DOI: 10.3745/KIPSTC.2009.16-C.3.335

Mobile Trusted Module 기반 단말에서의 안전한 키 백업 및 복구 방안에 대한 연구

강 동 완[†] · 전 성 익[††] · 이 임 영[†††]

요 약

정보통신이 발달함에 따라서 모바일 환경은 주된 통신 환경으로 자리잡았다. 모바일 환경은 유선환경 보다 개방된 네트워크 특성으로 인하여, 서비스를 이용함에 따라 사용자의 개인정보에 대한 스니핑이나 피싱, 불법 단말기의 사용으로 개인정보가 노출 될 수 있다. 따라서 신뢰 컴퓨팅을 표준화 하고 있는 TCG(Trusted Computing Group)는 모바일 환경의 보안을 위해 하드웨어 기반의 보안 모듈인 MTM(Mobile Trusted Module)을 제안하였다. MTM은 플랫폼에 임베디드되어 사용자 프라이버시와 플랫폼 무결성을 보호하고 물리적으로 안전하지만 강한 보안 기능을 제공하는 만큼 비밀 데이터를 다른 곳으로 이전할 때 보안적인 접근이 요구된다. 본 논문에서는 TCG 보안 기술과 함께 암호키 이전 방안에 대해서 살펴보고, 키 백업과 복구를 적용한 안전한 암호키 이전 방안을 제안한다.

키워드 : 신뢰 컴퓨팅, 모바일 신뢰 모듈, 키 백업 및 복구

A Study on Secure Key Backup/Recovery Scheme for Device based on Mobile Trusted Module

Kang Dong Wan[†] · Jun Sung Ik[††] · Lee Im Yeoung[†††]

ABSTRACT

Mobile environments are evolving the main communication environment as a develops of communication technology. In mobile environments, sensitive information can be compromised on-line, so demand for security has increased. Also, mobile devices that provide various services are in danger from malware and illegal devices, phishing and sniffing etc, and the privacy. Therefore, MTM(Mobile Trusted Module) is developed and promoted by TCG(Trusted Computing Group), which is an industry standard body to enhance the security level in the mobile computing environment. MTM protects user privacy and platform integrity, because it is embedded in the platform, and it is physically secure. However, a security approach is required when secret data is migrated elsewhere, because MTM provides strong security functions. In this paper, we analyze the TCG standard and migration method for cryptographic key, then we propose a secure migration scheme for cryptographic key using key Backup/Recovery method.

Keywords : Trusted Computing, Mobile Trusted Module, Key Backup/Recovery

1. 서 론

신뢰 컴퓨팅은 향후 유비쿼터스 환경에서 중요한 보안 기술로 그 역할을 할 것이다. 신뢰 컴퓨팅은 기존의 소프트웨어 기반의 보안 아키텍처와 다르게 하드웨어 보안 모듈을 사용한 신뢰를 기반으로 하는 보안 프레임 워크이다[5]. 이 신뢰의 근원에는 하드웨어 보안 모듈인 TPM/MTM이 있으며 이를 시작으로 컴퓨팅을 이루는 각 구성 요소들 간에 신뢰 체인을 이루며 안전한 컴퓨팅을 구현한다. 이러한 신뢰 컴퓨팅은 향후 컴퓨팅 환경이 모바일 환경으로 이동함에 따라, 모바일 환경에서의 주요한 보안 프레임 워크로 그 기능을 할 것임은 자명한 사실이다[2].

모바일 환경의 보안은 기존의 소프트웨어 보안으로 해결하기에는 다양한 보안 위협이 존재한다. 특히 단말기의 분실 및 물리적인 접근에 의한 공격은 모바일 환경의 대표적인 보안 위협이다[1 ,3]. 이러한 위협을 배경으로 신뢰 컴퓨팅을 이용하여 모바일 환경의 많은 보안 위협을 줄일 수 있으며, 또한 서비스 사업자나 단말기 제조업체에게도 개방된 표준을 수용함으로써 신뢰성 있는 안전성을 기대할 수 있는

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. [2006-S-041-03, 차세대 모바일 단말기의 보안 및 신뢰 서비스를 위한 공통 보안 핵심 모듈 개발]
† 준 회 원 : 순천향대학교 컴퓨터학부 석사
†† 정 회 원 : 한국전자통신연구원 SW서비스연구팀 책임연구원
††† 종신회원 : 순천향대학교 컴퓨터학부 교수(교신저자)
논문접수 : 2009년 1월 9일
수 정 일 : 2009년 3월 24일
심사완료 : 2009년 3월 25일

등의 큰 장점이 될 수 있다. 따라서 개방형 보안 표준으로써 신뢰할 수 있는 보안성을 얻을 수 있고, 자체적으로 보안을 위한 중복 투자를 할 필요가 없으며, 플랫폼 인증을 통해 사용자는 단말기에 대한 신뢰를 가질 수 있다.

본 논문에서는 신뢰 컴퓨팅 기술을 모바일 환경에 적용함에 있어 플랫폼 변경에 따른 비밀 데이터 이전 방안에 대한 문제점과 사용자의 인증 키 분실 지적하고자 한다. 플랫폼에 임베디드되는 보안 모듈로써의 MTM은 강한 보안성을 가지지만 그 만큼 암호키를 외부에 노출시키지 않기 때문에 보호된 데이터의 안전한 이동 방안이 필요하고, 다양한 암호와 인증 키를 관리해야 하는 사용자는, 키의 분실시에 대처할 수 있는 방안이 필수적으로 필요하게 된다[4]. 따라서 본 연구에서는 사용자 암호키의 분실이나, 모바일 단말의 데이터 이동성을 만족시킬 수 있는 안전한 키 백업 및 복구 방안에 대해서 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 연구 배경으로써 MTM의 모태가 되는 TPM에 대해 살펴보고, 모바일 환경에 MTM을 적용하는데 따른 제약사항과 그에 따른 보안 요구사항을 살펴본다. 이어 3장에서는 기존에 연구된 비밀 데이터 이전 방안으로써 TCG의 Migration과 Maintenance, CMK, 그리고 상용 솔루션으로써 BitLocker의 백업 및 복구 메커니즘에 대해서 분석하고, 4장에서는 키 백업 및 복구 메커니즘을 적용할 시나리오와 함께 제안방식을 설명한다. 5장에서는 2장에서의 보안 요구사항을 기반으로 제안방식을 분석하고 마지막으로 6장에서 결론과 향후 연구방향을 제시한다.

