



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0054792
(43) 공개일자 2008년06월19일

(51) Int. Cl.

G06F 21/00 (2006.01) G06F 15/00 (2006.01)
G06F 17/00 (2006.01)

(21) 출원번호 10-2006-0127362

(22) 출원일자 2006년12월13일

심사청구일자 없음

(71) 출원인

주식회사 케이티

경기 성남시 분당구 정자동 206

(72) 발명자

박세철

인천 부평구 삼산동 신성아파트 307-102

옥창석

경기 성남시 분당구 구미동 무지개마을건영아파트
1001-1301

김용

경기 성남시 분당구 서현동 276-1 시그마파크 72
2호

(74) 대리인

특허법인 신성

전체 청구항 수 : 총 15 항

(54) 하드웨어 보안 모듈 다중화 장치 및 그 방법

(57) 요약

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은 하드웨어 보안 모듈(HSM) 다중화 장치 및 그 방법과, 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은 전자 금융거래 및 고객 인증 등에 광범위하게 사용되는 하드웨어 보안 모듈(HSM)을 호스트나 HSM의 장애 발생시에도 정상 운용이 가능하도록 효율적으로 다중화(/이중화)한, 하드웨어 보안 모듈 다중화 장치 및 그 방법과, 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있음.

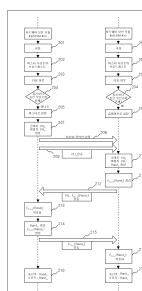
3. 발명의 해결방법의 요지

본 발명은, 하드웨어 보안 모듈(HSM) 다중화 방법에 있어서, 상기 HSM의 다중화시, 마스터 우선순위를 선정하는 단계; 각 HSM 간에 자신의 우선순위를 브로드캐스팅하여, 마스터 HSM을 결정하는 마스터 HSM 결정 단계; 마스터 HSM과 적어도 하나의 슬레이브 HSM 간에, 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 보안채널을 각각 형성하는 초기 설정 단계; 및 상기 형성된 각각의 보안채널을 통해, 상기 마스터 HSM이 신규 생성 및/또는 변경 정보를 모든 슬레이브 HSM에 복제하는 운용 단계를 포함한다.

4. 발명의 중요한 용도

본 발명은 전자금융거래 또는 가입자 인증 시스템 등에 이용됨.

대표도 - 도2



특허청구의 범위

청구항 1

하드웨어 보안 모듈(HSM) 다중화 장치에 있어서,

기 설정된 우선순위에 따라 마스터로 지정되어, 자신의 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 적어도 하나의 슬레이브 HSM과 보안채널을 각각 형성하고, 신규 생성 및/또는 변경 정보를 각각의 보안채널을 통해 상기 적어도 하나의 HSM에 복제하기 위한 마스터 HSM; 및

기 설정된 우선순위에 따라 슬레이브로 지정되어, 자신의 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 상기 마스터 HSM과 상기 보안채널을 각각 형성하고, 각각의 보안채널을 통해 전송되는 신규 생성 및/또는 변경 정보를 저장(복제)하고 있는 상기 적어도 하나의 슬레이브 HSM

을 포함하는 하드웨어 보안 모듈 다중화 장치.

청구항 2

제 1 항에 있어서,

상기 마스터 HSM의 장애 발생시,

상기 기 설정된 우선순위에 따라, 상기 적어도 하나의 슬레이브 HSM 중 차순위 HSM이 마스터로 자동 절체되는 것을 특징으로 하는 하드웨어 보안 모듈 다중화 장치.

청구항 3

제 1 항에 있어서,

상기 각 HSM은,

상기 복제 과정에서 오류 발생시, 복제하고자 하는 신규 생성 및/또는 변경 정보를 삭제하고 원상 복구시키는 것을 특징으로 하는 하드웨어 보안 모듈 다중화 장치.

청구항 4

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 각 HSM은,

서로 다른 마스터 우선순위를 가지며, 전원 인가시 자신의 마스터 우선순위를 네트워크상으로 브로드캐스트하여, 자신보다 우선순위가 높은 HSM으로부터 메시지가 수신되지 않는다면 자신을 마스터로 지정하는 것을 특징으로 하는 하드웨어 보안 모듈 다중화 장치.

청구항 5

제 4 항에 있어서,

상기 각 HSM은,

호스트로부터의 연결을 처리하기 위한 접속 관리자가 존재하고, 내부에 관리되고 있는 가상 슬롯을 통해 실제 키 생성, 암호/복호화를 처리하는 토큰으로 접속되는 것을 특징으로 하는 하드웨어 보안 모듈 다중화 장치.

청구항 6

하드웨어 보안 모듈(HSM) 다중화 방법에 있어서,

상기 HSM의 다중화시, 마스터 우선순위를 선정하는 단계;

각 HSM 간에 자신의 우선순위를 브로드캐스팅하여, 마스터 HSM을 결정하는 마스터 HSM 결정 단계;

마스터 HSM과 적어도 하나의 슬레이브 HSM 간에, 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 보안채널을 각각 형성하는 초기 설정 단계; 및

상기 형성된 각각의 보안채널을 통해, 상기 마스터 HSM이 신규 생성 및/또는 변경 정보를 모든 슬레이브 HSM에 복제하는 운용 단계

를 포함하는 하드웨어 보안 모듈 다중화 방법.

