(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년06월08일
(11) 등록번호 10-1628614
(24) 등록일자 2016년06월01일

(51) 국제특허분류(Int. Cl.)
G06F 21/42 (2013.01) *H04L 9/32* (2006.01)
H04W 12/06 (2009.01)
(52) CPC특허분류
G06F 21/42 (2013.01)
H04L 9/3247 (2013.01)
(21) 출원번호 10-2015-0054342
(22) 출원일자 2015년04월17일
심사청구일자 2015년04월17일
(56) 선행기술조사문헌
KR101364996 B1
JP2015037298 A
KR1020130101632 A
KR101260934 B1

(73) 특허권자
(주)에이티솔루션즈
서울특별시 마포구 성암로 189 , 1201호(상암동, 중소기업디엠씨타워)
(72) 발명자
김종서
서울특별시 강남구 압구정로11길 17 미성아파트

전체 청구항 수 : 총 15 항 심사관 : 문남두

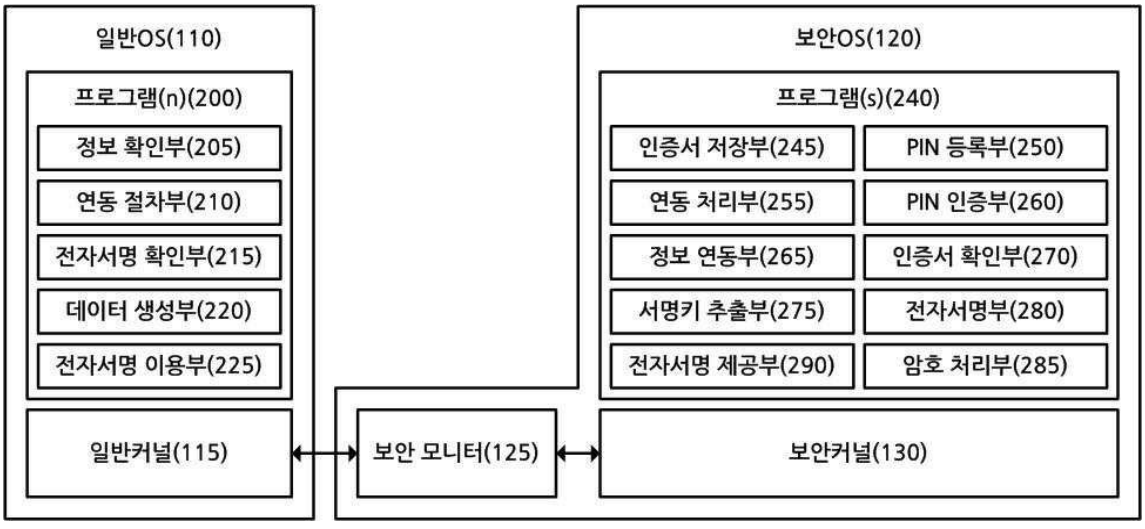
(54) 발명의 명칭 **보안운영체제를 이용한 전자서명 처리 방법**

(57) 요 약

본 발명은 보안운영체제를 이용한 전자서명 처리 방법에 관한 것으로, 본 발명에 따른 보안운영체제를 이용한 전자서명 처리 방법은, 보안커널(Secure Kennel)을 구비한 보안OS(Secure Operating System)와 커널구조가 공개된 일반OS(Normal Operating System)를 탑재한 무선단말을 통해 실행되는 방법에 있어서, 상기 일반OS의 프로그램

(뒷면에 계속)

대 표 도 - 도2



(n)이 상기 보안OS의 지정된 프로그램(s)에서 접근 가능한 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인하는 제1 단계와, 상기 프로그램(n)이 서명대상정보를 상기 메모리영역으로 제공하는 제2 단계와, 상기 보안OS의 프로그램(s)이 상기 메모리영역으로부터 서명대상정보를 확인하는 제3 단계와, 상기 프로그램(s)이 상기 보안OS에 구비된 인증서로부터 서명 키를 추출하여 상기 서명대상정보에 대한 전자서명 값을 생성하거나 또는 HSM(Hardware Security Module)을 통해 생성된 전자서명 값을 확인하는 제4 단계와, 상기 프로그램(s)이 상기 전자서명 값을 상기 메모리영역으로 제공하는 제5 단계와, 상기 프로그램(n)이 상기 메모리영역의 전자서명 값을 이용하여 전자서명 절차를 수행하는 제6 단계를 포함한다.

(52) CPC특허분류
H04L 9/3263 (2013.01)
H04W 12/06 (2013.01)

명 세 서

청구범위

청구항 1

보안커널(Secure Kennel)을 구비한 보안OS(Secure Operating System)와 커널구조가 공개된 일반OS(Normal Operating System)를 탑재한 무선단말을 통해 실행되는 방법에 있어서,

상기 일반OS의 프로그램(n)이 상기 보안OS의 지정된 프로그램(s)에서 접근 가능한 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인하는 제1 단계;

상기 프로그램(n)이 서명대상정보를 상기 메모리영역으로 제공하는 제2 단계;

상기 보안OS의 프로그램(s)이 상기 메모리영역으로부터 서명대상정보를 확인하는 제3 단계;

상기 프로그램(s)이 상기 보안OS에 구비된 인증서로부터 서명 키를 추출하여 상기 서명대상정보에 대한 전자서명 값을 생성하거나 또는 HSM(Hardware Security Module)을 통해 생성된 전자서명 값을 확인하는 제4 단계;

상기 프로그램(s)이 상기 전자서명 값을 상기 메모리영역으로 제공하는 제5 단계; 및

상기 프로그램(n)이 상기 메모리영역의 전자서명 값을 이용하여 전자서명 절차를 수행하는 제6 단계;를 포함하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 2

제 1항에 있어서, 상기 보안OS는,

프로세서에 탑재된 트러스트존(Trust Zone)을 포함하여 이루어지는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 3

제 1항에 있어서,

상기 프로그램(n)이 상기 보안OS에 지정된 프로그램(s)이 탑재되었음을 식별하거나 상기 보안OS에 탑재된 프로그램(s)을 식별하는 식별정보를 일반OS 저장영역에 저장하는 단계를 더 포함하며,

상기 제1 단계는, 상기 보안OS에 상기 프로그램(s)이 탑재된 경우에 상기 프로그램(n)이 상기 메모리영역을 할당하거나 확인하는 단계를 포함하여 이루어지는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 4

제 1항에 있어서,

상기 프로그램(s)이 보안OS의 인증서 저장영역 또는 HSM에 사용자의 인증서를 저장하는 단계를 더 포함하며,

상기 제1 단계는, 상기 보안OS의 인증서 저장영역 또는 HSM에 사용자의 인증서가 저장된 경우에 상기 프로그램(n)이 상기 메모리영역을 할당하거나 확인하는 단계를 포함하여 이루어지는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 5

제 1항에 있어서,

상기 일반OS의 프로그램(n)이 상기 무선단말의 통신수단을 통해 지정된 서버로부터 서명대상정보를 수신하는 단계를 더 포함하며,

상기 제2 단계는, 상기 프로그램(n)이 상기 서버로부터 수신된 서명대상정보를 상기 메모리영역으로 제공하는 단계를 포함하여 이루어지는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 6

제 1항에 있어서,

상기 일반OS의 프로그램(n)이 상기 서명대상정보를 생성하는 단계를 더 포함하며,

상기 제2 단계는, 상기 프로그램(n)이 상기 생성된 서명대상정보를 상기 메모리영역으로 제공하는 단계를 포함하여 이루어지는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 7

제 1항에 있어서,

상기 프로그램(n)이 상기 보안OS로 전환되기 직전의 상기 프로그램(n)에 대한 상태정보를 저장하여 유지하는 단계를 더 포함하며,

상기 제2 단계는, 상기 상태정보가 저장된 후 상기 프로그램(n)이 서명대상정보를 상기 메모리영역으로 제공하는 단계를 포함하여 이루어지는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 8

제 1항에 있어서, 상기 제1 단계는,

상기 프로그램(n)이 SMC(Secure Monitor Call) 명령을 통해 보안OS를 구동하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 9

제 1항에 있어서, 상기 제1 단계는,

상기 프로그램(n)이 일반OS에 상기 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인하는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 10

제 1항에 있어서, 상기 제1 단계는,

상기 프로그램(n)이 일반OS와 보안OS 간 전환 절차를 수행하는 보안 모니터에 상기 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인하는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 11

제 1항에 있어서, 상기 제1 단계는,

상기 프로그램(n)이 네트워크 상의 보안서버에 보안OS의 프로그램(s)에서 접근 가능한 메모리영역을 할당하거나

또는 기 할당된 메모리영역을 확인하는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 12

제 1항에 있어서, 상기 제1 단계는,

상기 프로그램(n)이 상기 메모리영역을 참조하는 일반OS 측의 프로세스로 상기 프로그램(n)을 설정하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 13

제 1항에 있어서,

상기 프로그램(s)이 상기 메모리영역으로부터 서명대상정보를 확인한 후,

상기 프로그램(s)이 보안OS를 통해 무선단말의 입력수단에 접근하여 PIN(Personal Identification Number)을 입력받는 단계; 및

상기 보안OS를 통해 입력된 PIN의 유효성을 인증하는 단계;를 더 포함하여 이루어지는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 14

제 1항에 있어서,

상기 프로그램(s)이 상기 전자서명 값을 확인한 후,

상기 프로그램(s)이 지정된 서버를 통해 복호화 가능하게 상기 전자서명 값을 암호화하는 단계를 더 포함하며,

상기 제5 단계는, 상기 암호화된 전자서명 값을 상기 메모리영역으로 제공하는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

청구항 15

제 14항에 있어서,

상기 프로그램(s)이 상기 암호화된 전자서명 값을 상기 메모리영역으로 제공한 후,

상기 프로그램(n)이 상기 메모리영역으로부터 상기 보안OS의 프로그램(s)를 통해 암호화된 전자서명 값을 확인하는 단계를 더 포함하며,

상기 제6 단계는, 상기 암호화된 전자서명 값을 이용하여 전자서명 절차를 수행하는 것을 특징으로 하는 보안운영체제를 이용한 전자서명 처리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 보안커널을 구비한 보안OS(Secure Operating System)와 커널구조가 공개된 일반OS를 탑재한 무선단말에서 일반OS와 고립된 별도의 보안OS 측에 인증서를 구비한 후 상기 보안OS의 인증서를 통해 전자서명하는 것이다.

배 경 기 술

[0002] 최근 하나의 물리 프로세서 코어를 시큐어월드(Secure World)와 노멀월드(Normal World)의 두 가지 월드로 나누고, 각각의 월드를 고립시켜 운영하는 트러스트존(Trust Zone) 기술이 제안되었다. 트러스트존 기술은 노멀월드에 일반적인 운영체제를 탑재하고 시큐어월드에 보안이 강화된 운영체제를 탑재하되 시큐어월드를 노멀월드와 고립시켜 운영함으로써, 노멀월드가 해킹되거나 위변조 되더라도 노멀월드와 고립된 시큐어월드의 보안을 보장하는 기술이다.

[0003] 트러스트존 기술에서 시큐어월드와 노멀월드의 고립은 시큐어월드의 보안을 보장하는 핵심사항 중의 하나이다. 시큐어월드에서 실행된 애플리케이션은 노멀월드의 운영체제를 이용하지 않고 직접 단말기에 구비된 디스플레이 장치, 통신장치, 입력장치 등의 각종 구성부에 직접 접근하여 제어할 수 있다(특허등록 제10-1259824호). 시큐어월드와 노멀월드는 물리적으로 하나의 단말기 내에서 하나의 프로세서 코어를 공유하고, 시큐어월드는 노멀월드를 통해 구동되기는 하지만, 하드웨어적인 측면과 소프트웨어적인 측면에서 시큐어월드와 노멀월드는 상호 고립된 서로 다른 시스템이다.

[0004] 따라서 시큐어월드와 노멀월드를 탑재한 무선단말에 인증서를 구비하는 경우, 상기 노멀월드와 무관하게 시큐어월드만을 통해 인증서 기능을 구현하는 것은 트러스트존과 관련된 기술 규격을 참조하여 당업자가 비교적 용이하게 도출할 수 있을 것이나, 상기 노멀월드와 시큐어월드를 실시간 연동하여 내부적으로는 각각의 고립된 월드를 통해 각기 필요한 절차를 고립시켜 수행하되, 외부적으로는 각 월드를 구별하지 않고 수행되는 것처럼 구현하기란 기술적으로 난해한 문제점을 지니고 있다.

발명의 내용

해결하려는 과제

[0005] 상기와 같은 문제점을 해소하기 위한 본 발명의 목적은, 무선단말에 일반OS(Normal Operating System)와 보안OS(Secure Operating System)를 포함하는 이종의 OS가 탑재된 경우, 상기 보안OS에 사용자의 인증서를 탑재한 후, 상기 일반OS의 프로그램(n)이 상기 보안OS의 지정된 프로그램(s)에서 접근 가능한 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인하여 상기 보안OS의 프로그램(s)으로 서명대상정보를 제공하면, 상기 보안OS의 프로그램(s)이 상기 보안OS에 탑재된 인증서를 이용하여 상기 서명대상정보를 전자서명하는, 보안운영체제를 이용한 전자서명 처리 방법을 제공함에 있다.