2. 연구 배경

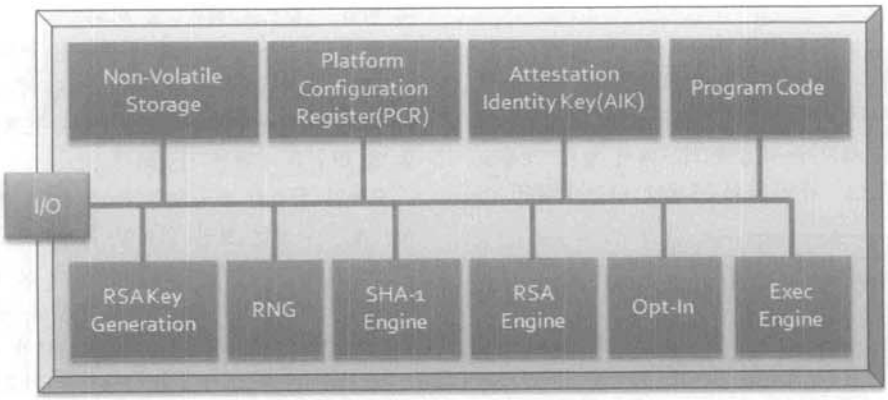
본 장에서는 신뢰 컴퓨팅에 대한 표준화 단체인 TCG의 보안기술에 대해 살펴보고, 모바일 환경에서 MTM 적용과 관련된 제약사항과 그에 따른 보안 요구사항을 분석한다.

2.1 TCG와 MTM 사용의 제약사항

TCG는 신뢰컴퓨팅을 위한 보안기술로써 하드웨어 기반의 보안 모듈을 표준화하고 있는데 일반 PC(Personal Computer) 환경을 위한 TPM(Trusted Platform Module)과 TPM을 모바일 환경에 적용하기 위한 MTM(Mobile Trusted Module)이 각각 2004과 2006년에 제안되었으며 현재까지 지속적으로 표준화가 진행 중이다[6, 7]. TPM은 보안기능을 제공하기 위해 (그림 1)과 같은 하드웨어 구조를 가지고 있으며, TPM의 구성요소 중 키와 관련된 몇 가지 주요한 항목을 살펴보면 다음과 같다[10 ,11].

- EK(Endorsement Key) : EK는 TPM의 유일한 키로써 TPM 제조 시 제조사가 생성하여 TPM 내부의 안전한 비휘발성 저장소에 저장하는 개인키/공개키 쌍이다. EK의 개인키는 TPM 내부에서 외부로 노출이 되지 않고, 변경되지 않으며 제조사의 개인키에 의해 서명된다.
- SRK(Storage Root Key) : SRK는 TPM이 안전한 저장소를 제공하기 위해 사용되는 핵심적인 키이다. 안전한 저장소는 일반적인 물리 저장 공간 중에 SRK로 보호된 영역을 의미하며 이 공간에 저장되는 데이터는 SRK에 의해서 암호화되어 저장되기 때문에 정당한 절차를 거치지 않으면 해당 데이터를 알 수 없다.
- AIK(Attestation Identity Key) : TPM에서는 AIK를 만들어 각각의 용도에 따른 식별키를 가지게 된다. 사용자는 AIK를 여러 개 만들 수 있으며 이 AIK는 인증기관인 CA(Certificate Authority)로 부터 정당한 AIK임을 인증 받는다.
- PCR(Platform Configuration Register) : TPM은 시스템 부팅시 BIOS(Basic Input Output System)보다 먼저 동작하여 BIOS부터 차례로 시스템을 점검해 나간다. 이러한 secure booting 과정을 위해 TPM은 플랫폼의 시스템 소프트웨어와 운영체제 및 응용 계층의 특정 애플리케이션에 이르기까지 플랫폼의 무결성 정보를 모두 저장하고 관리하며 수집된 무결성 정보를 해쉬하여 TPM 내부의 휘발성 저장소인 PCR의 해당 인덱스에 저장한다.

TPM은 일반 PC 환경을 기반으로 하는 보안 모듈로써



(그림 1) TPM의 하드웨어 구성

표준화 되었다. 점차 컴퓨팅 환경이 이동성을 중요하게 다루는 모바일 환경으로 변화함에 따라 TPM을 모바일 환경에 접목하려고 하는 움직임이 있었으며, 이는 TCG의 MPWG (Mobile Phone Working Group)에 의해 MTM(Mobile Trusted Module)로 표준화 되었다[8]. 하지만 MTM은 아직까지 모바일 환경에 적용하고자 할 때에 제약사항이 존재한다. MTM은 플랫폼에 임베디드되어 사용되는 보안 모듈로써 사용자에게 강한 안전성을 제공하지만[9], 이 안전성은 해당 플랫폼을 벗어나 다른 플랫폼으로의 데이터 이전에 있어 큰 제약사항이 된다[4]. MTM에서의 키 관리는 모듈 내부 안전한 저장소의 SRK를 기반으로 이루어지는데 SRK의 개인키는 외부로 유출이 되지 않는다. 따라서 SRK에 의해 보호되고 있던 데이터들을 다른 플랫폼으로 이전하기 위한 방안이 필요하다. 여기서의 이전 대상인 비밀 데이터는 SRK, 혹은 사용자의 비밀 키 및 일반 응용 프로그램에서 사용되는 암호 키 등을 대상으로 한다.

