 것, 즉 각 전자 디바이스(14)는 워치독 디바이스(12)에 접속되는 경우에만 동작할 수 있도록 하는 것을 목표로 한다. 이 경우에, 각 디바이스(14)의 메모리(20)는, n 및 K에 부가하여 워치독 디바이스(12)의 공개 식별자(V)만을 저장한다.

[0044] 또 다른 실시예에서, 각 전자 디바이스(14)의 사용은 각각 워치독 디바이스를 구비한 몇개의 로컬 네트워크로 제한될 수 있다. 따라서, 전자 디바이스(14)는 몇 개의 워치독 디바이스와 관련될 수 있다. 이 경우에, 각 디바이스(14)의 메모리(20)는 관련된 각각의 워치독 디바이스의 공개 식별자(V)를 저장한다.

[0045] 전자 디바이스(14)는 세개의 기본 상태, 즉, 도 2에 도시된 버진(virgin) 상태(32), 구성 상태(34) 및 블록(blocked) 상태(36)에 있을 수 있다.

[0046] 버진 상태(32)는 전자 디바이스(14)의 메모리(20)가 워치독 디바이스의 공개 식별자를 저장하지 않고 있는 상태에 대응한다.

[0047] 구성 상태(34)는 전자 디바이스(14)가 자신의 메모리(20)에 워치독 디바이스(12)의 공개 식별자(V)를 저장하고 있는 상태에 대응한다. 전자 디바이스(14)는 워치독 디바이스(12)가 존재하는 경우, 즉, 디바이스(14)가 워치독 디바이스(12)가 또한 접속되어 있는 네트워크에 접속되는 경우에만 동작한다.

[0048] 또 다른 실시예에서, 구성 상태는, 각 디바이스(14)의 메모리(20)가 몇개의 소정 워치독 디바이스의 공개 식별자(V)를 저장하는 상태에 대응한다. 전자 디바이스(14)는 워치독 디바이스들 중 하나에 접속되면 동작할 수 있되, 상기 전자 디바이스는 접속된 워치독 디바이스를 위한 공개 식별자(V)를 포함한다.

[0049] 블록 상태(36)는, 전자 디바이스가 구성되었음에도 불구하고, 워치독 디바이스용으로 전자 디바이스가 구성되지 않은, 즉, 워치독 디바이스용으로 전자 디바이스가 공개 식별자(V)를 갖고 있지 않는 워치독 디바이스에 전자 디바이스가 접속되거나 또는 그 밖에 임의의 워치독 디바이스에 접속되지 않음에 따라 동작할 수 없는 상태에 대응한다.

[0050] 본 명세서에서, 전자 디바이스(14)의 상태는 메모리(20)에 저장된 변수(e)로 정의되며, 이는 전자 디바이스(14)가 버진 상태(32)에 있으면 값 0이 할당되고, 구성 상태(34)에 있는 경우에는 값 1이 할당되며, 블록 상태(36)에 있으면 값 2가 할당된다.

[0051] 워치독 디바이스(12)의 공개 식별자(V)가 전자 디바이스(14)의 메모리(20)에 기록되는 동안 구성 단계(38)에 의해 버진 상태(32)로부터 구성 단계(34)로 진행하여 전자 디바이스(14)가 워치독 디바이스(12)를 식별하고 그 존재에서 동작하는 것이 가능하다.

[0052] 본 실시예에서, 구성 단계(38)는, 예를 들면, 네트워크(10) 전자 디바이스(14)를 접속하는 동안, 또는 처음에 전자 디바이스(14)를 시동할 때 자동적이다.

[0053] 변형예로서, 구성 단계(38)는, 예를 들면, 비밀 코드의 입력, 물리적 또는 전자키의 사용, 또는 디지털 또는 음성 지문의 인식과 같은 생체 인식 수단에 의한 사용자 인증을 통해 사용자에 의해 수동으로 트리거링될 수 있다.