과제의 해결 수단

[0006] 본 발명에 따른 보안운영체제를 이용한 전자서명 처리 방법은, 보안커널(Secure Kennel)을 구비한 보안OS(Secure Operating System)와 커널구조가 공개된 일반OS(Normal Operating System)를 탑재한 무선단말을 통해 실행되는 방법에 있어서, 상기 일반OS의 프로그램(n)이 상기 보안OS의 지정된 프로그램(s)에서 접근 가능한 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인하는 제1 단계와, 상기 프로그램(n)이 서명대상정보를 상기 메모리영역으로 제공하는 제2 단계와, 상기 보안OS의 프로그램(s)이 상기 메모리영역으로부터 서명대상정보를 확인하는 제3 단계와, 상기 프로그램(s)이 상기 보안OS에 구비된 인증서로부터 서명 키를 추출하여 상기 서명대상정보에 대한 전자서명 값을 생성하거나 또는 HSM(Hardware Security Module)을 통해 생성된 전자서명 값을 확인하는 제4 단계와, 상기 프로그램(s)이 상기 전자서명 값을 상기 메모리영역으로 제공하는 제5 단계와, 상기 프로그램(n)이 상기 메모리영역의 전자서명 값을 이용하여 전자서명 절차를 수행하는 제6 단계를 포함한다.

[0007] 본 발명에 따르면, 상기 보안OS는 프로세서에 탑재된 트러스트존(Trust Zone)을 포함할 수 있다.

[0008] 본 발명에 따르면, 상기 보안운영체제를 이용한 전자서명 처리 방법은, 상기 프로그램(n)이 상기 보안OS에 지정된 프로그램(s)이 탑재되었음을 식별하거나 상기 보안OS에 탑재된 프로그램(s)을 식별하는 식별정보를 일반OS 저장영역에 저장하는 단계를 더 포함하며, 상기 제1 단계는, 상기 보안OS에 상기 프로그램(s)이 탑재된 경우에 상기 프로그램(n)이 상기 메모리영역을 할당하거나 확인하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0009] 본 발명에 따르면, 상기 보안운영체제를 이용한 전자서명 처리 방법은, 상기 프로그램(s)이 보안OS의 인증서 저장영역 또는 HSM에 사용자의 인증서를 저장하는 단계를 더 포함하며, 상기 제1 단계는, 상기 보안OS의 인증서 저장영역 또는 HSM에 사용자의 인증서가 저장된 경우에 상기 프로그램(n)이 상기 메모리영역을 할당하거나 확인하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0010] 본 발명에 따르면, 상기 보안운영체제를 이용한 전자서명 처리 방법은, 상기 일반OS의 프로그램(n)이 상기 무선단말의 통신수단을 통해 지정된 서버로부터 서명대상정보를 수신하는 단계를 더 포함하며, 상기 제2 단계는, 상기 프로그램(n)이 상기 서버로부터 수신된 서명대상정보를 상기 메모리영역으로 제공하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0011] 본 발명에 따르면, 상기 보안운영체제를 이용한 전자서명 처리 방법은, 상기 일반OS의 프로그램(n)이 상기 서명대상정보를 생성하는 단계를 더 포함하며, 상기 제2 단계는, 상기 프로그램(n)이 상기 생성된 서명대상정보를 상기 메모리영역으로 제공하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0012] 본 발명에 따르면, 상기 보안운영체제를 이용한 전자서명 처리 방법은, 상기 프로그램(n)이 상기 보안OS로 전환되기 직전의 상기 프로그램(n)에 대한 상태정보를 저장하여 유지하는 단계를 더 포함하며, 상기 제2 단계는, 상기 상태정보가 저장된 후 상기 프로그램(n)이 서명대상정보를 상기 메모리영역으로 제공하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0013] 본 발명에 따르면, 상기 제1 단계는 상기 프로그램(n)이 SMC(Secure Monitor Call) 명령을 통해 보안OS를 구동하는 단계를 더 포함할 수 있다.

[0014] 본 발명에 따르면, 상기 제1 단계는 상기 프로그램(n)이 일반OS에 상기 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인할 수 있다.

[0015] 본 발명에 따르면, 상기 제1 단계는 상기 프로그램(n)이 일반OS와 보안OS 간 전환 절차를 수행하는 보안 모니터에 상기 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인할 수 있다.

[0016] 본 발명에 따르면, 상기 제1 단계는 상기 프로그램(n)이 네트워크 상의 보안서버에 보안OS의 프로그램(s)에서 접근 가능한 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인할 수 있다.

[0017] 본 발명에 따르면, 상기 제1 단계는 상기 프로그램(n)이 상기 메모리영역을 참조하는 일반OS 측의 프로세스로 상기 프로그램(n)을 설정하는 단계를 더 포함할 수 있다.

[0018] 본 발명에 따르면, 상기 보안운영체제를 이용한 전자서명 처리 방법은, 상기 프로그램(s)이 상기 메모리영역으로부터 서명대상정보를 확인한 후, 상기 프로그램(s)이 보안OS를 통해 무선단말의 입력수단에 접근하여 PIN(Personal Identification Number)을 입력받는 단계 및 상기 보안OS를 통해 입력된 PIN의 유효성을 인증하는 단계;를 더 포함하여 이루어지는 것을 특징으로 한다.

[0019] 본 발명에 따르면, 상기 보안운영체제를 이용한 전자서명 처리 방법은, 상기 프로그램(s)이 상기 전자서명 값을 확인한 후, 기 프로그램(s)이 지정된 서버를 통해 복호화 가능하게 상기 전자서명 값을 암호화하는 단계를 더 포함하며, 상기 제5 단계는, 상기 암호화된 전자서명 값을 상기 메모리영역으로 제공하는 것을 특징으로 한다.

[0020] 본 발명에 따르면, 상기 보안운영체제를 이용한 전자서명 처리 방법은, 상기 프로그램(s)이 상기 암호화된 전자서명 값을 상기 메모리영역으로 제공한 후, 상기 프로그램(n)이 상기 메모리영역으로부터 상기 보안OS의 프로그

램(s)를 통해 암호화된 전자서명 값을 확인하는 단계를 더 포함하며, 상기 제6 단계는, 상기 암호화된 전자서명 값을 이용하여 전자서명 절차를 수행하는 것을 특징으로 한다.

발명의 효과

[0021] 본 발명에 따르면, 무선단말에 일반OS와 보안OS를 포함하는 이종의 OS가 탑재된 경우, 보안OS에 사용자의 인증서를 구비한 후 일반OS에서 보안OS로 서명대상정보를 제공하여 보안OS의 인증서를 통해 보안OS 내에서 전자서명함으로써, 일반OS의 해킹이나 변조에 대하여 안전한 전자서명을 제공하는 이점이 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 실시 방법에 따른 무선단말의 기능 구성을 도시한 도면이다.

도 2는 본 발명의 실시 방법에 따른 프로그램의 기능 구성을 도시한 도면이다.

도 3은 본 발명의 실시 방법에 따라 보안OS에 프로그램(s)을 준비하는 과정을 도시한 도면이다.

도 4는 본 발명의 실시 방법에 따라 일반OS와 보안OS 간 거래 연동 과정을 도시한 도면이다.

도 5는 본 발명의 실시 방법에 따라 보안OS를 통해 전자서명을 생성하여 일반OS를 통해 이용하는 과정을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0023] 이하 첨부된 도면과 설명을 참조하여 본 발명의 바람직한 실시예에 대한 동작 원리를 상세히 설명한다. 다만, 하기에 도시되는 도면과 후술되는 설명은 본 발명의 특징을 효과적으로 설명하기 위한 여러 가지 방법 중에서 바람직한 실시 방법에 대한 것이며, 본 발명이 하기의 도면과 설명만으로 한정되는 것은 아니다.

[0024] 또한, 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서, 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 발명에서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0025] 결과적으로, 본 발명의 기술적 사상은 청구범위에 의해 결정되며, 이하 실시예는 진보적인 본 발명의 기술적 사상을 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 효율적으로 설명하기 위한 일 수단일 뿐이다.

[0026] 도면1은 본 발명의 실시 방법에 따른 무선단말(100)의 기능 구성을 도시한 도면이다.

[0027] 보다 상세하게 본 도면1은 보안커널(130)을 구비한 보안OS(120)와 커널구조가 공개된 일반OS(110)를 탑재한 무선단말(100)에서 상기 보안OS(120)에 구비된 인증서를 이용하여 서명대상정보의 전자서명을 처리하는 기능 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면1을 참조 및/또는 변형하여 상기 무선단말(100) 기능에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면1에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다. 바람직하게, 본 도면1의 무선단말(100)은 보안OS(120)와 일반OS(110)를 탑재한 스마트폰, 태블릿PC, PDA 등의 각종 단말기를 포함할 수 있다.

[0028] 도면1을 참조하면, 상기 무선단말(100)은, 제어부(105)와 메모리부(175)와 화면출력부(140)와 사용자입력부(145)와 사운드처리부(150)와 근거리 무선 통신부(155)와 무선망 통신부(160)와 NFC부(170)와 USIM 리더부(165) 및 USIM를 구비하며, 전원 공급을 위한 배터리를 구비한다.

[0029] 상기 제어부(105)는 상기 무선단말(100)의 동작을 제어하는 구성의 총칭으로서, 물리적으로 프로세서와 실행 메모리를 포함하여 구성되며, 상기 무선단말(100)에 구비된 각 구성부와 버스(BUS)를 통해 연결된다. 바람직하게, 상기 프로세서는 ARM 프로세서를 포함할 수 있다.

[0030] 본 발명에 따르면, 상기 제어부(105)는 커널구조와 API 및 드라이버 등이 공개된 일반OS(110)(Normal Operating System)가 운영되는 노멀월드와, 상기 일반OS(110)와 구별되는 보안커널(130)을 구비한 보안OS(120)(Secure Operating System)가 운영되는 시큐어월드를 포함하여 이루어진다. 상기 노멀월드와 시큐어월드는 상호 고립된 구조로 이루어진다. 바람직하게, 상기 보안OS(120)는 ARM 프로세서의 트러스트존(Trust Zone)을 포함한다. 이하, 편의상 상기 일반OS(110)와 보안OS(120) 상에서 본 발명을 위한 기능적 구성을 본 제어부(105)에 도시하여 설명하기로 한다.

[0031] 상기 메모리부(175)는 상기 무선단말(100)에 구비된 저장수단에 대응하는 비휘발성 메모리의 총칭으로서, 상기 제어부(105)를 통해 실행되는 적어도 하나의 프로그램코드와 상기 프로그램코드가 이용하는 적어도 하나의 데이터셋트를 저장하여 유지한다.

[0032] 본 발명에 따르면, 상기 메모리부(175)는 일반OS(110)에서 접근하는 일반OS 저장영역과 보안OS(120)에서 접근하는 보안OS 저장영역을 포함할 수 있으며, 일반OS(110)는 보안OS 저장영역에 접근할 수 없다. 상기 일반OS 저장영역에는 일반OS(110)를 통해 실행되는 애플리케이션에 대응하는 프로그램코드와 상기 일반OS(110)의 애플리케이션이 이용하는 적어도 하나의 데이터셋트를 저장할 수 있다. 한편 상기 보안OS 저장영역에는 보안OS(120)를 통해 실행되는 애플리케이션에 대응하는 프로그램코드와 상기 보안OS(120)의 애플리케이션이 이용하는 적어도 하나의 데이터셋트를 저장할 수 있다.

[0033] 상기 일반OS(110)는 커널구조가 공개된 커널(이하, 보안OS(120)의 보안커널(130)과 대비하여 “일반커널(115)”이라고 함)을 구비하며, 상기 일반OS(110)의 일반커널(115)은 상기 화면출력부(140), 사용자입력부(145), 사운드처리부(150), 근거리 무선 통신부(155), 무선망 통신부(160) 등, 상기 무선단말(100)의 각종 자원에 접근할 수 있으며, 이를 위한 일반OS(110) 상의 드라이버를 구비할 수 있다. 상기 일반OS(110)의 일반커널(115)은 상기 보안OS 저장영역에는 접근할 수 없으며, 상기 일반OS(110)와 보안OS(120)는 상호 고립된다.

[0034] 상기 보안OS(120)는 커널구조가 공개되지 않은 보안커널(130)을 구비하며, 상기 보안OS(120)의 보안커널(130)은 상기 화면출력부(140), 사용자입력부(145), 사운드처리부(150), 근거리 무선 통신부(155), 무선망 통신부(160) 등, 상기 무선단말(100)의 각종 자원에 접근할 수 있으며, 이를 위한 보안OS(120) 상의 드라이버를 구비할 수 있다. 바람직하게, 상기 보안OS(120)의 보안커널(130)은 상기 일반OS 저장영역에 접근할 수 없으며, 상기 보안OS(120)와 일반OS(110)는 상호 고립된다.

[0035] 본 발명의 실시 방법에 따르면, 보안OS 저장영역은 HSM(Hardware Security Module)(135)으로 운영되는 HSM영역을 포함할 수 있다.