2.2 보안 요구사항

MTM을 사용하기 위해서는 데이터의 이동성이 제공되어야 하며, 이를 위해서는 키의 안전한 이동이 필수적이다. 따라서 본 절에서는 MTM에서의 안전한 키 이전을 위한 키 백업과 복구 방법에서의 보안 요구사항을 제시한다.

- 인증 : 백업 데이터를 생성하거나, 백업 데이터에 대한 복원 프로세스는 사전에 정의된 정당한 사용자 및 권한자에 의해서만 이루어 져야 한다. 이를 위해서 백업 시스템은 절차에 따른 객체에 대한 인증을 수행해야 한다.
- 기밀성 : 백업 대상의 정보는 본래 키의 소유자나 혹은 정당한 절차에 의해 복호되는 경우를 제외하고 다른 제 3자에 의해 키의 정보가 노출되어서는 안 된다.
- 무결성 : 암호화 되어 백업된 키가 변조나 위조 등으로써 해당 정보가 원래 보관 하고자 했던 키 정보와 비교하여 변경되지 않았다는 것을 증명할 수 있어야 한다.
- 완전성 : 암호키에 대한 백업 프로세스는 언제나 그 동작을 수행할 수 있어야 하며, 어떠한 상황이 오더라도 보관, 혹은 유지하고 있는 정보들에 대해서 정당한 객체가 접근할 수 있도록 해야 한다.
- 안전한 저장소 : 백업되는 데이터는 해당 사용자에 대한 비밀 정보로써 해당 데이터에 대한 파괴 및 삭제, 악의적인 변조 등은 백업 시스템을 무력하게 만들 수 있다. 백업 시스템은 이러한 공격에 대해 탐지하는 것 뿐만 아니라 적극적인 복구도 가능하도록 설계되어야 한다.

3. 관련 연구

본 장에서는 플랫폼 변경에 따른 기존 연구로써 TCG 표준에서 제안하고 있는 Migration과 Maintenance, CMK 및 BitLocker에 대해서 살펴본다.

3.1 TCG 표준 메커니즘

TCG는 임베디드된 특성을 가진 TPM/MTM을 사용하는데 있어 플랫폼의 변경에 따라서 모듈 내부의 암호키를 모듈 밖으로 빼내어 다른 모듈로 이전시키는 메커니즘을 정의하였다. 이 메커니즘은 Migration과 Maintenance, CMK로 정의되며, 이를 사용하여 보안 모듈 내부의 암호키를 다른 모듈로 이동시킬 수 있다[10, 11].

TPM에서 사용되는 키는 모두 속성을 가지고 있으며 그 중에 Migration에 관한 속성이 정의되어 있다. 이는 migratable과 non-migratable 속성 중 한 가지를 가지게 된다. Migratable은 Migration 메커니즘을 사용하여 다른 TPM으로 이동할 수 있는 키 이며, non-migratable 속성을 가진 키는 Migration 메커니즘으로 이동시킬 수 없고, Maintenance 메커니즘을 통해서만 다른 TPM으로 이동시킬 수 있는 키 이다.

TPM에서는 내부에서 생성된 키 이외에 외부로부터 유입된 키는 실질적으로 TPM이 인증하지 않는다. 이러한 문제점으로 인하여 TPM v1.2에서는 CMK가 등장하였다. CMK는 외부의 신뢰 개체의 참여로써 migratable하면서도 TPM 내부에서 이전이 가능한 키를 의미한다[11].

Migration과 Maintenance는 TPM에서 키를 외부의 다른 TPM으로 이동시키는 수단으로써 키 백업보다는 플랫폼 이전에 따른 키의 이동으로 제안되었다. 또한 이들 메커니즘은 표준 문서에 그 절차가 기술되어 있지만 실질적인 구현 방안에서는 TPM 제조사에 위임하고 있다. 더욱이 Maintenance의 경우에는 필수적으로 구현 사항이 아니기 때문에 여타 다른 TPM 제조사들간의 Maintenance는 상당한 어려움이 예상된다. 이는 단말의 사업자간 이동에 따른 큰 문제점이 될 수 있다.

3.2 BitLocker

Microsoft의 운영체제에서 제공되는 보안 솔루션으로써 BitLocker가 있다. 이는 컴퓨터의 마더보드에 내장된 TPM을 사용하는 보안 솔루션으로써, 디스크의 암호화를 제공한다[12]. 이 BitLocker는 256bit키로써 AES암호화를 통해 디스크를 보호한다. 키는 TPM에 의해 보호되며 해당 TPM에 의해서만 복호될 수 있다. BitLocker는 키 백업을 위해 크게 여러가지 방안을 제시하고 있다. 복구 암호와 복구 키이다. 복구 암호는 48자리 숫자로 되어 있으며 이는 사용자가 따로 출력해서 보관하거나, USB 메모리 같은 휴대용 저장장치에 보관할 수 있다. 복구 키는 256bit의 바이너리 데이터로써 VMK(Volume Master Key)를 암호화하는데 사용된 키이다. 복구 암호나 복구 키로 암호화된 복구 정보는 시스템 볼륨에 저장된다. 복구시에는 복구 암호나 복구 키를 입력함으로써 시스템 볼륨에 있는 복구 데이터를 복호하여 원래의 VMK를 복호하고, 이를 사용하여 궁극적으로 FVEK

(Full Volume Encryption Key)에 접근할 수 있다.

하지만 사실상 BitLocker는 TPM 외부에서 생성된 키를 사용하는 메커니즘이 아니다. TPM 외부에서 생성하여 SRK (Storage Root Key)하에서 암호화시켜 보관해 놓는 방식이며, 이에 따른 복구 정보 역시 해당 디스크의 시스템 볼륨에 저장하는 방법이다. 이는 TPM의 Migration이나 Maintenance 등의 메커니즘 없이 쉽게 사용될 수 있다. 하지만 이 방식은 실제 디스크의 분실 및 시스템 볼륨의 손상에 따라서 쉽게 복구할 수 없는 단점이 존재한다.