청구항 7

제 1 항에 있어서,

상기 마스터 HSM의 장애 발생시, 상기 HSM 결정 단계를 통해 상기 적어도 하나의 슬레이브 HSM 중 차순위 HSM이 마스터로 결정되는 단계

를 더 포함하는 하드웨어 보안 모듈 다중화 방법.

청구항 8

제 6 항에 있어서,

상기 운용 단계에서,

상기 신규 생성 및/또는 변경 정보의 복제 오류 발생시, 복제하고자 하는 신규 생성 및/또는 변경 정보를 삭제하고 원상 복구시키는 단계

를 더 포함하는 하드웨어 보안 모듈 다중화 방법.

청구항 9

제 6 항 내지 제 8 항 중 어느 한 항에 있어서,

상기 초기 설정 단계에서,

상기 마스터 HSM과 상기 적어도 하나의 슬레이브 HSM 간에 데이터 전송은 난수로 암호화되어 처리하는 것을 특징으로 하는 하드웨어 보안 모듈 다중화 방법.

청구항 10

제 9 항에 있어서,

상기 초기 설정 단계는,

상기 마스터 HSM이 자신의 공개키와 비밀키 쌍(PU_m , PR_m)을 생성하는 단계;

상기 마스터 HSM이 자신의 공개키(PU_m)를 적어도 하나의 슬레이브 HSM으로 전송하는 단계;

상기 적어도 하나의 슬레이브 HSM이 자신의 공개키와 비밀키 쌍(PU_n , PR_n)을 생성하고, 제1 난수($Rand_n$)를 생성하여 이를 상기 마스터 HSM의 공개키(PU_m)로 암호화하여($E_{PU_m}(Rand_n)$), 자신의 공개키(PU_n)와 함께 응답 메시지를 통해 상기 마스터 HSM으로 전달하는 단계;

상기 마스터 HSM이 상기 $E_{PU_m}(Rand_n)$ 을 자신의 비밀키(PR_m)로 복호화하여 상기 제1 난수($Rand_n$)를 상기 적어도 하나의 슬레이브 HSM에 대한 송신 세션키, 제2 난수($Rand_m$)를 수신 세션키로 설정하는 단계;

상기 마스터 HSM이 상기 제2 난수($Rand_m$)를 상기 적어도 하나의 슬레이브 HSM의 공개키(PU_n)로 암호화하여($E_{PU_n}(Rand_m)$) 응답 메시지로써 상기 적어도 하나의 슬레이브 HSM으로 전달하는 단계; 및

상기 적어도 하나의 슬레이브 HSM이 상기 $E_{PU_n}(Rand_m)$ 을 자신의 비밀키(PR_n)로 복호화하여 상기 제2 난수($Rand_m$)를 상기 마스터 HSM에 대한 수신 세션키, 상기 제1 난수($Rand_n$)를 송신 세션키로 설정하는 단계

를 포함하는 하드웨어 보안 모듈 다중화 방법.

청구항 11

제 10 항에 있어서,

상기 운용 단계는,

호스트에서 상기 마스터 HSM으로 커넥션이 설정되는 단계;

상기 마스터 HSM이 상기 신규 생성 및/또는 변경 정보를 감지하는 단계;

상기 마스터 HSM이 상기 형성된 각각의 보안채널을 통해 상기 적어도 하나의 슬레이브 HSM으로 복제를 시도하는 단계

를 포함하는 하드웨어 보안 모듈 다중화 방법.

청구항 12

제 10 항에 있어서,

상기 운용 단계는,

호스트에서 상기 적어도 하나의 슬레이브 HSM 중 일 슬레이브 HSM으로 커넥션이 설정되는 단계;

상기 일 슬레이브 HSM이 상기 신규 생성 및/또는 변경 정보를 감지하는 단계;

상기 일 슬레이브 HSM이 상기 신규 생성 및/또는 변경 정보를 해당 보안채널을 통해 상기 마스터 HSM으로 전달하는 단계; 및

상기 마스터 HSM이 상기 형성된 각각의 보안채널을 통해 상기 적어도 하나의 슬레이브 HSM 중 타 슬레이브 HSM으로 복제를 시도하는 단계

를 포함하는 하드웨어 보안 모듈 다중화 방법.

청구항 13

프로세서를 구비한 하드웨어 보안 모듈(HSM) 다중화 장치에,

상기 HSM의 다중화시, 마스터 우선순위를 선정하는 기능;

각 HSM 간에 자신의 우선순위를 브로드캐스팅하여, 마스터 HSM을 결정하는 마스터 HSM 결정 기능;

마스터 HSM과 적어도 하나의 슬레이브 HSM 간에, 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 보안채널을 각각 형성하는 초기 설정 기능; 및