[0036] 상기 화면출력부(140)는 상기 무선단말(100)에 구비된 화면출력수단으로서, 바람직하게 LCD(Liquid Crystal Display)와 같은 디스플레이를 포함하거나, 또는 터치입력부를 포함하는 터치스크린을 포함할 수 있다.

[0037] 상기 일반OS(110)의 일반커널(115)은 상기 화면출력부(140)의 디스플레이 내지 터치스크린에 접근하여 제어하기 위한 드라이버를 구비하며, 상기 일반커널(115)이 상기 화면출력부(140)에 접근하여 제어하는 경우 상기 보안

OS(120)는 상기 화면출력부(140)에 접근할 수 없다.

[0038] 상기 보안OS(120)의 보안커널(130)은 상기 화면출력부(140)의 디스플레이 내지 터치스크린에 접근하여 제어하기 위한 별도의 보안 드라이버를 구비하며, 상기 보안커널(130)이 상기 화면출력부(140)에 접근하여 제어하는 경우 상기 일반OS(110)는 상기 화면출력부(140)에 접근할 수 없다.

[0039] 상기 사용자입력부(145)는 상기 무선단말(100)에 구비된 사용자 입력수단으로서, 상기 화면출력부(140)가 터치스크린을 포함하는 경우 상기 터치스크린의 터치입력부를 포함할 수 있으며, 실시 방법에 따라 키패드, 키버튼을 포함할 수 있다.

[0040] 상기 일반OS(110)의 일반커널(115)은 상기 사용자입력부(145)의 터치입력부 내지 키패드나 키버튼에 접근하여 제어하기 위한 드라이버를 구비하며, 상기 일반커널(115)이 상기 사용자입력부(145)에 접근하여 제어하는 경우 상기 보안OS(120)는 상기 사용자입력부(145)에 접근할 수 없다.

[0041] 상기 보안OS(120)의 보안커널(130)은 상기 사용자입력부(145)의 터치입력부 내지 키패드나 키버튼에 접근하여 제어하기 위한 별도의 보안 드라이버를 구비하며, 상기 보안커널(130)이 상기 사용자입력부(145)에 접근하여 제어하는 경우 상기 일반OS(110)는 상기 사용자입력부(145)에 접근할 수 없다.

[0042] 상기 사운드처리부(150)는 상기 무선단말(100)에 구비된 사운드출력수단과 사운드입력수단으로서, 사운드를 출력하는 스피커와 사운드를 입력받는 마이크로폰을 포함할 수 있다.

[0043] 상기 일반OS(110)의 일반커널(115)은 상기 사운드처리부(150)의 스피커 내지 마이크로폰에 접근하여 제어하기 위한 드라이버를 구비하며, 상기 일반커널(115)이 상기 사운드처리부(150)에 접근하여 제어하는 경우 상기 보안OS(120)는 상기 일반OS(110)가 제어하는 사운드처리부(150)에 접근할 수 없다.

[0044] 상기 보안OS(120)의 보안커널(130)은 상기 사운드처리부(150)의 스피커 내지 마이크로폰에 접근하여 제어하기 위한 별도의 보안 드라이버를 구비하며, 상기 보안커널(130)이 상기 사운드처리부(150)에 접근하여 제어하는 경우 상기 일반OS(110)는 상기 보안OS(120)가 제어하는 사운드처리부(150)에 접근할 수 없다.

[0045] 상기 무선망 통신부(160)와 근거리 무선 통신부(155)는 상기 무선단말(100)을 통신망에 접속시키는 통신수단으로서, 바람직하게 상기 무선단말(100)은 무선망 통신부(160)를 기본 통신수단으로 구비할 수 있으며, 하나 이상의 근거리 무선 통신부(155)를 더 구비할 수 있다.

[0046] 상기 무선망 통신부(160)는 상기 무선단말(100)을 기지국을 경유하는 무선 통신망에 접속시키는 통신수단의 총칭으로서, 특정 주파수 대역의 무선 주파수 신호를 송수신하는 안테나, RF모듈, 기저대역모듈, 신호처리모듈을 적어도 하나 포함한다. 상기 무선망 통신부(160)는 상기 무선단말(100)을 교환기를 경유하는 통화채널과 데이터 채널을 포함하는 통화망에 연결할 수 있으며, 경우에 따라 상기 교환기를 경유하지 않고 패킷 통신 기반의 무선망 데이터 통신(예컨대, 인터넷)을 제공하는 데이터망에 연결할 수 있다.

[0047] 본 발명의 실시 방법에 따르면, 상기 무선망 통신부(160)는 CDMA/WCDMA/LTE 규격에 따라 이동 통신망에 접속, 위치등록, 호처리, 통화연결, 데이터통신, 핸드오프를 적어도 하나 수행하는 이동 통신 구성을 포함한다. 한편 당업자의 의도에 따라 상기 무선망 통신부(160)는 IEEE 802.16 관련 규격에 따라 휴대인터넷에 접속, 위치등록,

데이터통신, 핸드오프를 적어도 하나 수행하는 휴대 인터넷 통신 구성을 더 포함할 수 있으며, 상기 무선망 통신부(160)가 제공하는 무선 통신 구성에 의해 본 발명이 한정되지 아니함을 명백히 밝혀두는 바이다. 즉, 상기 무선망 통신부(160)는 무선 구간의 주파수 대역이나 통신망의 종류 또는 프로토콜에 무관하게 셀 기반의 기지국을 통해 무선 통신망에 접속하는 구성부의 총칭이다.

[0048] 상기 일반OS(110)의 일반커널(115)은 상기 무선망 통신부(160)에 접근하여 제어하기 위한 드라이버를 구비하며, 상기 일반커널(115)이 상기 무선망 통신부(160)에 접근하여 제어하는 경우 상기 보안OS(120)는 상기 일반OS(110)가 제어하는 무선망 통신부(160)에 접근할 수 없다.

[0049] 상기 보안OS(120)의 보안커널(130)은 상기 무선망 통신부(160)에 접근하여 제어하기 위한 별도의 보안 드라이버를 구비하며, 상기 보안커널(130)이 상기 무선망 통신부(160)에 접근하여 제어하는 경우 상기 일반OS(110)는 상기 보안OS(120)가 제어하는 무선망 통신부(160)에 접근할 수 없다.

[0050] 상기 근거리 무선 통신부(155)는 일정 거리 이내(예컨대, 10m 내외)에서 무선 주파수 신호를 통신매체로 이용하여 통신세션을 연결하고 이를 기반으로 상기 무선단말(100)을 통신망에 접속시키는 통신수단의 총칭으로서, 바람직하게 와이파이 통신, 블루투스 통신, 공중무선 통신, UWB 중 적어도 하나를 통해 상기 무선단말(100)을 통신망에 접속시킬 수 있다. 본 발명의 실시 방법에 따르면, 상기 근거리 무선 통신부(155)는 무선AP를 통해 상기 무선단말(100)을 패킷 통신 기반의 근거리 무선 데이터 통신을 제공하는 데이터망에 연결할 수 있다.

[0051] 상기 일반OS(110)의 일반커널(115)은 상기 근거리 무선 통신부(155)에 접근하여 제어하기 위한 드라이버를 구비하며, 상기 일반커널(115)이 상기 근거리 무선 통신부(155)에 접근하여 제어하는 경우 상기 보안OS(120)는 상기 일반OS(110)가 제어하는 근거리 무선 통신부(155)에 접근할 수 없다.

[0052] 상기 보안OS(120)의 보안커널(130)은 상기 근거리 무선 통신부(155)에 접근하여 제어하기 위한 별도의 보안 드라이버를 구비하며, 상기 보안커널(130)이 상기 근거리 무선 통신부(155)에 접근하여 제어하는 경우 상기 일반OS(110)는 상기 보안OS(120)가 제어하는 근거리 무선 통신부(155)에 접근할 수 없다.

[0053] 상기 NFC부(170)는 근접 거리(예컨대, 10cm 내외)에서 무선 주파수 신호를 통신매체로 이용하여 양방향 근접 무선 통신, 전이중 근접 무선 통신, 반이중 근접 무선 통신 중 하나 이상의 근접 무선 통신을 처리하는 통신 자원의 총칭으로서, 바람직하게 13.56Mz 주파수 대역의 NFC(Near Field Communication) 규격에 따라 근접 무선 통신을 처리할 수 있다.

[0054] 상기 일반OS(110)의 일반커널(115)은 상기 NFC부(170)에 접근하여 제어하기 위한 드라이버를 구비하며, 상기 일반커널(115)이 상기 NFC부(170)에 접근하여 제어하는 경우 상기 보안OS(120)는 상기 일반OS(110)가 제어하는 NFC부(170)에 접근할 수 없다.

[0055] 상기 보안OS(120)의 보안커널(130)은 상기 NFC부(170)에 접근하여 제어하기 위한 별도의 보안 드라이버를 구비하며, 상기 보안커널(130)이 상기 NFC부(170)에 접근하여 제어하는 경우 상기 일반OS(110)는 상기 보안OS(120)가 제어하는 NFC부(170)에 접근할 수 없다.

[0056] 상기 USIM 리더부(165)는 ISO/IEC 7816 규격을 기반으로 상기 무선단말(100)에 탑재 또는 이탈착되는 범용가입자식별모듈(Universal Subscriber Identity Module)과 적어도 하나의 데이터셋트를 교환하는 구성의 총칭으로서, 상기 데이터셋트는 APDU(Application Protocol Data Unit)를 통해 반이중 통신 방식으로

교환된다.

[0057] 상기 USIM은 상기 ISO/IEC 7816 규격에 따른 IC칩이 구비된 SIM 타입의 카드로서, 상기 USIM 리더부(165)와 연결되는 적어도 하나의 접점을 포함하는 입출력 인터페이스와, 적어도 하나의 IC칩용 프로그램코드와 데이터셋트를 저장하는 IC칩 메모리와, 상기 입출력 인터페이스와 연결되어 상기 무선단말(100)로부터 전달되는 적어도 하나의 명령에 따라 상기 IC칩용 프로그램코드를 연산하거나 상기 데이터셋트를 추출(또는 가공)하여 상기 입출력 인터페이스로 전달하는 프로세서를 포함하여 이루어진다.

[0058] 본 발명에 따르면, 일반OS(110)에는 일반커널(115)을 이용하여 동작하는 각종 애플리케이션이 탑재되며, 사용자는 상기 일반OS(110)에서 실행된 각종 애플리케이션이 상기 일반커널(115)을 통해 제어되는 화면출력부(140)를 통해 하나 이상의 인터페이스 화면을 표시한 상태에서 상기 일반커널(115)을 통해 제어되는 사용자입력부(145)에 의한 사용자 조작을 수행하며, 이를 기반으로 상기 일반OS(110)의 애플리케이션은 지정된 거래 동작을 수행하여 사용자에게 각종 서비스를 제공한다. 이하, 일반OS(110) 상에서 본 발명에 따라 동작하는 애플리케이션(또는 애플리케이션에 내장되거나 연동하는 프로그램모듈)을 편의상 “프로그램(n)(200)”이라고 한다. 바람직하게, 상기 프로그램(n)(200)은 일반OS(110)에서 실행되는 뱅킹 앱(Banking Application)이나 결제 앱(Payment Application) 또는 인증 앱(Certification Application)과 같이 전자서명을 이용하는 애플리케이션을 포함할 수 있다. 그러나 상기 프로그램(n)(200)이 뱅킹 앱이나 결제 앱 또는 인증 앱으로만 한정되는 것은 결코 아니며, 일반OS(110) 상에서 실행되는 애플리케이션이라면 어떠한 애플리케이션이라도 무방하며, 본 발명의 권리범위에 귀속된다.

[0059] 본 발명의 실시 방법에 따르면, 상기 일반OS(110)의 프로그램(n)(200)은 OS 구조 상 일반커널(115)의 상위에 구비되며, 일반커널(115)을 이용하여 동작한다.

[0060] 본 발명에 따르면, 보안OS(120)에는 보안커널(130)을 기반으로 동작하는 적어도 하나의 보안 애플리케이션이 탑재된다. 상기 보안OS(120) 상의 보안 애플리케이션은 보안커널(130)을 이용하여 동작하며, 필요에 따라 상기 무선단말(100)의 화면출력부(140), 사용자입력부(145), 사운드처리부(150), 무선망 통신부(160), 근거리 무선 통신부(155) 등의 제어 권한을 획득하여 이를 이용할 수 있다. 이하, 일반OS(110) 상에서 본 발명에 따라 동작하는 보안 애플리케이션(또는 보안 애플리케이션에 내장되거나 연동하는 프로그램모듈)을 편의상 “프로그램(s)(240)”이라고 한다. 바람직하게, 상기 프로그램(s)(240)은 보안OS(120)에서 실행되는 인증서 앱을 포함할 수 있다.

[0061] 본 발명의 실시 방법에 따르면, 상기 보안OS(120)의 프로그램(s)(240)은 OS 구조 상 보안커널(130)의 상위에 구비되며, 보안커널(130)을 이용하여 동작한다.

[0062] 본 발명의 실시 방법에 따르면, 상기 프로그램(s)(240)은 보안OS(120) 상에서 HSM(135)을 운영하는 프로그램코드를 포함할 수 있다.