[0054] 구성 단계(34)는, 워치독 디바이스(12)용으로 전자 디바이스(14)가 구성된 워치독 디바이스(12)가 아닌 워치독 디바이스, 즉, 워치독 디바이스의 공개 식별자(V)가 전자 디바이스(14)의 메모리(20)에 저장되지 않은 워치독 디바이스에 전자 디바이스(14)가 접속되거나, 또는 임의의 워치독 디바이스에 접속되지 않을 때 트리거되는 자동 디스에이블링 단계(40)를 통해 블록 상태로 진행한다.

[0055] 블록 상태(36)는 자동 언블록킹 단계(42)를 통해 구성 상태(34)로 진행한다. 이 단계는, 블록된 전자 디바이스(14)가 워치독 디바이스(12)용의 공개 식별자(V)를 포함하는 워치독 디바이스(12)에 다시 접속되는 경우에 트리거된다. 다음에, 전자 디바이스(14)는, 도 3을 참조하여 하기에 설명되는 제로-인식 챌린지/응답 타입의 테스트 구현후에, 구성 상태(34)에서 발견된다.

[0056] 변형예로서, 언블록킹 단계(42)는, 예를 들면, 비밀번호 입력동안, 물리적 또는 전자키의 사용동안 또는 생체인식 수단에 의한 사용자의 인증동안 수동으로 트리거될 수 있다.

[0057] 마지막으로, 구성 상태(34)는, 인증된 사용자가 전자 디바이스(14)의 메모리(20)에 저장된 워치독 디바이스 공개 식별자 모드를 소거하는 동안 리셋 단계(44)를 통해 버진 상태(32)로 진행한다.

[0058] 전자 디바이스(14)를 임의의 타입의 워치독 디바이스(46)에 결합하는 방법은 도 3의 기능도에서 설명된다.

[0059] 이 결합 방법은, 네트워크 또는 주기 클럭 동기 펄스에 접속하는 전자 디바이스(14)의 시동과 같은 트리거링 이벤트에 의해 형성된다. 임의의 경우에, 전자 디바이스는 워치독 디바이스(46)가 또한 접속되는 네트워크에 접속된다는 것을 가정한다.

[0060] 다음 단계(50) 동안, 전자 디바이스(14)는 자신을 식별하기 위해 워치독 디바이스(46)를 요청하는 커맨드를 네트워크 상에 전송한다.

[0061] 다음에, 단계(52) 동안, 워치독 디바이스(46)는 자신의 공개 식별자(V) 및 서명(SigV)을 전자 디바이스에 전송한다.

[0062] 단계(52) 이후에, 전자 디바이스(14)는 테스트(54)를 수행한다. 이 테스트는 워치독 디바이스(46)에 의해 전송된 공개 식별자(V)와 전자 디바이스(14)에 저장된 공개키(K)를 사용하여 서명(SigV)을 체크하는 것을 포함한다.

[0063] 테스트(54) 결과가 네거티브이면, 즉, 서명(SigV)이 전송된 식별자(V)에 대응하지 않으면, 상기 방법은 초기화 단계(48)로 연기된다.

[0064] 테스트(54)의 결과가 포지티브라면, 테스트(56)는 전자 디바이스(14)의 메모리(20)에 저장된 변수(e)에 수행된다.

[0065] 변수(e)가 값 0이면, 즉, 전자 디바이스(14)가 버진 상태(32)에 있다면, 단계(58)는 디바이스(14)가 자신의 메모리에 공개 식별자(V)를 저장하는 단계에 도달한다. 단계(58)에 이어 전술한 구성 단계(38)가 이어진다. 이 단계동안, 변수(e)는 값 1을 취하고 전자 디바이스(14)는 구성 상태(34)에 있게 된다. 다음에 과정은 초기화 단계(48)로 연기된다.

[0066] 단계(56)에서, 변수(e)가 1 또는 2라면, 테스트 단계(60)는 전자 디바이스(14)가 워치독 디바이스(46)에 의해 전송된 공개 식별자(V)를 메모리(20)에 저장된 공개 식별자(V_0)에 비교한다.