4. 제안방식

모바일 환경에서의 데이터 이동성은, MTM을 사용한 모바일 신뢰 컴퓨팅에서 중요하게 고려해야 하는 사항이다. 강력한 암호화를 제공하는 만큼 데이터 이동성의 제약이 생기기 때문에 이를 위해 적절한 비밀 데이터의 이동방안이 필요하다. 본 제안 방식에서는 키 백업과 복구를 사용하여 사용자의 암호키를 이전하는 방법으로 모바일 신뢰 컴퓨팅에서의 데이터 이동성을 제공하는 방안을 제시한다.

키 백업과 복구는 가장 중요한 사항으로써 백업을 하기 위한 암호 키로써의 백업키와 백업된 데이터를 보관하는 백업 데이터의 저장소를 들 수 있다. 백업 키와 저장소는 백업 및 복구 프로세스에 있어서 가장 중요한 요소로써, 이 두 요소를 중심으로 다음과 같은 단말의 교체 상황을 고려할 수 있다.

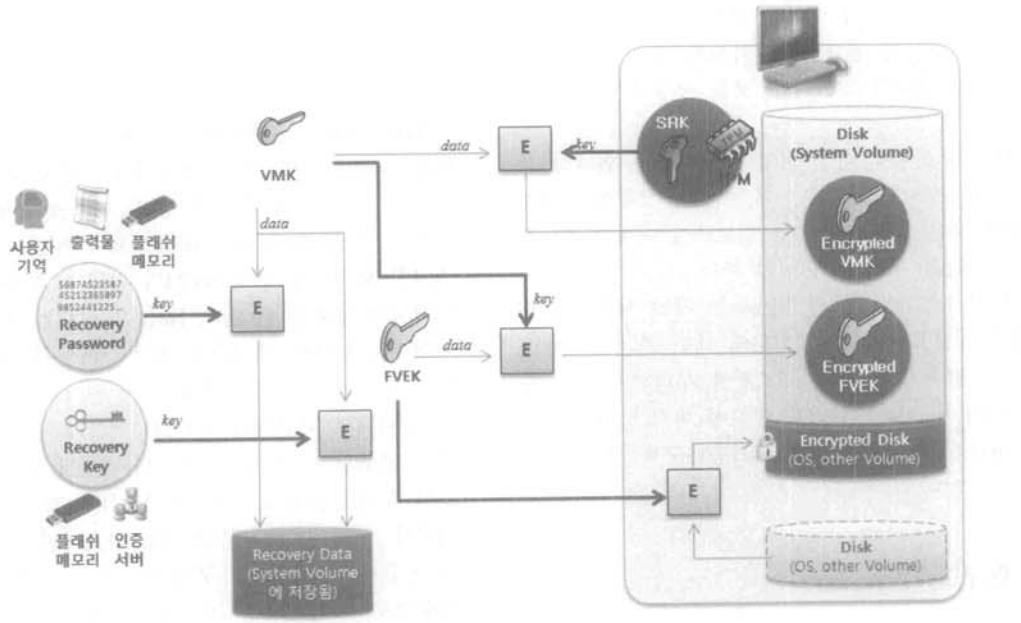
- 사용자의 의도적인 단말의 교체
- 단말의 분실 및 단말 자체 기능의 손상에 따른 단말의 교체
- 단말의 MTM 모듈 손상에 따른 단말의 교체

사용자가 의도하는 단말의 교체 상황에서는 사용자가 사용하던 단말기가 온전하게 존재하기 때문에 MTM의 이전 메커니즘을 통해 이전 될 수 있다. 물론 단말의 제조사가 다르게 되면 TCG의 표준 이전 메커니즘으로는 해결하기 어려운 상황도 존재한다.

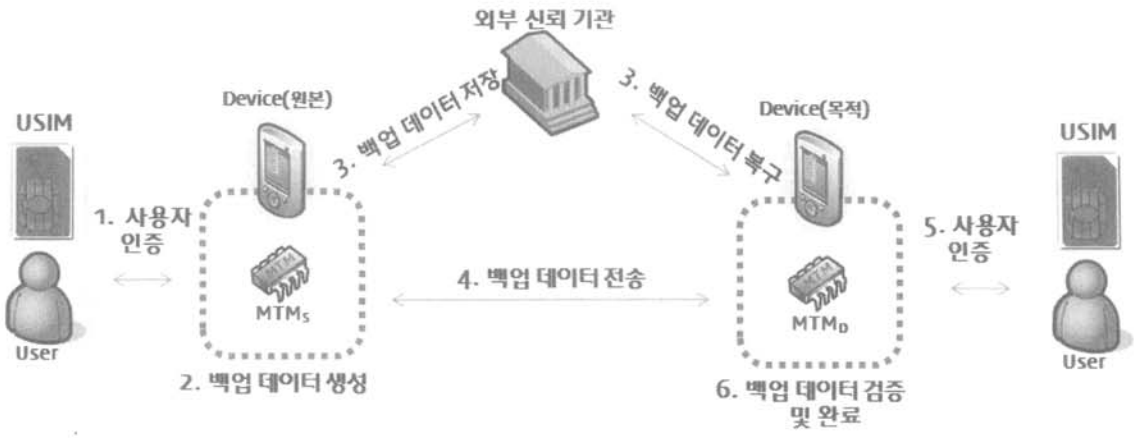
단말의 분실에 따른 단말의 교체는 사용자가 이전에 소유했던 단말기를 가지고 있지 않은 상태이다. 따라서 이는 단말의 정보에 접근할 수 없기 때문에 외부에 백업된 정보로써 데이터를 복구해야 한다. 따라서 이 상황에서는 사용자가 특정 장소에 데이터를 보관해 놓고 있어야 한다.