[0063] 본 발명의 실시 방법에 따르면, 상기 프로그램(s)(240)은 상기 NFC부(170)를 통해 무선단말(100)의 외부에 구비된 NFC 기반의 HSM(135)과 연동할 수 있다.

[0064] 본 발명에 따르면, 상기 보안OS(120)(또는 일반OS(110)와 보안OS(120) 사이)에는 상기 무선단말(100)의 OS를 일반OS(110)에서 보안OS(120)로 전환하기 위한 일련의 절차를 수행하거나, 또는 보안OS(120)에서 일반OS(110)로 전환하기 위한 일련의 절차를 수행하는 보안 모니터(125)(Secure Monitor)를 구비한다. 상기 보안 모니터(125)는 보안OS(120)의 명령을 사용하므로, 편의상 본 도면1은 상기 보안 모니터(125)가 보안OS(120)에 구비된 것으

로 도시하여 설명하기로 한다.

[0065] 상기 보안 모니터(125)는 커널을 통해 SMC(Secure Monitor Call) 명령이 발생하거나, OS전환에 대응하는 IRQ(Interrupt Request) 내지 FIQ(Fast Interrupt Request)가 발생하는 경우에 무선단말(100)의 OS를 전환하는 절차를 수행할 수 있다.

[0066] 도면2는 본 발명의 실시 방법에 따른 프로그램의 기능 구성을 도시한 도면이다.

[0067] 보다 상세하게 본 도면2는 일반OS(110)의 프로그램(n)(200)과 보안OS(120)의 프로그램(s)(240)의 기능 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면2를 참조 및/또는 변형하여 상기 프로그램의 기능에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면2에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0068] 도면2를 참조하면, 상기 보안OS(120)의 프로그램(s)(240)은, 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 사용자의 인증서를 저장하고 관리하는 인증서 저장부(245)를 구비한다.

[0069] 상기 프로그램(s)(240)은 보안OS(120)에서 실행되어 보안OS(120)에서 이용하는 인증서를 관리하는 프로그램의 총칭으로서, 바람직하게 인증기관을 통해 발급된 사용자의 인증서를 보안OS(120) 상의 지정된 인증서 저장영역에 저장하여 관리하거나, 또는 보안OS(120)에 구현된 HSM(135)에 인증서를 발급하는 절차를 수행할 수 있다.

[0070] 상기 보안OS(120)에 탑재된 프로그램(s)(240)이 최초 1회 이상 실행되면, 상기 인증서 저장부(245)는 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 사용자의 인증서가 구비되어 있는지 확인한다. 만약 상기 인증서 저장영역 또는 HSM(135)에 사용자의 인증서가 저장되지 않은 경우, 상기 인증서 저장부(245)는 지정된 절차에 따라 사용자의 인증서를 발급받거나 또는 복사하여 상기 인증서 저장영역 또는 HSM(135)에 저장할 수 있다.

[0071] 본 발명의 일 실시 방법에 따르면, 인증서 발급 절차의 지정된 단말/서버에서 키 쌍(예컨대, 공개키, 개인키 등)을 생성하여 인증기관으로 제출하면, 인증기관은 상기 키 쌍을 통해 인증서를 생성하여 인증기관에 등록한 후 상기 인증서를 발급하며, 상기 인증서 저장부(245)는 상기 무선단말(100)의 무선망 통신부(160) 또는 근거리 무선 통신부(155)를 통해 상기 인증서를 제공받아 보안OS(120)의 인증서 저장영역에 저장할 수 있다.

[0072] 한편 보안OS(120)에 소프트웨어적으로 구현 HSM(135)이 구현된 경우, 상기 보안OS(120)의 HSM(135)에서 키 쌍을 생성하면, 상기 인증서 저장부(245)는 상기 무선단말(100)의 무선망 통신부(160) 또는 근거리 무선 통신부(155)를 통해 상기 HSM(135)에서 생성한 공개키를 인증기관으로 제출한다. 한편 상기 인증기관은 HSM(135)에 저장된 키를 활용하여 해당 HSM(135)이 특정한 사용자에게 배부된 것임을 확인할 수 있으며, 이를 위해 상기 인증서 저장부(245)는 상기 HSM(135)에 저장된 키를 상기 인증서버로 제공할 수 있다. 상기 HSM(135)에 저장된 키를 이용하여 상기 HSM(135)이 특정 사용자에게 배부된 것임이 확인되면, 상기 인증기관은 인증서를 생성하여 인증기관에 등록한 후 상기 인증서를 발급하며, 상기 인증서 저장부(245)는 상기 무선단말(100)의 무선망 통신부(160) 또는 근거리 무선 통신부(155)를 통해 상기 인증서를 제공받아 보안OS(120)의 HSM(135)에 저장할 수 있다.

[0073] 또는 보안OS(120)에서 무선단말(100)의 NFC부(170)를 통해 외부의 HSM(135)과 연동하는 경우, 상기 NFC부(170)를 통해 연동된 HSM(135)에서 키 쌍을 생성하면, 상기 인증서 저장부(245)는 상기 무선단말(100)의 무선망 통신부(160) 또는 근거리 무선 통신부(155)를 통해 상기 HSM(135)에서 생성한 공개키를 인증기관으로 제출한다. 한편 상기 인증기관은 HSM(135)에 저장된 키를 활용하여 해당 HSM(135)이 특정한 사용자에게 배부된 것임을 확

인할 수 있으며, 이를 위해 상기 인증서 저장부(245)는 상기 HSM(135)에 저장된 키를 상기 인증서버로 제공할 수 있다. 상기 HSM(135)에 저장된 키를 이용하여 상기 HSM(135)이 특정 사용자에게 배부된 것임이 확인되면, 상기 인증기관은 인증서를 생성하여 인증기관에 등록한 후 상기 인증서를 발급하며, 상기 인증서 저장부(245)는 상기 무선단말(100)의 무선망 통신부(160) 또는 근거리 무선 통신부(155)를 통해 상기 인증서를 제공받아 상기 NFC부(170)를 통해 상기 HSM(135)에 저장할 수 있다.

[0074] 한편 인증기관을 통해 사용자의 인증서가 기 발급된 경우, 상기 인증서 저장부(245)는 지정된 인증서 복사 절차를 수행하여 사용자에게 기 발급된 인증서를 상기 보안OS(120)의 인증서 저장영역 또는 보안OS(120)에 구현된 HSM(135) 또는 NFC부(170)를 통해 연동하는 HSM(135)으로 복사하여 저장하는 절차를 수행할 수 있다. 이 때 상기 인증서 저장부(245)는 상기 HSM(135)에 저장된 키를 상기 인증서버로 제공할 수 있다. 상기 인증기관에서 상기 HSM(135)에 저장된 키를 이용하여 상기 HSM(135)이 특정 사용자에게 배부된 것임을 확인한 경우, 상기 인증서 저장부(245)는 상기 인증된 HSM(135)으로 사용자에게 기 발급된 인증서를 복사하여 저장할 수 있다. 이하, 편의상 상기 보안OS(120)에 구현된 HSM(135) 또는 NFC부(170)를 통해 연동하는 HSM(135)을 통칭하여 “HSM(135)”이라고 한다.

[0075] 도면2를 참조하면, 상기 보안OS(120)의 프로그램(s)(240)은, 보안OS(120) 상에서 인증서를 이용한 전자서명을 위한 PIN(Personal Identification Number) 인증을 수행하기 위한 PIN 정보를 등록하는 PIN 등록부(250)를 구비한다.

[0076] 상기 보안OS(120)에 탑재된 프로그램(s)(240)이 최초 1회 이상 실행되면, 상기 PIN 등록부(250)는 보안OS 저장영역 상의 지정된 PIN 저장영역에 전자서명을 위한 PIN 정보가 저장되어 있는지 확인한다. 만약 상기 PIN 저장영역에 PIN 정보가 저장되지 않은 경우, 상기 PIN 등록부(250)는 지정된 절차에 따라 상기 화면출력부(140)와 사용자입력부(145)의 접근 권한을 획득하여 상기 화면출력부(140)에 PIN 등록을 위한 인터페이스를 표시하고, 상기 사용자입력부(145)를 통해 PIN 정보를 입력받아 상기 PIN 저장영역에 저장한다. 바람직하게, 상기 PIN 등록부(250)는 상기 PIN 정보를 지정된 암호화 방식에 따라 암호화하여 상기 PIN 저장영역에 저장할 수 있다. 일반OS(110)는 상기 PIN 저장영역에 접근할 수 없다.

[0077] 도면2를 참조하면, 상기 일반OS(110)의 프로그램(n)(200)은, 지정된 동작을 수행하는 중에 사용자의 인증서를 이용하여 전자서명할 서명대상정보를 확인하는 정보 확인부(205)와, 상기 서명대상정보를 확인 시 일반커널(115)을 통해 보안OS(120)로 전환하는 일련의 절차를 수행하며, 상기 보안OS(120)의 지정된 프로그램(s)(240)에서 접근 가능한 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인하고, 상기 확인된 서명대상정보를 상기 메모리영역으로 제공하는 연동 절차부(210)를 구비한다. 한편 본 발명의 다른 실시 방법에 따르면, 상기 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인 절차는 보안OS(120)의 프로그램(s)(240)을 통해 수행될 수 있으며, 본 발명은 프로그램(s)(240)에서 상기 메모리영역을 할당/확인하는 구성을 권리범위로 포함할 수 있음을 명백하게 밝혀두는 바이다.

[0078] 상기 프로그램(n)(200)은 일반OS(110)에서 실행되어 뱅킹, 결제, 인증 중 적어도 하나의 지정된 동작을 수행하며, 상기 정보 확인부(205)는 상기 지정된 동작을 수행하는 중에 사용자의 인증서를 이용하여 전자서명할 서명대상정보를 확인한다. 상기 서명대상정보는 인증서 로그인을 위한 인증정보, 사용자 인증을 위한 인증정보, 상기 일반OS(110)의 프로그램(n)(200)을 통해 수행되는 거래 동작에 대응하는 거래의 부인을 방지하기 위한 거래정보 중 적어도 하나를 포함할 수 있다.

[0079] 본 발명의 제1 서명대상 확인 방식에 따르면, 상기 정보 확인부(205)는 상기 무선단말(100)의 통신수단을 통해 지정된 서버로부터 서명대상정보를 수신할 수 있다. 예를들어, 상기 프로그램(n)(200)이 뱅킹 앱인 경우, 상기 정보 확인부(205)는 지정된 뱅킹서버로부터 상기 뱅킹 앱을 통한 뱅킹거래에 대응하는 거래정보를 포함하는 서명대상정보를 수신할 수 있다. 또는 상기 프로그램(n)(200)이 결제 앱인 경우, 상기 정보 확인부(205)는 지정된

결제서버로부터 상기 결제 앱을 통한 지불결제할 결제정보를 포함하는 서명대상정보를 수신할 수 있다. 또는 상기 프로그램(n)(200)이 인증 앱인 경우, 상기 정보 확인부(205)는 지정된 인증서버로부터 상기 인증 앱을 통한 인증을 위한 인증정보를 포함하는 서명대상정보를 수신할 수 있다.

[0080] 본 발명의 제2 서명대상 확인 방식에 따르면, 상기 정보 확인부(205)는 상기 프로그램(n)(200)의 지정된 동작 중에 서명대상정보를 생성할 수 있다. 예를들어, 상기 프로그램(n)(200)이 뱅킹 앱인 경우, 상기 정보 확인부(205)는 상기 뱅킹 앱을 통해 입력된 거래정보를 포함하는 서명대상정보를 생성할 수 있다. 또는 상기 프로그램(n)(200)이 결제 앱인 경우, 상기 정보 확인부(205)는 결제 앱을 통해 입력된 결제정보를 포함하는 서명대상정보를 생성할 수 있다. 또는 상기 프로그램(n)(200)이 인증 앱인 경우, 상기 정보 확인부(205)는 인증 절차에 이용될 인증정보(예컨대, 무선단말(100)의 MIN, IMSI, IMEI 등)를 포함하는 서명대상정보를 생성할 수 있다.

[0081] 본 발명의 제3 서명대상 확인 방식에 따르면, 상기 정보 확인부(205)는 상기 제1 내지 제2 서명대상 확인 방식을 적어도 둘 조합하여 서명대상정보를 확인할 수 있다. 예를들어, 상기 서명대상정보 중 일부는 지정된 서버로부터 수신되고 다른 일부는 프로그램(n)(200)의 지정된 동작 중에 생성될 수 있다.

[0082] 상기 연동 절차부(210)는 상기 일반OS(110)에 상기 프로그램(n)(200)이 탑재되어 적어도 최초 1회 실행 시, 상기 무선단말(100)에 보안OS(120)가 탑재되어 있는지 확인하며, 상기 무선단말(100)에 보안OS(120)가 탑재된 경우 상기 보안OS(120)에 사용자의 인증서를 관리하고 전자서명을 처리하는 프로그램(s)(240)을 탑재하기 위한 일련의 절차를 수행할 수 있다. 만약 상기 보안OS(120)에 사용자의 인증서를 관리하고 전자서명을 처리하는 프로그램(s)(240)이 탑재된 경우, 상기 연동 절차부(210)는 상기 보안OS(120)에 상기 프로그램(s)(240)이 탑재되었음을 식별하는 정보 및/또는 상기 보안OS(120)에 탑재된 프로그램(s)(240)을 식별하는 정보 중 적어도 하나의 식별정보를 일반OS 저장영역에 저장하여 유지할 수 있다.