상기 형성된 각각의 보안채널을 통해, 상기 마스터 HSM이 신규 생성 및/또는 변경 정보를 모든 슬레이브 HSM에 복제하는 운용 기능

을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 14

제 13 항에 있어서,

상기 마스터 HSM의 장애 발생시, 상기 HSM 결정 기능을 통해 상기 적어도 하나의 슬레이브 HSM 중 차순위 HSM이 마스터로 결정되는 기능

을 더 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 15

제 13 항에 있어서,

상기 운용 기능에서,

상기 신규 생성 및/또는 변경 정보의 복제 오류 발생시, 복제하고자 하는 신규 생성 및/또는 변경 정보를 삭제하고 원상 복구시키는 기능

을 더 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <6> 본 발명은 하드웨어 보안 모듈 다중화 장치 및 그 방법과, 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것으로, 보다 상세하게는 전자 금융거래 및 고객 인증 등에 광범위하게 사용되는 하드웨어 보안 모듈(HSM : Hardware Security Module)을 호스트나 HSM의 장애 발생시에도 정상 운용이 가능하도록 효율적으로 다중화(/이중화)한, 하드웨어 보안 모듈 다중화 장치 및 그 방법과, 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.
- <7> 정보보호 및 인증기술에 있어서, 개인의 인증정보와 및 금융 거래를 위한 비밀번호 등의 정보를 하드웨어적으로 또한 암호학적으로 안전하게 관리하는 장치 및 시스템의 개발기술 필요성은 인터넷의 보급과 함께 제기되어 왔다.
- <8> 이 비밀정보는 개인을 인증하고 본인이 직접 특정 행위를 한 것을 확인하는 수단이 되기 때문에, 만일 이 비밀정보가 타인에게 노출된다면 행위자를 특정할 수 없어서 전체 금융거래 체계가 붕괴될 수 있으므로 매우 안전하게 관리되어야 한다.
- <9> 이와 같은 고도의 보안성을 제공하기 위해, 하드웨어적으로 동시에 암호학적으로 안전한 키 관리시스템을 탑재한 하드웨어 보안 모듈(HSM)이라는 개념이 소개되고 있다.
- <10> HSM은 내부에 자체적으로 비밀 마스터 키를 생성하고 이를 바탕으로 유도 키 생성 및 데이터의 암호/복호화를 처리하는 장치로서, 어떠한 방법으로도 내부에 저장된 데이터를 추출할 수 없고, 만일 물리적인 방법으로 데이터를 추출하고자 한다면 자체적으로 데이터를 소멸시키는 등의 안전장치를 확보하고, 이에 대한 공인기관의 인증을 받음으로써 비밀정보의 안전을 보장할 수 있는 장치이다.
- <11> 따라서, HSM은 사이버 거래와 같이 대면이 아닌 거래 방식에서 거래의 안전성을 확실하게 보장할 수 있는 수단이 되기 때문에, 금융거래, 통신회사의 가입자 인증 시스템 등에 널리 이용되고 있다.
- <12> 그러나, 만일 HSM 장치가 작동 중단 혹은 오작동 될 경우, 모든 고객 및 거래에 대한 처리가 중단되어 전체 시스템이 마비되는 문제가 발생되기 때문에, 이에 대비한 다중화(/이중화)는 반드시 필요하지만, 고도의 보안성을 확보하기 위한 장비의 폐쇄적인 성격으로 인해 다중화(/이중화)는 매우 어려운 형편이다
- <13> HSM을 다중화(/이중화)하기 위한 방법의 일례로, 다중화(/이중화) 전용의 호스트를 두고 이 호스트에 설치된 소프트웨어 방식의 프로그램이 다중화(/이중화)를 지원하는 방식이 존재하는데, 이 호스트의 장애 발생시 역시 시스템의 작동이 중단되는 문제가 있고, 또한 다중화(/이중화)에 있어서도 정적인 형태의 다중화(/이중화)만 지원하여, 만약 운용 중에 신규 정보가 생성될 경우 정상적으로 처리되지 못하는 문제점이 있다
- <14> 이와 같이, 전자 금융거래 및 고객 인증 등에 광범위하게 사용되는 HSM을 다중화(/이중화) 운용하는데 있어서, 모든 HSM의 정보가 항상 일치된 상태를 유지하여야 하기 때문에, 서비스 운용에 앞서 HSM 정보를 동일하게 맞추는 과정이 반드시 필요하다. 만약, HSM에 새로운 정보를 추가하고자 한다면, 관리자가 서비스를 중단시키고 추가된 정보를 다른 HSM으로 복제한 후에 다시 서비스를 개시하는 번거로운 과정을 거치는데, 고도의 보안성이 유지되어야 하는 HSM의 특성상 이를 자동화하기에는 어려운 문제점이 있다.

발명이 이루고자 하는 기술적 과제

- <15> 본 발명은 상기 문제점을 해결하기 위하여 제안된 것으로, 전자 금융거래 및 고객 인증 등에 광범위하게 사용되는 하드웨어 보안 모듈(HSM)을 호스트나 HSM의 장애 발생시에도 정상 운용이 가능하도록 효율적으로 다중화(/이중화)한, 하드웨어 보안 모듈 다중화 장치 및 그 방법과, 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있다.
- <16> 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실

현될 수 있음을 쉽게 알 수 있을 것이다.