단말의 손상은 두 가지로 분류할 수 있다. 먼저 보안 모듈인 MTM이 손상된 경우와 단말기 자체가 손상된 경우이다. 보안 모듈인 MTM이 손상된 경우에는 단말 자체의 저장소에 저장된 정보는 접근 할 수 있어도, MTM의 보안 기능을 사용할 수 없는 상황이 된다. 이는 MTM의 SRK에 의해 보호된 키를 사용할 수 없게 되며, MTM의 이전 메커니즘도 사용할 수 없는 상황이 된다. 이 경우에는 외부에 백업된 사용자 키를 가지고 신규 단말에 등록하는 방법을 사용해야 한다.

그리고 또 다른 단말의 손상으로써, 단말 자체의 손상은 MTM의 기능을 사용할 수 있지만, 외부의 저장소가 손상된 경우로 볼 수 있다. 이 경우에 MTM 내부의 저장소 이외의 외부 저장소에 접근이 불가능 하므로 키의 백업이 무의미해지는 경우가 발생한다. 따라서 이와 같은 경우에는 단말의 일반적인 저장소에 저장된 암호화된 데이터에 대한 백업이 진행된다면 복구를 수행할 수 있다. 하지만 이는 키를 백업하는 것에 비해서 비용이 매우 클 수 있다.



(그림 2) BitLocker의 구조



(그림 3) 제안하는 키 백업 및 복구 방식의 전체적인 구조

4.1 시스템 계수

본 절에서는 제안방식에서 사용된 기호를 기술한다.

- $*$: 참여 객체(CA, USIM, MTM, MTM_{NEW} : 새로운 단말, 혹은 기존의 초기화된 단말기)
- ID_* : 개체 $*$의 식별자
- $UserKey$: MTM에서 사용되는 사용자 키를 보호하는 SRK 아래의 사용자 루트키
- $AuthValue$: MTM의 사용자에 대한 소유자 인증 정보
- $tpmProof$: MTM 내부의 고유한 비밀값(오직 MTM 자신만 접근하고 확인할 수 있음)
- PU_{bk}, PR_{bk} : 사용자 키 이전을 위한 백업 공개키/개인키 쌍
- $Sign_*(data)$: data에 대한 $*$의 서명 값
- $E_*[data]$: $*$의 공개키로 암호화한 데이터
- $H(data)$: data의 일방향 해쉬 함수 값
- TS : 재전송 공격 방지를 위해 동기화된 MTM의 타임스탬프 값

4.2 키 백업 및 복구를 이용한 키 이전 방안 제안

본 제안 방식은 사용자의 모바일 단말간의 데이터 이전에 적용되는 것으로써, 주요한 특징으로는 구성된 사용자의 암호키 구조에 기반하여 $UserKey$를 CMK 기반으로 생성하고, MTM에서 이를 백업하기 위한 별도의 백업키로써 백업 공개키 쌍인 PU_{bk}, PR_{bk}를 생성하는 방식이다. 각 제안방식들은 크게 세 과정로 구분된다. 첫 번째는 사용자가 단말을 초기 소유하면서 백업키 및 복구 프로세스를 위한 인증 정보를 생성하는 초기 설정 과정이며, 두 번째는 백업 키로써 사용자의 루트키인 $UserKey$를 백업하고, 백업 데이터를 외부에 저장하는 백업 과정이다. 마지막 과정은 외부의 백업 데이터를 사용하여 다른 단말기에 이전하는 복구 과정이다 (그림 3). 세부적으로 본 제안방식은 다음의 세 가지 방안으로 각각의 단말 교체 상황을 분류한 <표 1> 따라 제안하였다.

4.2.1. CMK와 MTM 기반의 사용자 키 백업 및 복구 방안(제안방식 1)

본 제안 방식은 사용자를 인증하고, 모바일 단말의 MTM에 대한 소유권을 설정하며, 백업키 및 백업 프로세스에 대한 인증정보를 생성한다. 먼저 사용자는 정당한 USIM의 소유자임을 인증 받았고, MTM의 소유자 인증 과정을 마쳤다고 가정한다.

4.2.1.1 초기 설정 과정

단계 1. MTM은 내부에서 백업 공개키 쌍인 PU_{bk}, PR_{bk}를 생성한다. 생성 후에, MTM은 USIM에 $Sign_{AIK}(PU_{bk})$를 전송한다.

단계 2. USIM은 전송된 $Sign_{AIK}(PU_{bk})$을 검증하고, 백업 공개키를 확인한다. 그리고 인증 난수인 $AuthNonce$를 생성하여 $g^{H(AuthNonce)}$를 다시 MTM에 전송한다.

단계 3. MTM은 받은 $g^{H(AuthNonce)}$에 사용자의 MTM에 대한 소유자 인증정보인 $AuthValue$를 다시 지수승하여 복구 프로세스에 대한 인증 정보 $g^{H(AuthNonce)\cdot H(AuthValue)}$인 $AuthRecoveryProc$를 생성한다.

〈표 1〉 단말의 교체 상황에 따른 제안방식

단말의 교체 상황	제안방식
사용자의 의도적인 단말의 교체	CMK와 MTM 기반의 사용자 키 백업 및 복구 방안(제안방식 1)
단말의 분실 및 단말 자체의 기능 손상에 따른 교체	CMK와 외부 신뢰 기관을 사용한 키 백업 및 복구 방안(제안방식 2)
단말의 MTM 모듈 손상에 따른 교체	CMK와 USIM을 사용한 키 백업 및 복구 방안(제안방식 3)

4.2.1.2. 백업 과정

복구 인증 정보를 생성한 후에는 사용자의 루트키인 $UserKey$를 백업하게 된다.