[0083] 상기 정보 확인부(205)를 통해 서명대상정보를 확인한 경우, 상기 연동 절차부(210)는 상기 식별정보를 근거로 상기 보안OS(120)에 상기 프로그램(s)(240)이 탑재되어 있음을 확인하거나 및/또는 상기 보안OS(120)에 탑재된 프로그램(s)(240)을 확인한다.

[0084] 상기 서명대상정보를 확인하거나 및/또는 상기 식별정보를 통해 상기 보안OS(120)의 프로그램(s)(240)을 확인한 경우, 상기 연동 절차부(210)는 일반커널(115)을 통해 상기 보안OS(120)로 전환하기 직전의 프로그램(n)(200)에 대한 상태정보를 유지시킨다. 바람직하게, 상기 연동 절차부(210)는 무선단말(100)의 OS를 일반OS(110)에서 보안OS(120)로 전환하는 시점에 일반커널(115)을 통해 상기 사용자의 인증서를 관리하고 전자서명을 처리하는 프로그램(s)(240)의 상태정보를 일반OS 저장영역에 저장함으로써, 상기 무선단말(100)의 OS가 일반OS(110)에서 보안OS(120)로 전환된 후 다시 보안OS(120)에서 일반OS(110)로 전환되는 경우에 상기 프로그램(n)(200)의 상태(예컨대, 프로그램(n)(200)의 인터페이스 화면 상태, 프로그램(n)(200)의 통신세션 상태 등)를 유지하도록 할 수 있다.

[0085] 본 발명의 실시 방법에 따르면, 상기 연동 절차부(210)는 일반커널(115)을 통해 상기 보안OS(120)로 전환 직전(예컨대, SMC 명령을 통해 보안OS(120)를 구동하기 직전)의 프로그램(n)(200)의 상태정보를 유지시킴으로써, 상기 일반OS(110)를 보안OS(120)로 전환하는 과정에서 상기 프로그램(n)(200)이 초기화되거나 및/또는 상기 일반OS(110)를 보안OS(120)로 전환 절차 중에 페이지폴트가 발생하는 등의 예외상황이 발생하더라도, 상기 무선단말(100)의 OS를 보안OS(120)에서 일반OS(110)로 전환하는 시점에 상기 상태정보를 이용하여 상기 프로그램(n)(200)의 상태를 상기 보안OS(120)로 전환 직전의 상태로 복원할 수 있다.

[0086] 상기 서명대상정보를 확인하거나 및/또는 상기 보안OS(120)의 프로그램(s)(240)을 확인하거나 및/또는 상기 프로그램(n)(200)의 상태정보를 저장한 경우, 상기 연동 절차부(210)는 일반커널(115)을 통해 보안OS(120)를 구동

하는 SMC 명령을 발생시킨다. 상기 보안 모니터(125)는 상기 SMC 명령의 유효성을 검증하고, 검증 성공한 경우에 SMC 명령에 따라 보안OS(120)를 구동하는 절차를 수행한다.

[0087] 한편 상기 보안OS(120)의 구동을 개시하기 전, 중, 직후의 어느 지정된 일 시점에, 상기 연동 절차부(210)는 상기 프로그램(n)(200)에서 접근 가능하면서 상기 보안OS(120)의 지정된 프로그램(s)(240)에서 접근 가능한 메모리영역을 할당하거나, 또는 기 할당된 메모리영역을 확인한다. 예를들어, 상기 할당되는 메모리영역은 일반OS(110)의 프로그램(n)(200)과 보안OS(120)의 프로그램(s)(240) 사이의 프로세스 간 통신을 위한 공유메모리를 포함할 수 있다. 통상의 공유메모리가 동일한 OS 내의 프로세스 간 통신을 위해 해당 OS 내에 할당되는 반면, 본원의 메모리영역은 일반OS(110)와 보안OS(120)를 포함하는 이종의 OS에서 실행된 이종의 프로세스 간 통신을 제공하기 위한 공유메모리라는 점에서 기술적 특징을 지닌다.

[0088] 본 발명의 제1 메모리영역 할당 실시 방식에 따르면, 상기 연동 절차부(210)는 일반OS(110) 상에 상기 메모리영역을 할당하거나, 또는 상기 일반OS(110) 상에 할당된 메모리영역을 확인할 수 있다. 이 경우 상기 보안 모니터(125)는 상기 일반OS(110)의 메모리영역에 접근하거나 모니터링할 수 있으며, 상기 보안OS(120)의 프로그램(s)(240)은 보안 모니터(125)를 통해 상기 일반OS(110)의 메모리영역에 간접적으로 접근(또는 참조 접근)할 수 있다.

[0089] 본 발명의 제2 메모리영역 할당 실시 방식에 따르면, 상기 연동 절차부(210)는 보안 모니터(125) 상에 상기 메모리영역을 할당하거나, 또는 상기 보안 모니터(125)에 할당된 메모리영역을 확인할 수 있다. 이 경우 상기 연동 절차부(210)는 SMC 명령을 통해 상기 보안 모니터(125)에 상기 메모리영역을 할당하거나 또는 상기 보안 모니터(125)에 할당된 메모리영역을 확인할 수 있다.

[0090] 본 발명의 제3 메모리영역 할당 실시 방식에 따르면, 상기 연동 절차부(210)는 상기 프로그램(n)(200)에서 접근(또는 접속) 가능하며 또한 보안OS(120)의 프로그램(s)(240)에서 접근(또는 접속) 가능한 네트워크 상의 보안서버에 상기 메모리영역을 할당하거나, 또는 상기 보안서버에 할당된 메모리영역을 확인할 수 있다. 상기 메모리영역이 네트워크 상의 보안서버에 할당되는 경우, 상기 일반OS(110)의 프로그램(n)(200)과 보안OS(120)의 프로그램(s)(240)은 각기 상기 보안서버와 통신하여 상기 메모리영역에 주고받을 데이터를 읽거나 쓸 수 있다.

[0091] 상기 연동 절차부(210)는 상기 할당된 메모리영역을 참조하는 일반OS(110) 측의 프로세스로 상기 프로그램(n)(200)을 설정할 수 있다. 바람직하게, 상기 연동 절차부(210)는 상기 메모리영역에 상기 프로그램(n)(200)의 PID(Process ID)를 제공함으로써, 상기 보안OS(120)의 프로그램(s)(240)이 동작한 후 상기 프로그램(s)(240)이 상기 할당된 메모리영역에 기록한 데이터를 읽어올 일반OS(110) 측의 프로세스로서 상기 프로그램(n)(200)을 설정할 수 있다.

[0092] 상기 제1 내지 3 메모리영역 할당 실시 방식 중 적어도 하나를 통해 상기 보안OS(120)의 프로그램(s)(240)에서 접근 가능한 메모리영역이 할당되거나 또는 기 할당된 메모리영역이 확인된 경우, 상기 연동 절차부(210)는 상기 보안OS(120)에서 상기 할당된 메모리영역에 접근 가능한 프로세스로서 지정된 프로그램(s)(240)을 설정할 수 있다. 예를들어, 상기 연동 절차부(210)는 상기 할당된 메모리영역의 주소 정보(예컨대, RAM 상의 메모리주소, 또는 프로세서에 구비된 RAM의 메모리주소, 또는 상기 메모리영역이 네트워크 상에 할당된 경우 상기 메모리영역을 식별하는 네트워크 주소(및/또는 식별 값) 등)를 확인하고, 상기 보안 모니터(125)를 통해 상기 보안OS(120)의 프로그램(s)(240)이 사용하는 가상의 메모리 주소 공간으로 매핑할 수 있다.

[0093] 상기 보안OS(120)의 프로그램(s)(240)에서 접근 가능한 메모리영역이 할당/확인되거나 및/또는 상기 메모리영역을 상기 보안OS(120)의 프로그램(s)(240)에서 접근 가능하게 설정한 경우, 상기 연동 절차부(210)는 상기 보안 모니터(125)와 연동하여 상기 일반OS(110)의 프로세스 중 상기 프로그램(n)(200)을 제외한 다른 프로세스에서

상기 메모리영역에 접근하지 못하도록 설정할 수 있다. 바람직하게, 상기 연동 절차부(210)는 상기 보안 모니터(125)의 메모리 접근 제어 기능을 이용하여 상기 일반OS(110)의 프로세스 중 상기 프로그램(n)(200)을 제외한 다른 프로세스에서 상기 메모리영역에 접근하지 못하도록 설정할 수 있다.

[0094] 한편 상기 제1 내지 3 메모리영역 할당 실시 방식 중 적어도 하나를 통해 상기 보안OS(120)의 프로그램(s)(240)에서 접근 가능한 메모리영역이 할당되거나 또는 기 할당된 메모리영역이 확인되거나, 및/또는 상기 메모리영역의 접근 제어 절차가 수행된 경우, 상기 연동 절차부(210)는 상기 정보 확인부(205)를 통해 확인된 서명대상정보를 상기 메모리영역으로 제공함으로써, 상기 보안OS(120)의 프로그램(s)(240)이 사용자의 인증서를 이용하여 상기 서명대상정보를 전자서명하게 처리한다.

[0095] 상기 SMC 명령에 의해 보안OS(120)가 구동되고 상기 보안OS(120)의 프로그램(s)(240)이 실행되면, 상기 할당/확인된 메모리영역의 접근 권한은 상기 보안 모니터(125)에 의해 상기 보안OS(120)의 지정된 프로그램(s)(240)에게 부여된다.

[0096] 도면2를 참조하면, 상기 보안OS(120)의 프로그램(s)(240)은, 상기 제1 내지 3 메모리영역 할당 실시 방식 중 적어도 하나를 통해 할당된 메모리영역을 확인하고 상기 메모리영역을 참조하기 위한 절차를 수행하는 연동 처리부(255)를 구비한다.

[0097] 상기 보안OS(120)가 구동되고 상기 보안OS(120)의 프로그램(s)(240)이 실행되면, 상기 연동 처리부(255)는 상기 보안 모니터(125)를 통해 수행되는 동작 절차와 연동하여 상기 제1 내지 3 메모리영역 할당 실시 방식 중 적어도 하나를 통해 할당된 메모리영역을 확인하고, 상기 프로그램(s)(240)에서 상기 메모리영역에 접근하기 위한 일련의 절차를 수행한다. 바람직하게, 상기 연동 처리부(255)는 상기 메모리영역에 대한 접근 권한을 획득하는 절차를 수행할 수 있다.

[0098] 한편 상기 연동 처리부(255)는 프로그램(s)(240)에서 상기 메모리영역을 참조하기 전에 언제라도 상기 메모리영역을 확인할 수 있으며, 상기 연동 처리부(255)가 상기 메모리영역을 확인하는 특정한 시점에 의해 본 발명이 한정되지 아니한다.

[0099] 도면2를 참조하면, 상기 보안OS(120)의 프로그램(s)(240)은, 상기 PIN 등록부(250)를 통해 보안OS(120)의 지정된 PIN 저장영역에 사용자의 PIN 정보가 저장된 경우, 상기 무선단말(100)의 입력수단을 통해 PIN 정보를 입력받아 유효성을 인증하는 PIN 인증부(260)를 구비할 수 있다.

[0100] 상기 보안OS(120)가 구동되고 상기 보안OS(120)의 프로그램(s)(240)이 실행되면, 상기 PIN 인증부(260)는 지정된 절차에 따라 상기 화면출력부(140)와 사용자입력부(145)의 접근 권한을 획득하여 상기 화면출력부(140)에 PIN 인증을 위한 인터페이스를 표시하고, 상기 사용자입력부(145)를 통해 PIN 정보를 입력받은 후, 상기 PIN 저장영역에 저장된 PIN 정보와 비교(또는 검증 연산)을 수행하여 상기 입력된 PIN 정보의 유효성을 인증할 수 있다.

[0101] 도면2를 참조하면, 상기 보안OS(120)의 프로그램(s)(240)은, 상기 프로그램(n)(200)과 공유된 메모리영역으로부터 서명대상정보를 확인하는 정보 연동부(265)와, 상기 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 구비된 사용자의 인증서를 확인하는 인증서 확인부(270)와, 상기 인증서로부터 서명키를 추출하는 서명키 추출부(275)와, 상기 서명키를 이용하여 상기 서명대상정보의 전자서명 값을 생성하는 전자서명부(280)와, 상기 생성된 전자서명 값을 상기 메모리영역으로 제공하는 전자서명 제공부(290)를 구비하며, 상기 전자서명 값을 암호화하는 암호 처리부(285)를 구비할 수 있다. 한편 실시 방법에 따라 사용자의 인증서가 HSM(135)에 구비된 경우, 상기

서명키 추출부(275)와 전자서명부(280)는 상기 HSM(135) 내에 구비될 수 있다.

[0102] 상기 보안OS(120)가 구동되고 상기 보안OS(120)의 프로그램(s)(240)이 실행되거나 및/또는 상기 PIN 인증이 성공한 경우, 상기 정보 연동부(265)는 상기 연동 처리부(255)와 연계하여 상기 일반OS(110)의 프로그램(n)(200)과 공유된 메모리영역으로부터 상기 일반OS(110)의 거래 동작에 대응하는 서명대상정보를 확인한다.