발명의 구성 및 작용

- <17> 상기 목적을 달성하기 위한 본 발명은, 하드웨어 보안 모듈(HSM) 다중화 장치에 있어서, 기 설정된 우선순위에 따라 마스터로 지정되어, 자신의 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 적어도 하나의 슬레이브 HSM과 보안채널을 각각 형성하고, 신규 생성 및/또는 변경 정보를 각각의 보안채널을 통해 상기 적어도 하나의 HSM에 복제하기 위한 마스터 HSM; 및 기 설정된 우선순위에 따라 슬레이브로 지정되어, 자신의 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 상기 마스터 HSM과 상기 보안채널을 각각 형성하고, 각각의 보안채널을 통해 전송되는 신규 생성 및/또는 변경 정보를 저장(복제)하고 있는 상기 적어도 하나의 슬레이브 HSM을 포함하여 이루어진 것을 특징으로 한다.
- <18> 한편, 본 발명은, 하드웨어 보안 모듈(HSM) 다중화 방법에 있어서, 상기 HSM의 다중화시, 마스터 우선순위를 선정하는 단계; 각 HSM 간에 자신의 우선순위를 브로드캐스팅하여, 마스터 HSM을 결정하는 마스터 HSM 결정 단계; 마스터 HSM과 적어도 하나의 슬레이브 HSM 간에, 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 보안채널을 각각 형성하는 초기 설정 단계; 및 상기 형성된 각각의 보안채널을 통해, 상기 마스터 HSM이 신규 생성 및/또는 변경 정보를 모든 슬레이브 HSM에 복제하는 운용 단계를 포함하여 이루어진 것을 특징으로 한다.
- <19> 또한, 본 발명은, 상기 마스터 HSM의 장애 발생시, 상기 HSM 결정 단계를 통해 상기 적어도 하나의 슬레이브 HSM 중 차순위 HSM이 마스터로 결정되는 단계를 더 포함하여 이루어진 것을 특징으로 한다.
- <20> 또한, 본 발명은, 상기 운용 단계에서, 상기 신규 생성 및/또는 변경 정보의 복제 오류 발생시, 복제하고자 하는 신규 생성 및/또는 변경 정보를 삭제하고 원상 복구시키는 단계를 더 포함하여 이루어진 것을 특징으로 한다.
- <21> 한편, 본 발명은, 프로세서를 구비한 하드웨어 보안 모듈(HSM) 다중화 장치에, 상기 HSM의 다중화시, 마스터 우선순위를 선정하는 기능; 각 HSM 간에 자신의 우선순위를 브로드캐스팅하여, 마스터 HSM을 결정하는 마스터 HSM 결정 기능; 마스터 HSM과 적어도 하나의 슬레이브 HSM 간에, 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 보안채널을 각각 형성하는 초기 설정 기능; 및 상기 형성된 각각의 보안채널을 통해, 상기 마스터 HSM이 신규 생성 및/또는 변경 정보를 모든 슬레이브 HSM에 복제하는 운용 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.
- <22> 또한, 본 발명은, 상기 마스터 HSM의 장애 발생시, 상기 HSM 결정 기능을 통해 상기 적어도 하나의 슬레이브 HSM 중 차순위 HSM이 마스터로 결정되는 기능을 더 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.
- <23> 또한, 본 발명은, 상기 운용 기능에서, 상기 신규 생성 및/또는 변경 정보의 복제 오류 발생시, 복제하고자 하는 신규 생성 및/또는 변경 정보를 삭제하고 원상 복구시키는 기능을 더 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.
- <24> 본 발명은 전자 금융거래 및 고객인증 등에 광범위하게 사용되는 HSM을 호스트나 HSM의 장애 발생시에도 정상 운용이 가능하도록 효율적으로 다중화(/이중화)하고자 한다. 특히, 다중화(/이중화) 운용 상태에서 비밀키 등의 신규 정보를 생성할 경우에도, 생성된 정보가 자동적으로 이중화에 참여하고 있는 다른 HSM 장치로 고도의 보안성이 유지된 상태로 안전하게 복제되어, 다중화(/이중화) 작업이 정상적으로 처리될 수 있도록 한다(고도의 보안성이 유지된 상태로 HSM의 다중화(/이중화)).
- <25> 즉, 본 발명은 다수의 HSM 중 하나를 자동적으로 마스터 HSM으로 설정하고, 이 마스터 HSM이 본연의 기능인 공개키/비밀키 쌍에 의한 암호화 방식에 의해 다른 HSM들과 보안채널을 생성하여, 이 생성된 보안채널을 통해 운용중에 신규 생성 및 변경된 정보를 자동 복제하여 HSM간 데이터를 일치시킴으로써 서비스 운용중에 HSM의 다중화(/이중화)를 안전하게 제공할 수 있다.
- <26> 본 발명에 따르면, 전자지불 등의 사이버 금융 시스템이나 휴대인터넷(WiBro) 가입자 인증 장치 등에 필수적인 하드웨어 보안 모듈(HSM)을 안전하고 효율적으로 다중화(/이중화)할 수 있도록 함으로써, 만일에 발생할 수 있는 서비스의 장애에 효과적으로 대처할 수 있고, 향후 트래픽 증가에 따라 저렴하고 편리하게 시스템 처리 용량을 확장할 수 있는 확장성 있는(Scalable) 시스템을 구축할 수 있다.
- <27> 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에

따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명하기로 한다.