단계 1. $UserKey$는 먼저 사용자의 MTM에 대한 소유자 인증 정보인 $Auth\,Value$를 대칭키로 하여 초기 암호화 데이터 $EncIn$을 다음과 같이 생성한다.

$$E_{Auth\,Value}[UserKey]$$

단계 2. 생성된 초기 암호화 데이터 $EncIn$은 다시 백업 키 PU_{bk}로 암호화하여, 이중 암호화 데이터 $EncOut$을 다음과 같이 생성한다.

$$E_{PU_{bk}}[EncIn]$$

단계 3. 그리고 MTM의 서명키인 AIK로 $EncOut$의 해쉬값과 복구 프로세스 인증 정보의 해쉬값 $H(AuthRecoveryProc)$을 함께 서명하여 $EncOut$과 함께 백업 데이터 $BackupData$를 생성한다. 생성된 $BackupData$는 USIM이나 별도의 저장소에 따로 보관하게 된다.

$$BackupData = EncOut, Sign_{AIK}[H(EncOut), H(AuthRecoveryProc)]$$

4.2.1.3. 복구 과정

복구 과정은 사용자의 데이터가 다른 단말로 옮겨졌을 경우나, 단말의 리셋에 따라서 진행되는 과정이다. 이는 이전에 암호화된 사용자의 데이터를 복구하기 위해 복구 프로세스에 대해 정당한 객체가 수행하는 것인지에 대한 인증을 수행하여, 복구 데이터에서 사용자 루트키를 복구해 낸다. 이 과정은 기존의 단말, 혹은 새로운 단말에 대한 MTM의 소유자 인증이 사전에 이루어 졌다고 가정한다.

단계 1. 먼저 사용자는 새로운 단말, 혹은 기존의 초기화된 단말기(MTM_{NEW})에 USIM을 삽입하고, 단말이 제공하는 복구 모드로 들어가게 된다.

단계 2. MTM_{NEW}은 사용자로부터 이전의 소유자 인증정보인 $Auth\,Value$를 입력받고, USIM으로 부터는 인증 난수인 $AuthNonce$를 전송받는다. 그리고 복구 프로세스를 위한 $AuthRecoveryProc$를 다음과 같이 계산한다.

$$AuthRecoveryProc' = g^{H(AuthNonce)\,\cdot\,H(Auth\,Value)}$$

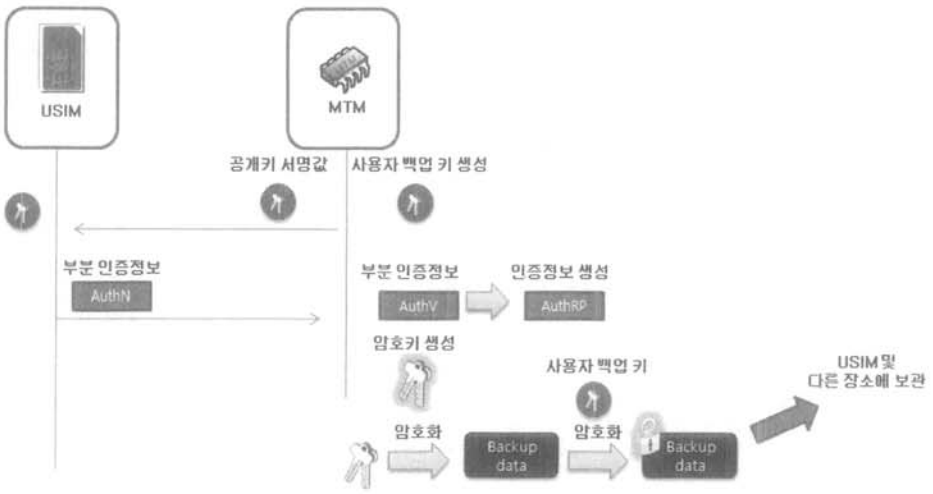
단계 3. MTM_{NEW}은 백업 데이터인 $BackupData$를 USIM이나, 다른 사용자의 저장매체를 통해 전송받는다. 그 후에, $AuthRecoveryProc'$와 함께 $BackupData$에 대한 AIK의 서명을 검증한다.

$$Verify\ D_{PU_{AIK}}[BackupData] \stackrel{?}{=} H(EncOut), H(AuthRecoveryProc')]$$

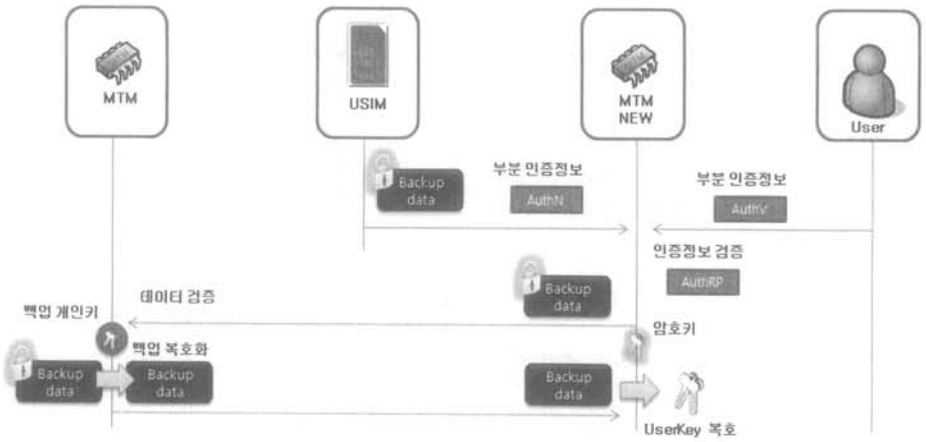
단계 4. 검증 후에, 이전의 모바일 단말기에 이중으로 암호화된 사용자 루트키인 $EncOut$과 복구 인증정보인 $AuthRecoveryProc$, $Auth\,Value$를 해쉬한 $H(AuthRecoveryProc), H(Auth\,Value)$, 현재 단말의 AIK_{NEW}로 전자서명한 $Sign_{AIK_{NEW}}[H(EncOut), H(AuthRecoveryProc')]$을 원래 단말로 전송한다.