[0103] 상기 보안OS(120)가 구동되고 상기 보안OS(120)의 프로그램(s)(240)이 실행되거나 및/또는 상기 PIN 인증이 성공한 경우, 상기 인증서 확인부(270)는 상기 인증서 저장부(245)를 통해 상기 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 저장된 사용자의 인증서를 확인한다.

[0104] 상기 인증서 확인부(270)를 통해 상기 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 구비된 사용자의 인증서가 확인되고, 실시 방법에 따라 상기 PIN 인증이 성공한 경우, 보안OS(120) 상에서 상기 사용자의 인증서를 이용한 서명 절차가 수행된다. 만약 HSM(135)에 사용자의 인증서가 구비되고 상기 인증서를 이용한 서명 절차가 HSM(135)을 통해 수행되는 경우, 상기 인증서 확인부(270)는 상기 HSM(135)으로 상기 서명대상정보를 제공할 수 있다.

[0105] 상기 서명키 추출부(275) 또는 HSM(135)은 상기 PIN 인증 결과를 근거로 상기 사용자의 인증서로부터 서명키(예컨대, 사용자 개인키 등)를 추출하고, 상기 전자서명부(280) 또는 HSM(135)은 상기 서명키를 통해 상기 서명대상정보를 전자서명하여 전자서명 값을 생성한다.

[0106] 상기 전자서명 값이 생성되면, 상기 전자서명 제공부(290)는 상기 연동 처리부(255)를 통해 확인된 메모리영역으로 상기 전자서명 값을 제공하며, 상기 보안 모니터(125)는 지정된 절차에 따라 상기 무선단말(100)의 OS를 상기 보안OS(120)에서 일반OS(110)로 전환시킨다. 바람직하게, 상기 전자서명 제공부(290)는 상기 일반OS(110)의 프로그램(n)(200)을 통해 상기 전자서명 값을 읽어가거나 또는 참조할 수 있도록 상기 메모리영역에 상기 전자서명 값을 기록할 수 있다.

[0107] 한편 상기 전자서명 값이 생성된 경우, 상기 암호 처리부(285)는 지정된 암호방식에 따라 상기 전자서명 값을 암호화(예컨대, 사용자 공개키를 통해 암호화)하며, 상기 전자서명 제공부(290)는 상기 연동 처리부(255)를 통해 확인된 메모리영역으로 상기 암호화된 전자서명 값을 제공할 수 있다. 상기 전자서명 값은 상기 일반OS(110)의 프로그램(n)(200)을 통해 복호화 가능하게 암호화되거나, 또는 상기 전자서명 값을 인증하는 지정된 서버를 통해 복호화되게 암호화될 수 있다.

[0108] 본 발명의 다른 실시 방법에 따르면, 상기 전자서명부(280)는 상기 서명키를 통해 상기 서명대상정보를 전자서명하여 생성한 전자서명 값을 포함하는 서명데이터(예컨대, 전자서명 값과 서명대상정보의 조합)를 생성하고, 상기 전자서명 제공부(290)는 상기 메모리영역으로 상기 서명데이터를 제공할 수 있으며, 실시 방법에 따라 상기 암호 처리부(285)를 통해 상기 서명데이터를 암호화하여 상기 메모리영역으로 제공할 수 있다.

[0109] 본 발명의 실시 방법에 따라 상기 무선단말(100)의 OS가 상기 일반OS(110)로 전환되면, 상기 프로그램(n)(200)의 연동 절차부(210)는 상기 메모리영역의 접근 권한을 획득하고(또는 기 획득된 권한을 근거로) 상기 메모리영역에 접근한다. 한편 상기 프로그램(n)(200)의 연동 절차부(210)는 상기 상태정보를 이용하여 상기 보안OS(120)로 전환되기 직전의 프로그램(n)(200)의 상태를 복원할 수 있다.

[0110] 도면2를 참조하면, 상기 일반OS(110)의 프로그램(n)(200)은, 상기 메모리영역을 참조하여 보안OS(120)의 프로그

램(s)(240)에서 제공한 전자서명 값을 확인하는 전자서명 확인부(215)와, 상기 전자서명 값을 포함하는 서명데이터를 지정된 서버로 전송하거나, 또는 상기 프로그램(n)(200)의 동작에 상기 전자서명 값을 이용하는 전자서명 이용부(225)를 구비하며, 상기 전자서명 값을 포함하는 서명데이터를 생성하는 데이터 생성부(220)를 구비할 수 있다.

[0111] 상기 무선단말(100)의 OS가 일반OS(110)로 전환되면, 상기 전자서명 확인부(215)는 상기 연동 절차부(210)와 연동하여 상기 메모리영역을 참조함으로써, 상기 보안OS(120)의 프로그램(s)(240)이 상기 메모리영역으로 제공한 전자서명 값을 확인한다. 만약 상기 보안OS(120)의 프로그램(s)(240)에서 상기 전자서명 값을 포함하는 서명데이터를 생성하여 제공한 경우, 상기 전자서명 확인부(215)는 상기 메모리영역으로부터 상기 전자서명 값을 포함하는 서명데이터를 확인할 수 있다. 만약 상기 보안OS(120)의 프로그램(s)(240)에서 제공한 전자서명 값(또는 서명데이터)이 상기 프로그램(n)(200)을 통해 복호화되게 암호화된 경우, 상기 전자서명 확인부(215)는 상기 암호화된 전자서명 값(또는 서명데이터)를 복호화 처리할 수 있다.

[0112] 한편 상기 전자서명 확인부(215)를 통해 전자서명 값이 확인된 경우, 상기 데이터 생성부(220)는 상기 전자서명 값을 포함하는 서명데이터(예컨대, 전자서명 값과 서명대상정보의 조합)를 생성할 수 있다. 만약 상기 보안OS(120)의 프로그램(s)(240)에서 상기 전자서명 값을 포함하는 서명데이터를 제공한다면, 상기 데이터 생성부(220)는 생략 가능하다.

[0113] 상기 전자서명 이용부(225)는 상기 무선단말(100)의 통신수단을 통해 지정된 서버로 상기 서명데이터를 전송하거나, 또는 상기 프로그램(n)(200)의 지정된 동작에 상기 서명데이터가 이용되도록 처리함으로써, 상기 프로그램(n)(200)을 이용한 각종 인증서 기반 서비스(예컨대, 뱅킹, 결제, 인증 등)가 제공되도록 처리한다. 만약 상기 서명데이터가 상기 보안OS(120)의 프로그램(s)(240)를 통해 생성되어 지정된 서버를 통해 복호화되게 암호화된 경우, 상기 전자서명 이용부(225)는 상기 무선단말(100)의 통신수단을 통해 상기 암호화된 서명데이터를 상기 서버로 전송할 수 있다.

[0114] 도면3은 본 발명의 실시 방법에 따라 보안OS(120)에 프로그램(s)(240)을 준비하는 과정을 도시한 도면이다.

[0115] 보다 상세하게 본 도면3은 보안OS(120)에 프로그램(s)(240)을 탑재하고 사용자의 인증서를 저장하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면3을 참조 및/또는 변형하여 상기 프로그램(s)(240)을 준비하는 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면3에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0116] 도면3을 참조하면, 일반OS(110)의 프로그램(n)(200)은 자신이 탑재된 무선단말(100)의 기종(또는 프로세서의 종류)을 기반으로 무선단말(100)에 보안OS(120)(트러스트존)이 탑재되어 있는지 확인한다(300). 만약 상기 무선단말(100)에 보안OS(120)가 탑재되어 있다면, 상기 프로그램(n)(200)은 상기 보안OS(120)에 지정된 프로그램(s)(240)을 탑재하기 위한 절차를 수행한다(305).

[0117] 지정된 절차에 따라 상기 보안OS(120)에 프로그램(s)(240)이 탑재되고 실행되며(310), 상기 프로그램(s)(240)은 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 사용자의 인증서가 구비되어 있는지 확인한다(315). 만약 상기 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 구비된 사용자의 인증서가 확인되지 않으면, 상기 프로그램(s)(240)은 상기 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 사용자의 인증서를 발급하거나 또는 기 발급된 사용자의 인증서를 상기 보안OS(120)의 인증서 저장영역 또는 HSM(135)으로 복사하는 절차를 수행한다(320).

[0118] 만약 상기 인증서의 발급/복사 절차가 완료되면, 상기 프로그램(s)(240)은 상기 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 사용자의 인증서를 저장하고(325), 상기 보안OS(120)의 PIN 저장영역 또는 HSM(135)에 PIN 정보를 등록하는 절차를 수행하며, 그 결과로서 기 보안OS(120)의 PIN 저장영역 또는 HSM(135)에 PIN 정보를 저장할 수 있다(330).

[0119] 상기 보안OS(120)에 상기 프로그램(s)(240)이 탑재되면, 상기 일반OS(110)의 프로그램(n)(200)은 상기 보안OS(120)에 상기 프로그램(s)(240)이 탑재되었음을 식별하는 정보 및/또는 상기 보안OS(120)에 탑재된 프로그램(s)(240)을 식별하는 정보 중 적어도 하나의 식별정보를 저장한다(335).

[0120] 도면4는 본 발명의 실시 방법에 따라 일반OS(110)와 보안OS(120) 간 거래 연동 과정을 도시한 도면이다.

[0121] 보다 상세하게 본 도면4는 일반OS(110)의 프로그램(n)(200)이 지정된 동작을 수행하는 중에 서명대상정보를 확인한 경우에 보안OS(120)의 프로그램(s)(240)으로 서명대상정보를 제공하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면4를 참조 및/또는 변형하여 상기 일반OS(110)와 보안OS(120) 간 연동 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면4에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0122] 도면4를 참조하면, 일반OS(110)의 프로그램(n)(200)은 내부에 구현된 지정된 동작을 수행하며(400), 상기 지정된 동작 중에 사용자의 인증서를 이용하여 전자서명할 서명대상정보를 확인한다(405). 만약 상기 서명대상정보를 확인한 경우, 상기 프로그램(n)(200)은 식별정보를 이용하여 상기 무선단말(100)의 보안OS(120) 측에 사용자의 인증서를 관리하고 전자서명을 처리하는 프로그램(s)(240)이 탑재되어 있는지 확인한다(410). 상기 보안OS(120)에 상기 프로그램(s)(240)이 탑재되지 않은 경우, 상기 프로그램(n)(200)은 상기 보안OS(120)에 프로그램(s)(240)을 탑재하기 위한 절차를 수행할 수 있다.

[0123] 한편 상기 보안OS(120)에 상기 프로그램(s)(240)이 탑재된 경우, 상기 프로그램(n)(200)은 보안OS(120)로 전환 전에 상기 프로그램(n)(200)의 상태정보를 저장하여 유지시키며(415), 상기 무선단말(100)의 OS를 보안OS(120)로 전환 개시하여 상기 보안OS(120)의 프로그램(s)(240)에서 접근 가능한 메모리영역을 할당하거나 또는 기 할당된 메모리영역을 확인한다(420). 만약 상기 메모리영역이 할당/확인되면, 상기 프로그램(n)(200)은 상기 할당/확인된 메모리영역에 대한 프로그램(n)(200)의 접근 권한을 설정함과 동시에 상기 보안OS(120)에서 상기 프로그램(s)(240)이 상기 메모리영역에 접근하도록 설정하는 과정을 수행하면서(425), 상기 메모리영역으로 상기 확인된 서명대상정보를 제공하고(430), 보안 모니터(125)를 통해 상기 무선단말(100)의 OS가 상기 보안OS(120)로 전환되도록 처리한다(435).

[0124] 상기 무선단말(100)의 OS가 보안OS(120)로 전환되어 상기 프로그램(s)(240)이 실행되면(440), 상기 프로그램(s)(240)은 상기 도면3에 도시된 과정을 통해 보안OS(120)의 PIN 저장영역에 PIN 정보가 등록되어 있는지 확인하여 등록된 경우에 무선단말(100)의 화면출력부(140)와 사용자입력부(145)에 대한 접근 권한을 획득하여 PIN 정보를 입력하는 인터페이스를 출력하고 상기 인터페이스를 통해 입력된 PIN 정보를 확인한다(445). 만약 상기 PIN 정보가 입력되면, 상기 프로그램(s)(240)은 상기 PIN 저장영역에 저장된 PIN 정보를 통해 상기 입력된 PIN 정보의 유효성을 인증하며(450), 상기 PIN 정보의 유효성이 인증되지 않는 경우에 상기 프로그램(s)(240)은 상기 무선단말(100)의 OS를 일반OS(110)로 전환하도록 처리하며(455), 상기 무선단말(100)의 OS가 일반OS(110)로 전환된 경우에 상기 일반OS(110)의 프로그램(n)(200)은 상기 보안OS(120)로 전환 전 상기 프로그램(n)(200)의 상태를 복원한다(460).