- <28> 도 1 은 본 발명에 따른 하드웨어 보안 모듈(HSM) 다중화 장치의 일실시예 구성도이다.
- <29> 도 1에 도시된 바와 같이, 본 발명에 따른 하드웨어 보안 모듈(HSM) 다중화 장치는, 기 설정된 우선순위에 따라 마스터(master)로 지정되어, 자신의 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 적어도 하나의 슬레이브 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)과 보안채널을 각각 형성하고, 신규 생성 및/또는 변경 정보를 각각의 보안채널을 통해 적어도 하나의 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)에 복제하기 위한 마스터 하드웨어 보안 모듈(HSM#m)(20-m)과, 기 설정된 우선순위에 따라 슬레이브(slave)로 지정되어, 자신의 공개키/비밀키 쌍을 이용해 송/수신 세션키를 생성하여 마스터 하드웨어 보안 모듈(HSM#m)(20-m)과 보안채널을 각각 형성하고, 각각의 보안채널을 통해 전송되는 신규 생성 및/또는 변경 정보를 저장(복제)하고 있는 적어도 하나의 슬레이브 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)을 포함한다.
- <30> 여기서, 마스터 하드웨어 보안 모듈(HSM#m)(20-m)의 장애 발생시, 기 설정된 우선순위에 따라, 적어도 하나의 슬레이브 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n) 중 차순위 하드웨어 보안 모듈(HSM)이 마스터로 자동 교체된다.
- <31> 또한, 각 하드웨어 보안 모듈(HSM)(20)은, 복제 과정에서 오류 발생시, 복제하고자 하는 신규 생성 및/또는 변경 정보를 삭제하고 원상 복구시킨다.
- <32> 또한, 각 하드웨어 보안 모듈(HSM)(20)은, 서로 다른 마스터 우선순위를 가지며, 전원 인가시 자신의 마스터 우선순위를 네트워크상으로 브로드캐스트하여, 자신보다 우선순위가 높은 하드웨어 보안 모듈(HSM)(20)로부터 메시지가 수신되지 않는다면 자신을 마스터로 지정한다.
- <33> 다중화(/이중화)로 구성된 하드웨어 보안 모듈들(HSM)(20)은 LAN 방식의 이더넷 스위치 등을 통해 호스트(Host)(10)와 접속할 수 있는 형태로 구성된다.
- <34> 하드웨어 보안 모듈(HSM)(20)을 이용하여 어떤 처리를 하고자 하는 응용 프로그램들(11)은 호스트(Host)(10) 내에서 실행되며, HSM 제조업체에서 제공하는 공개키 암호작성 시스템(PKCS : Public-Key Cryptography System)#11 라이브러리(12)를 통해서 하드웨어 보안 모듈(HSM)(20)과 접속되는데, 이 라이브러리(12)는 다중화 관리자(13)에 연결되고, 이 다중화 관리자(13)를 통해 정상 상태의 여러 하드웨어 보안 모듈(HSM)(20) 중에 처리 중인 세션 수가 가장 적은 하드웨어 보안 모듈(HSM)(20)로 접속 관리자(14)를 통해 자동적으로 연결된다.
- <35> 한편, 하드웨어 보안 모듈(HSM)(20)에는 호스트(Host)(10)로부터의 연결을 처리하기 위한 접속 관리자(22)가 존재하고, 이는 하드웨어 보안 모듈(HSM)(20) 내부에 관리되고 있는 가상 슬롯(slot)을 통해 실제 키 생성, 암호화 등을 처리하는 토큰(token)으로 접속된다.
- <36> 또한, 하드웨어 보안 모듈(특히, 마스터로 동작하는 하드웨어 보안 모듈(HSM#m)(20-m))의 모니터링 데몬(21)은 해당 하드웨어 보안 모듈(HSM)(20)에 새로운 데이터 생성 요구가 있는지를 감시하여, 만일 데이터의 변경이 발생한 경우, 이를 다른 하드웨어 보안 모듈(특히, 슬레이브로 동작하는 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n))로 보안채널을 통해 복제하며, 이 작업이 정상적으로 처리되는지를 관리하여 만일 단 하나의 하드웨어 보안 모듈(HSM)(20)에서라도 정상적으로 처리되지 못한 경우 전체 작업을 원상 복구시키고 호스트(Host)(10)의 응용 프로그램(11)에 이를 통보하여 적절한 처리가 이루어질 수 있도록 감시하는 역할을 수행한다.
- <37> 또한, 하드웨어 보안 모듈(HSM)(20)의 보안채널 관리자(23)는 다중화(/이중화) 상태를 유지하기 위해 하드웨어 보안 모듈(특히, 마스터로 동작하는 하드웨어 보안 모듈(HSM#m)(20-m)) 내부의 신규 생성 및/또는 변경 정보를 다른 하드웨어 보안 모듈(특히, 슬레이브로 동작하는 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n))로 안전하게 전달하기 위한 채널을 설정 및 해제를 관리하고, 데이터(신규 생성 및/또는 변경 정보)를 올바르게 전송하기 위한 기능을 처리한다.
- <38> 본 발명의 하드웨어 보안 모듈(HSM)(20)의 다중화를 위해서는 하드웨어 보안 모듈(HSM)(20)간 보안 채널을 형성하고(초기 설정 절차), 설정된 보안 채널을 통해 데이터를 복제해야 한다(운용 절차).
- <39> 도 2 는 본 발명에 따른 하드웨어 보안 모듈(HSM) 다중화 방법 중 HSM 간 보안 채널 형성 과정을 보여주는 일실시예 흐름도로서, 초기 설정 과정에서 하드웨어 보안 모듈(HSM)(20) 간 보안 채널을 형성하기 위한 절차를 나타

낸다.