단계 5. 원래의 단말기는 송신자의 단말기가 보낸 AIK_{NEW}의 서명을 검증하고, $AuthRecoveryProc'$, $Auth\,Value$를 다음과 같이 검증한다.

$$Verify\ D_{PU_{AIK}}[BackupData] \stackrel{?}{=} H(EncOut), H(AuthRecoveryProc')]$$



(그림 4) 제안방식 1의 초기 설정 및 백업 과정



(그림 5) 제안방식 1의 복구 과정

검증 후에 $EncOut$을 자신의 백업 개인키 PR_{bk}로 복호하여 $EncIn$을 돌려준다.

단계 6. $EncIn$을 전송받은 단말기는 사용자로부터 입력된 $AuthValue$를 사용하여 $EncIn$을 복호하여 사용자 루트키인 $UserKey$를 새로운 단말기에 등록하고, 암호화 데이터에 대한 접근을 하게 된다.

4.2.2. CMK와 외부 신뢰 기관을 사용한 키 백업 및 복구 방안(제안방식 2)

본 제안 방식은 백업을 위해서 외부 신뢰 개체의 백업키를 사용하는 방법이다. 또한 생성된 백업 데이터 또한 반드시 외부의 신뢰된 저장소에 저장해야 하며, 이 방안에서는 외부 신뢰 개체의 보안이 매우 중요하게 된다. 외부 신뢰 개체는 MTM의 AIK 및 EK에 대해서 검증할 수 있으며, MTM 또한 외부 신뢰 개체의 공개키를 검증할 수 있다고 전제한다.

4.2.2.1. 초기 설정 과정

초기 설정 과정은 단말기가 백업을 위해서 별도의 백업키를 외부의 신뢰 개체로부터 받는 단계이다. 이 단계는 사용자의 인증 및 MTM의 소유자 인증이 수행된 이후 수행되는 과정이며, 이미 사용자 인증 및 MTM의 소유자 인증은 이루어 졌다고 가정한다.

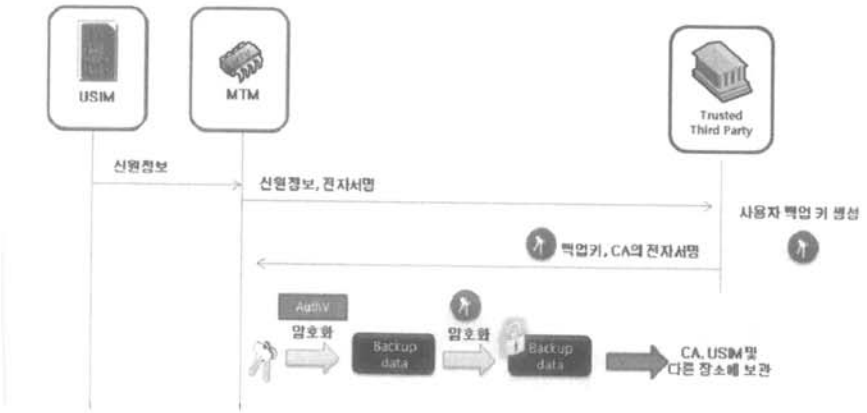
단계 1. MTM은 외부 신뢰 개체에 백업키를 요청하기 위해 자신의 신원정보로써 자신의 ID와 USIM의 ID, 백업키 요청 메시지를 AIK로 전자서명하여 다음과 같이 함께 전송한다.

$$ID_{MTM}, ID_{USIM}, BackupKeyReq, TS, Sign_{AIK}[h(ID_{MTM}, ID_{USIM}, BackupKeyReq, TS)]$$

단계 2. 외부 신뢰 객체 CA는 MTM의 메시지에 대해서 AIK의 유효성과 메시지의 전자서명을 공개된 AIK 공개키로써 검증한다.

$$h(ID_{MTM}, ID_{USIM}, BackupKeyReq, TS) \stackrel{?}{=} D_{PU_{AIK}}[Sign_{AIK}[h(ID_{MTM}, ID_{USIM}, BackupKeyReq, TS)]]$$

검증 후, 해당 단말기에 사용될 백업키 PU_{bk}/PR_{bk}를 생성한다. 생성된 백업 공개키인 PU_{bk}는 CA의 전자서명으로 다음과 같이 전송된다.



(그림 6) 제안방식 2의 초기 설정과정 및 백업 과정

$ID_{CA}, ID_{MTM}, ID_{USIM}, PU_{bk}, TS, Sign_{CA}$
$[h(ID_{CA}, ID_{MTM}, ID_{USIM}, PU_{bk}, TS)]$

단계 3. MTM은 CA의 공개키로 전송된 데이터의 CA 전자서명을 검증하여 유효성을 확인하고, 백업키 PU_{bk}를 해당 사용자에 대한 백업키로 내부에 안전하게 등록하게 된다.

4.2.2.2. 백업 과정

복구 인증 정보를 생성한 후에는 사용자의 루트키인 *UserKey*를 백업하게 된다.

단계 1. *UserKey*는 먼저 사용자의 MTM에 대한 소유자 인증 정보인 *Auth Value*를 대칭키로 하여 초기 암호화 데이터 *EncIn*을 다음과 같이 생성한다.

$E_{Auth\,Value}[UserKey]$

단계 2. 생성된 초기 암호화 데이터 *EncIn*은 다시 백업키 PU_{bk}로 암호화하여, 이중 암호화 데이터 *EncOut*을 다음과 같이 생성한다.