[0125] 한편 상기 PIN 정보의 유효성이 인증된 경우, 상기 프로그램(s)(240)은 상기 프로그램(n)(200)을 통해 할당되어

상기 프로그램(n)(200)과 공유 접근 가능한 메모리영역을 확인한다(465). 실시 방법에 따라 상기 메모리영역은 상기 프로그램(s)(240)을 통해 할당 가능하며, 본 발명이 상기 프로그램(s)(240)이 상기 메모리영역을 할당하는 실시예도 포함할 수 있다. 만약 상기 프로그램(s)(240)에서 접근 가능한 메모리영역이 확인되지 않으면, 상기 프로그램(s)(240)은 상기 무선단말(100)의 OS를 일반OS(110)로 전환하도록 처리하며(455), 상기 무선단말(100)의 OS가 일반OS(110)로 전환된 경우에 상기 일반OS(110)의 프로그램(n)(200)은 상기 보안OS(120)로 전환 전 상기 프로그램(n)(200)의 상태를 복원한다(460).

[0126] 한편 상기 프로그램(s)(240)에서 접근 가능한 메모리영역이 확인되면, 상기 프로그램(s)(240)은 상기 메모리영역에 대한 접근 권한을 확인한다(470). 만약 상기 메모리영역에 대한 접근 권한이 확인되지 않으면, 상기 프로그램(s)(240)은 상기 무선단말(100)의 OS를 일반OS(110)로 전환하도록 처리하며(455), 상기 무선단말(100)의 OS가 일반OS(110)로 전환된 경우에 상기 일반OS(110)의 프로그램(n)(200)은 상기 보안OS(120)로 전환 전 상기 프로그램(n)(200)의 상태를 복원한다(460).

[0127] 도면5는 본 발명의 실시 방법에 따라 보안OS(120)를 통해 전자서명을 생성하여 일반OS(110)를 통해 이용하는 과정을 도시한 도면이다.

[0128] 보다 상세하게 본 도면5는 보안OS(120)의 프로그램(s)(240)에서 서명대상정보를 전자서명하여 제공하면 일반OS(110)의 프로그램(n)(200)에서 상기 전자서명을 이용하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면5를 참조 및/또는 변형하여 상기 보안OS(120)를 통해 전자서명을 생성하여 일반OS(110)를 통해 이용하는 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면5에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0129] 도면5를 참조하면, 상기 도면4에 도시된 과정을 통해 보안OS(120)의 프로그램(s)(240)이 일반OS(110)의 프로그램(n)(200)과 공유하는 메모리영역을 확인하여 접근 권한을 확인한 경우, 상기 프로그램(s)(240)은 상기 메모리영역으로부터 상기 일반OS(110)의 프로그램(n)(200)이 제공한 서명대상정보를 확인한다(500). 만약 상기 메모리영역으로부터 상기 서명대상정보가 확인되지 않으면, 상기 프로그램(s)(240)은 상기 무선단말(100)의 OS를 일반OS(110)로 전환하도록 처리하며(540), 상기 무선단말(100)의 OS가 일반OS(110)로 전환된 경우에 상기 일반OS(110)의 프로그램(n)(200)은 상기 보안OS(120)로 전환 전 상기 프로그램(n)(200)의 상태를 복원한다(545).

[0130] 한편 상기 메모리영역으로부터 상기 서명대상정보가 확인되면, 상기 프로그램(s)(240)은 상기 도면3에 도시된 과정을 통해 보안OS(120)의 인증서 저장영역 또는 HSM(135)에 구비된 사용자의 인증서를 확인한다(505). 상기 HSM(135)에 사용자의 인증서가 구비된 경우, 상기 프로그램(s)(240)은 상기 HSM(135)으로 상기 서명대상정보를 제공할 수 있다.

[0131] 만약 상기 사용자의 인증서가 확인되면, 상기 프로그램(s)(240) 또는 HSM(135)은 상기 사용자의 인증서로부터 서명키를 추출한다(510). 만약 상기 서명키가 확인되면, 상기 프로그램(s)(240) 또는 HSM(135)은 상기 서명키를 이용하여 상기 확인된 서명대상정보에 대한 전자서명 값을 생성한다(515).

[0132] 본 발명의 일 실시 방법에 따르면, 상기 서명대상정보에 대한 전자서명 값이 생성된 경우, 상기 프로그램(s)(240)은 상기 전자서명 값을 상기 일반OS(110)의 프로그램(n)(200)과 공유하는 메모리영역으로 제공한다(520). 실시 방법에 따라 상기 프로그램(s)(240)은 상기 전자서명 값을 지정된 암호방식으로 암호화하여 상기 메모리영역으로 제공할 수 있다(520). 상기 프로그램(s)(240)은 상기 무선단말(100)의 OS를 일반OS(110)로 전환하도록 처리하며(535), 상기 무선단말(100)의 OS가 일반OS(110)로 전환된 경우에 상기 일반OS(110)의 프로그램(n)(200)은 상기 보안OS(120)로 전환 전 상기 프로그램(n)(200)의 상태를 복원한다(540).

[0133] 본 발명의 다른 일 실시 방법에 따르면, 상기 서명대상정보에 대한 전자서명 값이 생성된 경우, 상기 프로그램(s)(240)은 상기 전자서명 값을 포함하는 서명데이터를 생성하고(525), 상기 서명데이터를 상기 일반OS(110)의 프로그램(n)(200)과 공유하는 메모리영역으로 제공한다(530). 실시 방법에 따라 상기 프로그램(s)(240)은 상기 서명데이터를 지정된 암호방식으로 암호화하여 상기 메모리영역으로 제공할 수 있다(530). 상기 프로그램(s)(240)은 상기 무선단말(100)의 OS를 일반OS(110)로 전환하도록 처리하며(535), 상기 무선단말(100)의 OS가 일반OS(110)로 전환된 경우에 상기 일반OS(110)의 프로그램(n)(200)은 상기 보안OS(120)로 전환 전 상기 프로그램(n)(200)의 상태를 복원한다(540).

[0134] 상기 일반OS(110)의 프로그램(n)(200)은 상기 보안OS(120)의 프로그램(s)(240)와 공유된 메모리영역을 확인하여 접근하고(545), 상기 메모리영역으로부터 상기 보안OS(120)의 프로그램(s)(240)에서 제공한 전자서명 값(또는 서명데이터)를 확인한다(550). 만약 상기 전자서명 값(또는 서명데이터)가 확인되지 않으면, 상기 프로그램(n)(200)은 오류를 출력하고 상기 프로그램(n)(200)의 동작을 초기화할 수 있다(555).

[0135] 본 발명의 일 실시 방법에 따라 상기 메모리영역으로부터 전자서명 값이 확인된 경우, 상기 프로그램(n)(200)은 상기 전자서명 값을 포함하는 서명 데이터를 생성하고(560), 지정된 서버로 상기 서명데이터를 전송하거나(565), 또는 상기 프로그램(n)(200)의 동작에 상기 서명데이터가 이용되도록 처리함으로써(565), 상기 프로그램(n)(200)에서 서명데이터를 이용하는 동작 절차를 수행한다(570). 한편 상기 보안OS(120)의 프로그램(s)(240)에서 상기 전자서명 값을 상기 프로그램(n)(200)를 통해 복호화 가능하게 암호화한 경우, 상기 프로그램(n)(200)은 상기 암호화된 전자서명 값을 복호화하여 상기 복호화된 전자서명 값을 포함하는 서명 데이터를 생성하고(560), 지정된 서버로 상기 서명데이터를 전송하거나(565), 또는 상기 프로그램(n)(200)의 동작에 상기 서명데이터가 이용되도록 처리할 수 있다(565).

[0136] 본 발명의 다른 일 실시 방법에 따라 상기 메모리영역으로부터 전자서명 값을 포함하는 서명데이터가 확인된 경우, 상기 프로그램(n)(200)은 지정된 서버로 상기 서명데이터를 전송하거나(565), 또는 상기 프로그램(n)(200)의 동작에 상기 서명데이터가 이용되도록 처리함으로써(565), 상기 프로그램(n)(200)에서 서명데이터를 이용하는 동작 절차를 수행한다(570). 한편 상기 보안OS(120)의 프로그램(s)(240)에서 상기 서명데이터를 지정된 서버를 통해 복호화 가능하게 암호화한 경우, 상기 프로그램(n)(200)은 상기 암호화된 서명데이터를 상기 지정된 서버로 전송할 수 있다(565). 또는 상기 보안OS(120)의 프로그램(s)(240)에서 상기 서명데이터를 상기 프로그램(n)(200)를 통해 복호화 가능하게 암호화한 경우, 상기 프로그램(n)(200)은 상기 암호화된 서명데이터를 복호화하여 상기 프로그램(n)(200)의 동작에 이용되도록 처리할 수 있다(565).

부호의 설명

[0137]

100 : 무선단말	110 : 일반OS
115 : 일반커널	120 : 보안OS
125 : 보안 모니터	130 : 보안커널
200 : 프로그램(n)	205 : 정보 확인부
210 : 연동 절차부	215 : 전자서명 확인부
220 : 데이터 생성부	225 : 전자서명 이용부
240 : 프로그램(s)	245 : 인증서 저장부
250 : PIN 등록부	355 : 연동 처리부
260 : PIN 인증부	265 : 정보 연동부