- <40> 먼저, 다중화(/이중화)로 구성하기 위해, 모든 하드웨어 보안 모듈(HSM)(20) 내부에 마스터 우선순위를 서로 다르게 미리 설정해둔다. 예를 들면, 하드웨어 보안 모듈(HSM#m)(20-m)의 마스터 우선순위는 "1", 하드웨어 보안 모듈(HSM#1)(20-1)의 마스터 우선순위는 "2", 하드웨어 보안 모듈(HSM#n)(20-n)의 마스터 우선순위는 "3"으로 미리 설정한다.
- <41> 이후, 하드웨어 보안 모듈(HSM)(20)에 전원이 인가되면(201), 각 하드웨어 보안 모듈(HSM)(20)은 자신의 마스터 우선순위를 네트워크상으로 브로드캐스트(broadcast)하고(202), 일정 시간 경과 뒤에(203) 자신 보다 우선순위가 높은 하드웨어 보안 모듈(HSM)으로부터 메시지가 수신되지 않았다면(즉, 자신 보다 우선순위가 높은 HSM이 존재하지 않는 경우)(204), 자신을 마스터(하드웨어 보안 모듈(HSM#m)(20-m))로 지정한다(205).
- <42> 그러나, 자신(이 경우, 슬레이브로 동작하는 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)임)보다 우선순위가 높은 하드웨어 보안 모듈(이 경우, 마스터로 동작하는 하드웨어 보안 모듈(HSM#m)(20-m)임)로부터 메시지를 수신한 경우(즉, 자신 보다 우선순위가 높은 HSM이 존재하는 경우)(204), 해당 하드웨어 보안 모듈(마스터 하드웨어 보안 모듈(HSM#m)(20-m))을 마스터로 지정하고 자신은 슬레이브 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)이 된다(206).
- <43> 만약, 마스터 하드웨어 보안 모듈(HSM#m)(20-m)의 장애 발생시, 마스터 설정 절차부터 다시 실행하게 된다(202~206). 즉, 마스터 하드웨어 보안 모듈(HSM#m)(20-m)의 장애 발생시, 차순위 하드웨어 보안 모듈(HSM)(즉, 마스터 우선순위가 "2"인 하드웨어 보안 모듈(HSM#1)(20-1))이 마스터로 된다.
- <44> 한편, 마스터로 지정된 하드웨어 보안 모듈(HSM#m)(20-m)은 자신의 공개키와 비밀키 쌍(PU_m , PR_m)을 생성하고(207), 이를 자신의 저장장치에 저장한 후, 공개키(PU_m)를 미리 정의된 설정에 따라 다중화(/이중화)에 참여하는 슬레이브 하드웨어 보안 모듈(HSM#n)(20-n)로 전송한다(208,209),
- <45> 이후, 마스터 하드웨어 보안 모듈(HSM#m)(20-m)로부터 공개키(PU_m)를 전달받은 슬레이브 하드웨어 보안 모듈(HSM#n)(20-n)은 자신의 공개키와 비밀키 쌍(PU_n , PR_n)을 생성하여 자신의 저장장치에 저장한 후, 공지의 난수 생성 알고리즘에 의거하여 임의의 난수($Rand_n$)를 생성하고(210), 생성된 난수($Rand_n$)를 마스터 하드웨어 보안 모듈(HSM#m)(20-m)의 공개키(PU_m)로 암호화한 $E_{PU_m}(Rand_n)$ 을 생성하여(211), 자신의 공개키(PU_n)와 함께 응답 메시지를 통해 마스터 하드웨어 보안 모듈(HSM#m)(20-m)로 전달한다(212).
- <46> 다음으로, $E_{PU_m}(Rand_n)$ 을 수신한 마스터 하드웨어 보안 모듈(HSM#m)(20-m)은 $E_{PU_m}(Rand_n)$ 를 자신의 비밀키(PR_m)로 복호화한(213) 값인 난수($Rand_n$)를 슬레이브 하드웨어 보안 모듈(HSM#n)(20-n)에 대한 송신 세션키, 난수($Rand_m$)를 수신 세션키로 설정한다(216). 이때, 수신 세션키로 설정되는 임의의 난수 $Rand_m$ 는 마스터 하드웨어 보안 모듈(HSM#m)(20-m)에서 공지의 난수 생성 알고리즘에 의해서 생성한 값이다(214).
- <47> 그리고, 마스터 하드웨어 보안 모듈(HSM#m)(20-m)은 이렇게 생성된 난수($Rand_m$)를 슬레이브 하드웨어 보안 모듈(HSM#n)(20-n)의 공개키(PU_n)로 암호화한 $E_{PU_n}(Rand_m)$ 을 생성하여(214) 이를 응답 메시지로써 슬레이브 하드웨어 보안 모듈(HSM#n)(20-n)에게 전달한다(215).
- <48> 이후, $E_{PU_n}(Rand_m)$ 를 수신한 슬레이브 하드웨어 보안 모듈(HSM#n)(20-n)에서는 자신의 비밀키(PR_n)로 복호화한(217) 값인 난수($Rand_m$)를 마스터 하드웨어 보안 모듈(HSM#m)(20-m)에 대한 수신 세션키, 난수($Rand_n$)를 송신 세션키로 설정한다(218).
- <49> 이 과정을 통해 마스터 하드웨어 보안 모듈(HSM#m)(20-m)과 슬레이브 하드웨어 보안 모듈(HSM#n)(20-n)은 보안 채널을 형성하며, 이후 이 두 HSM(20-m, 20-n) 간의 데이터 전송은 난수($Rand_m$ 과 $Rand_n$)로 암호화되어 처리되어 외부에 노출되는 것을 막을 수 있다.
- <50> 이와 같은 방식을 반복하여 마스터 역할을 하는 하드웨어 보안 모듈(HSM#m)(20-m)과 슬레이브 역할을 하는 다른 모든 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n) 간에 보안채널이 형성되면, 초기 설정 과정이 완료된 것이며, 초기 설정이 완료되면 하드웨어 보안 모듈(HSM)(20)은 서비스를 제공할 수 있는 운용 상태가 될 수 있다.