[0067] 테스트(60)의 결과가 네거티브이면, 전자 디바이스(14)는 테스트(61)를 변수(e)에 수행한다. e가 2이고 디바이스가 이미 금지되어 있으면, 초기화 단계(48)로 진행한다. 그렇지 않다면, e를 1로 해서, 전술한 디스에이블링 단계(40)로 진행한다. 변수(e)는 이 단계에서 값 2를 취하는데, 즉, 전자 디바이스(14)는 블록 상태(36)에 있게된다. 다음에 과정은 초기화 단계(48)로 연기된다.

[0068] 테스트(60)의 결과가 포지티브라면, 단계(62)는 우선적으로 난수를 생성함으로써 워치독(46)이 제로-인식 챌린지/응답 프로토콜을 트리거하는 단계에 도달한다. 이 과정은 단계(62 내지 86)로 이어진다.

[0069] 이 단계(62)에 이어, 단계(64)는 워치독 디바이스(46)가 두개의 번호 r^2 및 r.S에서 무작위적으로 취해진 번호인 보안 번호(G)를 선택하며, 여기에서, S는 워치독 디바이스(46)의 비밀 번호이다. 그것은 자신의 선택을 알리지 않고 보안 번호(G)를 전자 디바이스(14)에 전송한다.

[0070] 다음 단계(66) 동안, 전자 디바이스(14)는 값 A 또는 B를 챌린지 C에 무작위적으로 할당한다. 다음에 이 챌린지 C를 워치독 디바이스(46)에 전송한다.

[0071] 다음 단계(66)에서, 워치독 디바이스(46)는 챌린지 C 상에 테스트(68)를 수행한다.

[0072] 테스트(68)가 챌린지 C가 A라는 것을 보여주면, 단계(70)로 진행하여 워지독 디바이스(46)가 값 r^2을 A에 할당하고 A를 전자 디바이스(14)로 다시 전송한다.

[0073] 단계(70)에 이어서, 전자 디바이스(14)는 보안 번호(G)의 값을 체크하기 위해 테스트(72)를 수행한다.

[0074] 이어지는 단계(64)에서, 보안 번호(G)는 r^2 또는 r.S라는 것이 공지된다. $A=r^2$이기 때문에 두가지 확률: G=A (여기서, $G=r^2$), 또는 $r^2.S^2=A.V \bmod n$(여기서, G=rS)이 존재한다. 사실상, 후자의 경우에, 공개 식별자(V)가 워치독 디바이스(46)에 대응하면, 즉, $S^2=V \bmod n$이면, $r^2.S^2=A.V \bmod n$이 된다. 따라서, V가 워치독 디바이스(46)의 식별자이면, G=A 또는 $G^2=A.V \bmod n$이 된다.

[0075] 테스트(72)가 포지티브이면, 즉, G=A 또는 $G^2=A.V \bmod n$이면, 단계(74)에서 값 1이 e에 주어지고, 즉, 전자 디바이스는 구성 상태(34)로 설정된다.

[0076] 단계(74)에 이어, 트리거링 이벤트 모니터링 단계(76)로 진행한다. 이 단계(76)에서, 소정 트리거링 이벤트의

세트에 속하는 트리거링 이벤트가 검출되자마자, 단계(62)로 진행한다. 이들 트리거링 이벤트는, 예를 들면, 단계(48)의 트리거링 이벤트와 동일하다.

[0077] 테스트(72)가 네거티브이면, 즉, $G \neq A$ 또는 $G^2 \neq A.V \bmod n$ 이면, 단계(78)로 진행하여 값 2가 e에 주어지고, 즉, 전자 디바이스가 블록 상태(36)로 설정된다.

[0078] 단계(78)에 이어, 트리거링 이벤트 모니터링 단계(76)가 이어진다.

[0079] 테스트(68)가 챌린지 C가 B라는 것을 보여주면, 단계(80)로 진행하여 워치독 디바이스(46)는 값 r.S을 B에 할당하고, B를 전자 디바이스(14)로 전송한다.