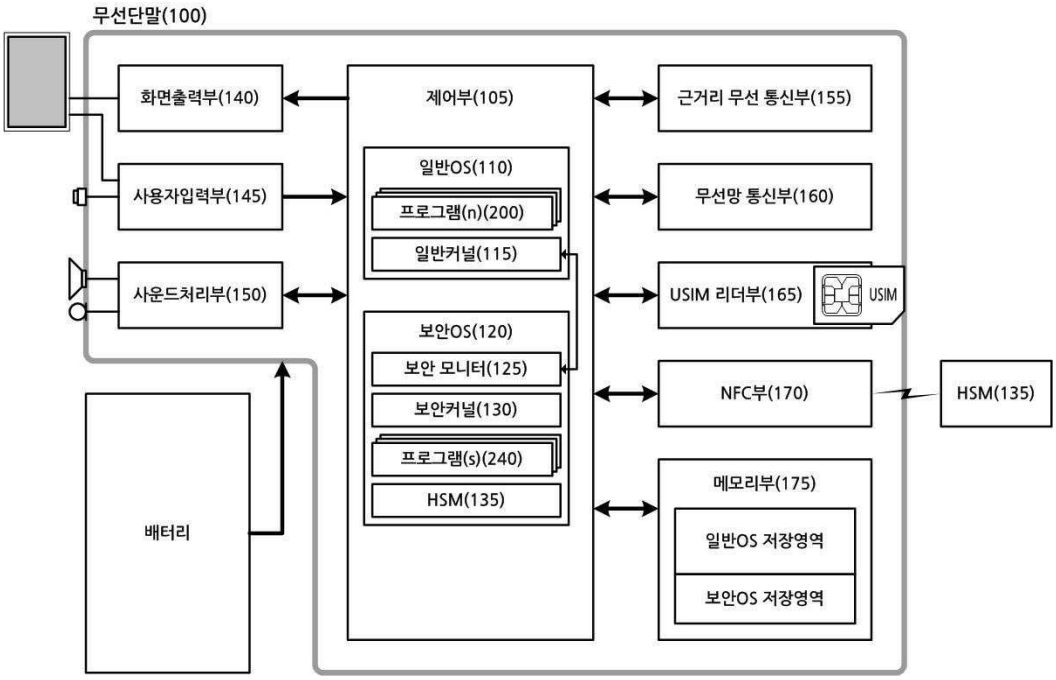
270 : 인증서 확인부 275 : 서명키 추출부

280 : 전자서명부 285 : 암호 처리부

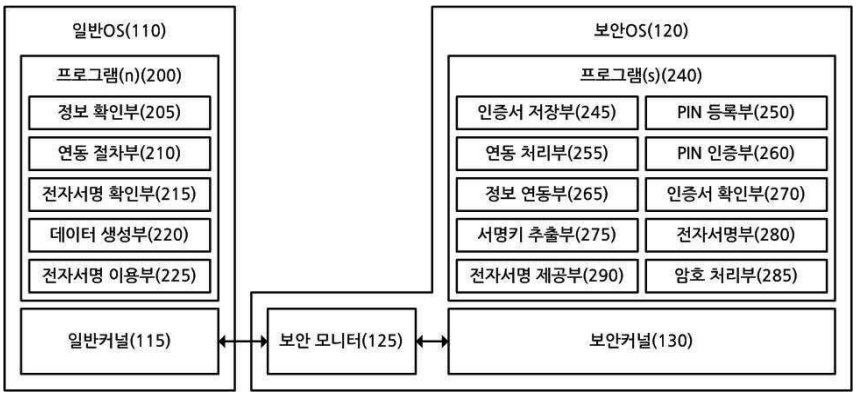
290 : 전자서명 제공부

도면

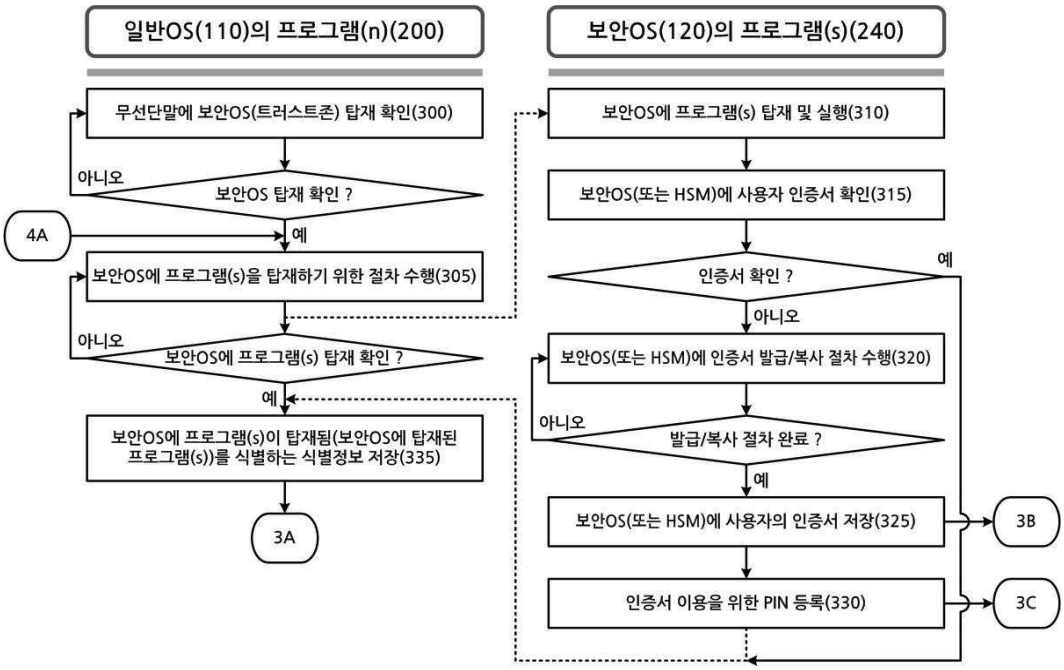
도면1



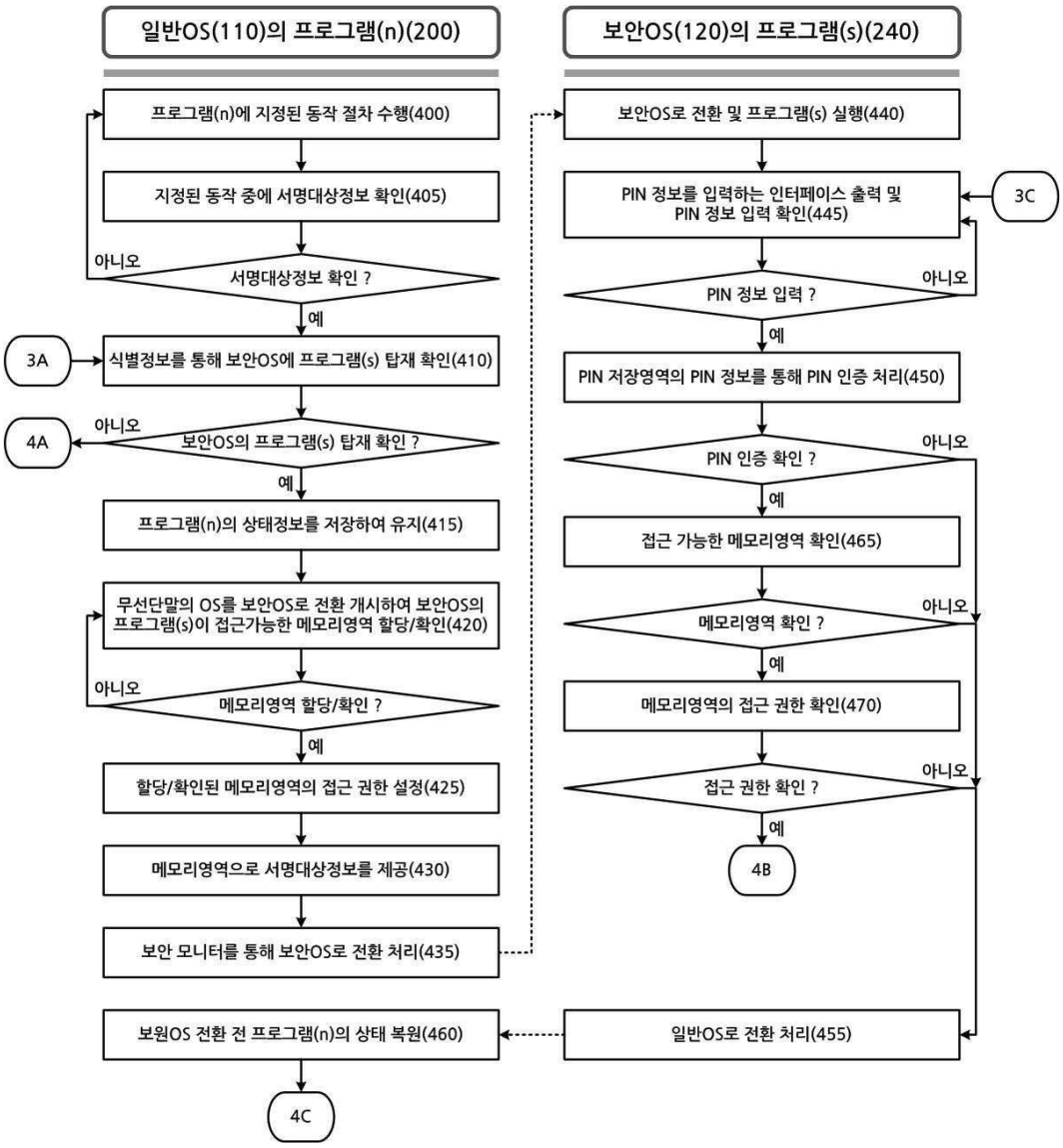
도면2



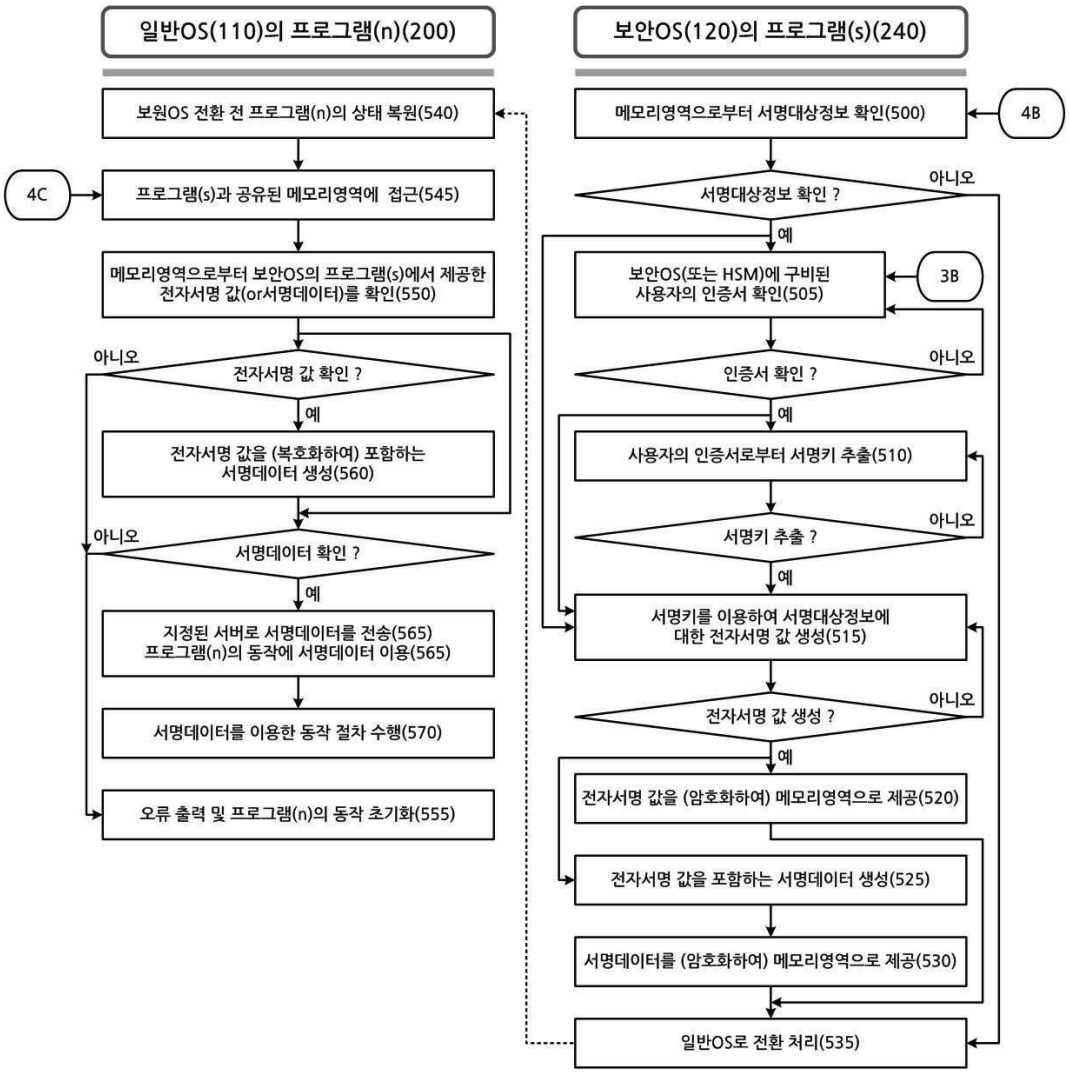
도면3


일반OS(110)의 프로그램(n)(200)
보안OS(120)의 프로그램(s)(240)
무선단말에 보안OS(트러스트존) 탑재 확인(300)
보안OS 탑재 확인 ?
아니오
예
4A
보안OS에 프로그램(s)을 탑재하기 위한 절차 수행(305)
보안OS에 프로그램(s) 탑재 확인 ?
아니오
예
보안OS에 프로그램(s)이 탑재됨(보안OS에 탑재된 프로그램(s))를 식별하는 식별정보 저장(335)
3A
보안OS에 프로그램(s) 탑재 및 실행(310)
보안OS(또는 HSM)에 사용자 인증서 확인(315)
인증서 확인 ?
예
아니오
보안OS(또는 HSM)에 인증서 발급/복사 절차 수행(320)
발급/복사 절차 완료 ?
아니오
예
보안OS(또는 HSM)에 사용자의 인증서 저장(325)
3B
인증서 이용을 위한 PIN 등록(330)
3C

도면4


일반OS(110)의 프로그램(n)(200)
보안OS(120)의 프로그램(s)(240)
프로그램(n)에 지정된 동작 절차 수행(400)
지정된 동작 중에 서명대상정보 확인(405)
서명대상정보 확인 ?
아니오
예
3A
식별정보를 통해 보안OS에 프로그램(s) 탑재 확인(410)
4A
보안OS의 프로그램(s) 탑재 확인 ?
프로그램(n)의 상태정보를 저장하여 유지(415)
무선단말의 OS를 보안OS로 전환 개시하여 보안OS의 프로그램(s)이 접근가능한 메모리영역 할당/확인(420)
메모리영역 할당/확인 ?
할당/확인된 메모리영역의 접근 권한 설정(425)
메모리영역으로 서명대상정보를 제공(430)
보안 모니터를 통해 보안OS로 전환 처리(435)
보원OS 전환 전 프로그램(n)의 상태 복원(460)
4C
보안OS로 전환 및 프로그램(s) 실행(440)
PIN 정보를 입력하는 인터페이스 출력 및 PIN 정보 입력 확인(445)
3C
PIN 정보 입력 ?
PIN 저장영역의 PIN 정보를 통해 PIN 인증 처리(450)
PIN 인증 확인 ?
접근 가능한 메모리영역 확인(465)
메모리영역 확인 ?
메모리영역의 접근 권한 확인(470)
접근 권한 확인 ?
4B
일반OS로 전환 처리(455)

도면5


일반OS(110)의 프로그램(n)(200)
보안OS(120)의 프로그램(s)(240)
보원OS 전환 전 프로그램(n)의 상태 복원(540)
4C
프로그램(s)과 공유된 메모리영역에 접근(545)
메모리영역으로부터 보안OS의 프로그램(s)에서 제공한 전자서명 값(or서명데이터)를 확인(550)
아니오
전자서명 값 확인 ?
예
전자서명 값을 (복호화하여) 포함하는 서명데이터 생성(560)
아니오
서명데이터 확인 ?
예
지정된 서버로 서명데이터를 전송(565) 프로그램(n)의 동작에 서명데이터 이용(565)
서명데이터를 이용한 동작 절차 수행(570)
오류 출력 및 프로그램(n)의 동작 초기화(555)
메모리영역으로부터 서명대상정보 확인(500)
4B
아니오
서명대상정보 확인 ?
예
보안OS(또는 HSM)에 구비된 사용자의 인증서 확인(505)
3B
아니오
인증서 확인 ?
예
사용자의 인증서로부터 서명키 추출(510)
아니오
서명키 추출 ?
예
서명키를 이용하여 서명대상정보에 대한 전자서명 값 생성(515)
아니오
전자서명 값 생성 ?
예
전자서명 값을 (암호화하여) 메모리영역으로 제공(520)
전자서명 값을 포함하는 서명데이터 생성(525)
서명데이터를 (암호화하여) 메모리영역으로 제공(530)
일반OS로 전환 처리(535)