- <51> 도 3 은 본 발명에 따른 하드웨어 보안 모듈(HSM) 다중화 방법 중 보안 채널을 통한 데이터 복제 과정에 대한 일실시에 흐름도로서, 운용 중인 하드웨어 보안 모듈(HSM#m)(20-m)에 신규 정보 및 변경 정보가 생성될 경우 이를 다중화(/이중화)에 참여하고 있는 모든 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)로 미리 형성된 보안채널을 통해 해당 신규 정보 및 변경 정보를 복제하는 절차를 나타낸다.
- <52> 운용 상태의 하드웨어 보안 모듈(HSM)(20)을 이용하여 키 생성 또는 암호/복호화 작업 등 본연의 기능을 처리하기 위해서는, 응용 프로그램(11)이 실행되는 호스트(10)에서 하드웨어 보안 모듈(HSM)(20)을 접속하게 되는데, 하드웨어 보안 모듈(HSM)(20)이 다중화(/이중화)된 환경에서는 이 하드웨어 보안 모듈(HSM)(20)들 중 하나로 커넥션이 설정되게 된다(301). 여기서, 마스터 하드웨어 보안 모듈(HSM#m)(20-m)로 연결(TCP/IP 커넥션)이 설정되었다고 가정하자.
- <53> 이후, 호스트(10)의 키 생성 요청에 따라(302), 마스터 하드웨어 보안 모듈(HSM#m)(20-m)에서 키(K_i)를 생성하게 되면(303), 이는 접속된 하나의 하드웨어 보안 모듈(마스터 하드웨어 보안 모듈(HSM#m)(20-m)) 내에서만 생성되기 때문에 만일 이 키를 이용한 작업을 원하는 다른 응용 프로그램(11)이 다른 하드웨어 보안 모듈(예를 들면, 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n))에 접속되게 되면 처리가 불가능하게 된다.
- <54> 따라서, 마스터 하드웨어 보안 모듈(HSM#m)(20-m) 내에 신규 정보의 생성을 감지한 모니터링 데몬(21)은 상기 도 2의 초기 설정과정에서 생성한 보안채널을 통해 신규 생성 및/또는 변경된 정보(예를 들면, 생성된 키(K_i)를 복제 대상 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)의 난수($Rand_1, \dots, Rand_i$)로 암호화한($E_{RAND_1}(K_i), \dots, E_{RAND_i}(K_i)$) 값)(304,307)를 다른 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)로 복제를 시도하여(305,308), 다른 슬레이브 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)로부터 정상 처리 메시지를 수신한 후에(306,309) 데이터 복제 절차를 종료하게 된다.
- <55> 따라서, 복제된 키(K_i)를 전달받은 슬레이브 하드웨어 보안 모듈들(HSM#1~HSM#n)(20-1~20-n)은 키가 생성된 마스터 하드웨어 보안 모듈(HSM#m)(20-m)과 동일한 작업이 가능하게 되므로 다중화(/이중화)된 상태를 유지 가능하다.
- <56> 만일 데이터 복제 도중 하나의 하드웨어 보안 모듈(HSM#1~HSM#n)(20-1~20-n)에서라도 오류가 발생할 경우(310), 복제하고자 했던 데이터를 삭제하여 원상 복구시키고 나서 오류를 응답하여 응용 프로그램(11)이 다시 적절한 처리를 하도록 한다(311).
- <57> 그런데, 만약 슬레이브로 동작하는 하드웨어 보안 모듈(HSM#1)(20-1)로 연결(TCP/IP 커넥션)이 설정되고, 호스트(10)의 키 생성 요청에 따라 슬레이브 하드웨어 보안 모듈(HSM#1)(20-1)에서 키(K_j)를 생성하게 되면, 슬레이브 하드웨어 보안 모듈(HSM#1)(20-1) 내에 신규 정보의 생성을 감지한 모니터링 데몬은 상기 도 2의 초기 설정과정에서 생성한 보안채널을 통해 마스터 하드웨어 보안 모듈(HSM#m)(20-m)로 신규 생성 및/또는 변경된 정보를 전달한다.
- <58> 그러면, 마스터 하드웨어 보안 모듈(HSM#m)(20-m)의 모니터링 데몬(21)은 상기 도 2의 초기 설정과정에서 생성한 보안채널을 통해 신규 생성 및/또는 변경된 정보(예를 들면, 생성된 키(K_j)를 복제 대상 하드웨어 보안 모듈(HSM#2~HSM#n)(20-2~20-n)의 난수($Rand_1, \dots, Rand_2$)로 암호화한($E_{RAND_1}(K_j), \dots, E_{RAND_2}(K_j)$) 값)를 다른 하드웨어 보안 모듈(HSM#2~HSM#n)(20-2~20-n)로 복제를 시도하여, 다른 슬레이브 하드웨어 보안 모듈(HSM#2~HSM#n)(20-2~20-n)로부터 정상 처리 메시지를 수신한 후에 데이터 복제 절차를 종료하게 된다.
- <59> 따라서, 복제된 키(K_j)를 전달받은 슬레이브 하드웨어 보안 모듈들(HSM#2~HSM#n)(20-2~20-n)은 키(K_j)가 생성된 하드웨어 보안 모듈(HSM#1)(20-1)과 동일한 작업이 가능하게 되므로 다중화(/이중화)된 상태를 유지 가능하다.
- <60> 이와 같은 과정을 통해 운용중에 하드웨어 보안 모듈(HSM)(20)에 생성된 키 정보는 다중화(/이중화)된 다른 하드웨어 보안 모듈(HSM)(20)으로 안전하게 자동적으로 전송되며, 서비스의 중단없이 다중화(/이중화) 상태를 정상적으로 유지할 수 있게 된다.
- <61> 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.
- <62> 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적