[0080] 이 단계(80)에 이어, 전자 디바이스(14)는 보안 번호(G)의 값을 체크하기 위해 테스트(82)를 수행한다.

[0081] 단계(64)에 따라, 보안 번호(G)가 r^2 또는 r.S라는 것이 공지된다. B=r.S이기 때문에, 두가지 확률: G=B(여기서 G=rS)이거나 또는 $r^2.S^2=G.V \bmod n$(여기서, $G=r^2$)이 존재한다. 사실상, 후자의 경우에, 공개 식별자(V)가 워치독 디바이스(46)에 대응하면, 즉, $S^2=V \bmod n$이면, $r^2.S^2=G.V \bmod n$이 된다. 따라서, V가 사실상 워치독 디바이스(46)의 식별자라면, G=B 또는 $B^2=G.V \bmod n$이 된다.

[0082] 테스트(82)가 포지티브라면, 즉, G=B 또는 $B^2=G.V \bmod n$이라면, 단계(84)로 진행하여 값 1이 e에 주어지고, 즉, 전자 디바이스가 구성 상태(34)로 설정된다.

[0083] 이 단계(84)에 이어, 트리거링 이벤트 모니터링 단계(76)로 진행한다.

[0084] 테스트(82)가 네거티브이면, 즉, $G \neq B$ 또는 $B^2 \neq A.V \bmod n$ 이면, 단계(86)로 진행하여 값 2가 e에 주어지고, 즉, 전자 디바이스가 블록 상태(36)로 설정된다.

[0085] 단계(78)에 이어, 트리거링 이벤트 모니터링 단계(76)가 이어진다.

[0086] 본 발명의 이점들 중, 인증된 디바이스의 리스트를 관리하기 위해 워치독을 요구하지 않으면서, 구성된 워치독 디바이스가 존재하는 경우에만 각각의 전자 디바이스를 동작하도록 할 수 있다는 것을 유의해야 한다.

[0087] 또한, 본 발명은 임의의 중앙 인증의 개입을 요구하지 않으면서 자동 도난 방지 테스트를 할 수 있다는 것을 유의해야 한다.

[0088] 마지막으로, 인증을 위해 제로-인식 챌린지/응답 프로토콜을 사용하기 때문에 비밀 정보가 전자 디바이스(14)에 저장되지 않는다.

도면의 간단한 설명

[0029] 본 발명은 단지 정보를 제공하고, 첨부 도면을 참조로 하는 후술의 상세한 설명으로부터 더 잘 이해될 것이다.

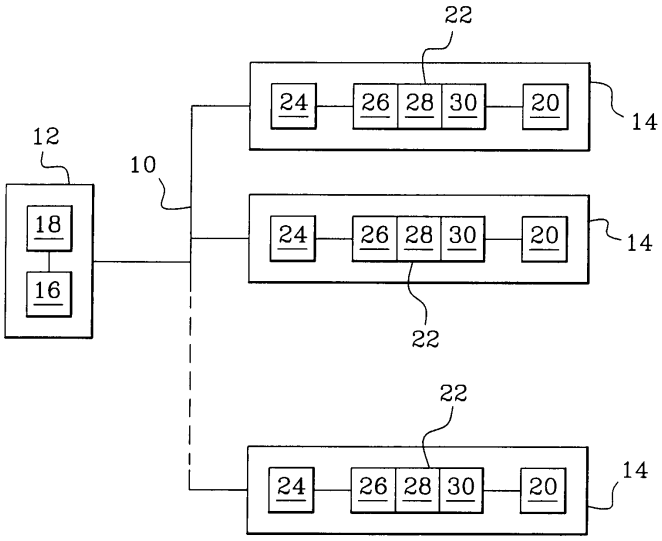
[0030] 도 1은 본 발명에 따른 도난방지 시스템의 개략도이다.

[0031] 도 2는 본 발명에 따른 전자 디바이스에 대한 상태 변경 방법의 기능도이다.