사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

발명의 효과

<63> 상기와 같은 본 발명은, 전자지불 등의 사이버 금융 시스템이나 휴대인터넷(WiBro) 가입자 인증 장치 등에 필수적인 하드웨어 보안 모듈(HSM)을 안전하고 효율적으로 이중화하는 방법을 제공함으로써, 만일에 발생할 수 있는 서비스의 장애에 효과적으로 대처할 수 있고, 향후 트래픽 증가에 따라 저렴하고 편리하게 시스템 처리 용량을 확장할 수 있는 Scalable한 시스템을 구축할 수 있는 효과가 있다.

<64> 특히, 본 발명은, 운용중에 HSM에 생성 및 변경된 키 정보를 다중화(/이중화)된 다른 HSM으로 안전하게 자동적으로 전송하며, 서비스의 중단없이 다중화(/이중화) 상태를 정상적으로 유지할 수 있는 효과가 있다.

도면의 간단한 설명

<1> 도 1 은 본 발명에 따른 하드웨어 보안 모듈(HSM) 다중화 장치의 일실시에 구성도,

<2> 도 2 는 본 발명에 따른 하드웨어 보안 모듈(HSM) 다중화 방법 중 HSM 간 보안 채널 형성 과정을 보여주는 일실시예 흐름도,

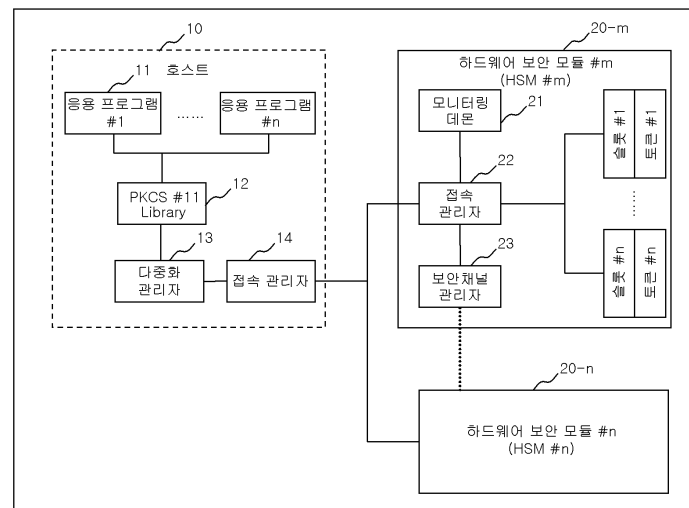
<3> 도 3 은 본 발명에 따른 하드웨어 보안 모듈(HSM) 다중화 방법 중 보안 채널을 통한 데이터 복제 과정에 대한 일실시예 흐름도이다.

<4> * 도면의 주요 부분에 대한 부호 설명

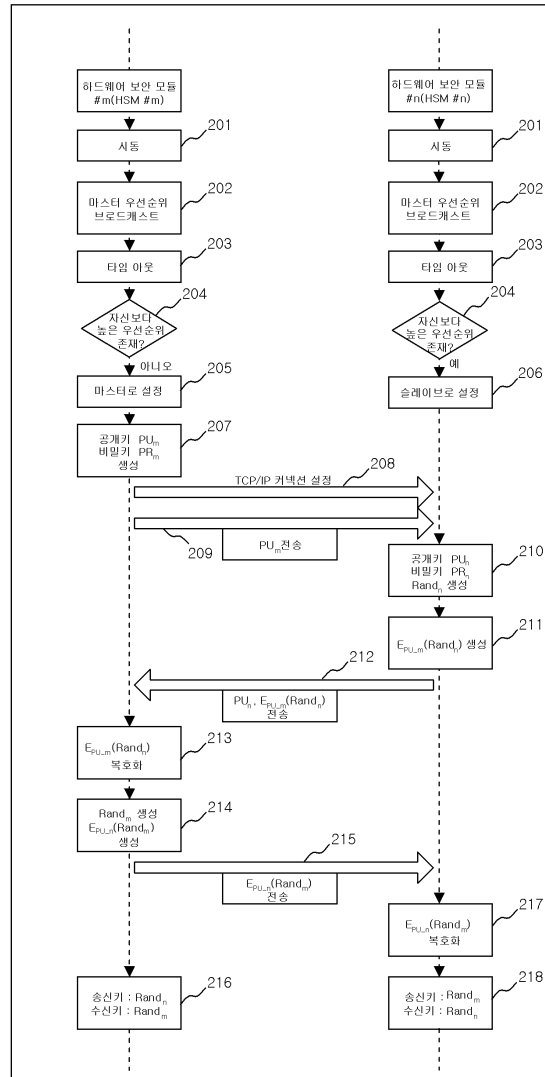
<5> 10 : 호스트 20 : 하드웨어 보안 모듈(HSM)

도면

도면1



도면2



도면3