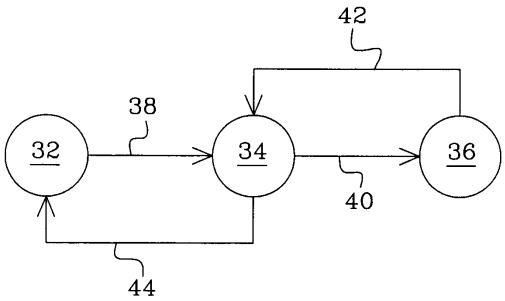
[0032] 도 3은 본 발명에 따라 전자 디바이스를 워치독 디바이스에 결합하기 위한 방법의 기능도이다.

도면

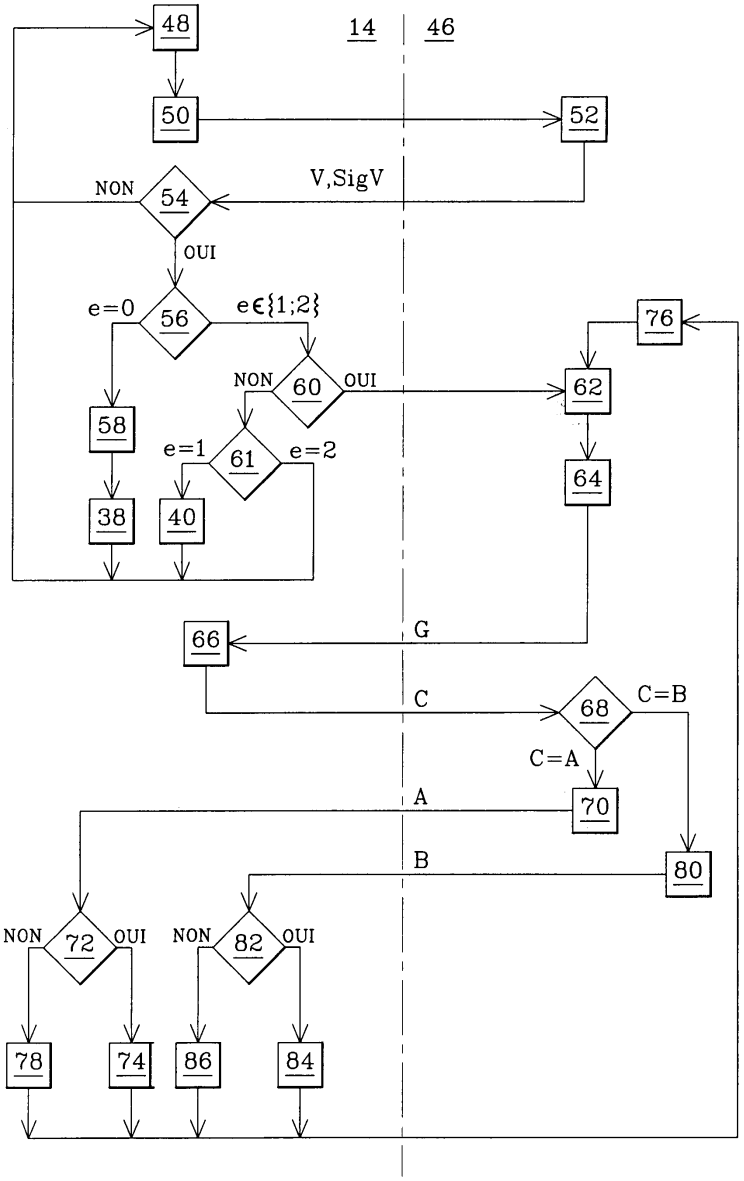
도면1


22
24
26
28
30
20
14
12
10
18
16
14
22
22
24
26
28
30
20
14

도면2


42
38
32
34
36
40
44

도면3


48
14
46
50
52
NON
54
V,SigV
OUI
e=0
56
e∈{1;2}
76
NON
60
OUI
62
58
e=1
61
e=2
64
38
40
66
G
C
68
C=B
C=A
70
A
B
80
NON
72
OUI
NON
82
OUI
78
74
86
84