$E_{PU_{bk}}[EncIn]$

단계 3. 그리고 MTM의 서명키인 AIK로 *EncOut*의 해쉬값을 함께 서명하여 *EncOut*과 함께 백업 데이터 *BackupData*를 생성한다. 생성된 *BackupData*는 USIM이나 별도의 저장소에 따로 보관하게 된다.

$BackupData = EncOut, Sign_{AIK}[H(EncOut)]$

4.2.2.3. 복구 과정

복구 과정에서는 MTM 단말기가 해당 사용자의 백업키를 복구하기 위해 외부 신뢰 객체인 CA에 요청하는 단계이다. 먼저 사용자는 해당 단말기에 대한 검증과 USIM의 소유자 인증을 수행했다고 가정한다.

단계 1. 먼저 사용자는 새로운 단말, 혹은 기존의 초기화된 단말기에 USIM을 삽입하고, 단말이 제공하는 복구 모드로 들어가게 된다. 복구모드에 들어간 단말기는 사용자의 복구 요청에 따라 USIM의 ID와 MTM 자신의 ID, *Auth Value*, 임시적으로 생성한 세션키인 sk를 가지고, 요청 메시지를 다음과 같이 생성한다.

$ID_{MTM}, ID_{USIM}, E_{PU_{CA}}[Auth\,Value, sk],$
$Sign_{AIK}[h(ID_{MTM}, ID_{USIM}, E_{PU_{CA}}[Auth\,Value, sk])]$

단계 2. CA는 복구 요청 메시지의 서명을 다음과 같이 검증한다.

$h(ID_{MTM}, ID_{USIM}, E_{PU_{CA}}[Auth\,Value, sk]$
$\stackrel{?}{=} D_{PU_{AIK}}[Sign_{AIK}[h(ID_{MTM}, ID_{USIM}, E_{PU_{CA}}[Auth\,Value, sk]]]$

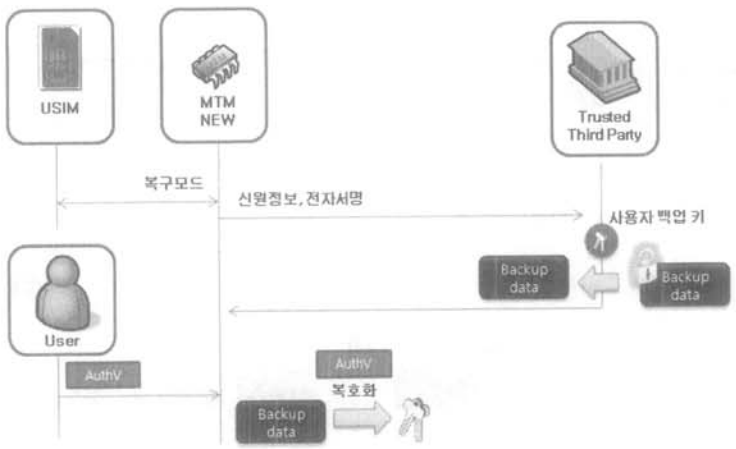
검증 후에, ID_{USIM}, ID_{MTM}에 대응되는 백업키를 자신의 저장소에서 찾는다.

단계 3. CA는 자신에 저장되어 있는 해당 사용자의 백업키와 백업 데이터를 찾은 후, 백업 개인키로 해당 복구 정보를 복호하여, 사용자의 *UserKey*를 복구한다.

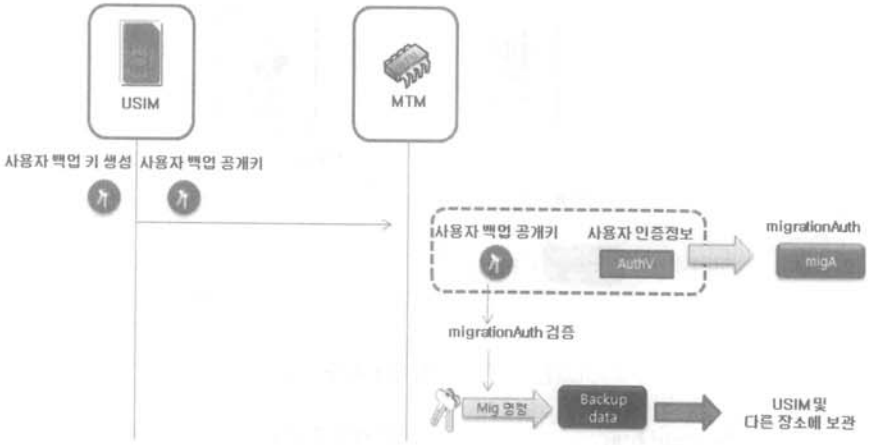
$UserKey = D_{PR_{bk}}[D_{Auth\,Value}[EncOut]]$

복구된 *UserKey*는 임시 세션키인 sk에 의해 $E_{sk}[UserKey]$과 같이 암호화 되어 CA의 전자 서명과 함께 다시 단말기에 전송되게 된다.

단계 4. 단말기는 CA로부터 sk로 암호화된 *UserKey*를 전송받고, sk로 복호하여 사용자의 *UserKey*를 MTM에 등록하게 된다.



(그림 7) 제안방식 2의 복구 과정



(그림 8) 제안방식 3의 초기 설정 과정 및 백업 과정

4.2.3. CMK와 USIM을 사용한 키 백업 및 복구 방안 (제안방식 3)

본 제안 방식은 USIM을 MTM이 인증할 수 있으며, 이에 따라서 USIM의 인증된 백업키를 사용하는 방식이다. 먼저 사용자는 정당한 USIM의 소유자임을 인증 받았고, MTM의 소유자 인증 과정을 마쳤다고 가정한다. 또한 백업키는 USIM으로부터 인증되어 MTM이 신뢰하는 키이다.

4.2.3.1. 초기 설정 과정

단계 1. 사용자의 USIM은 초기 발급시에 백업키로써 PU_{bk}/PR_{bk}를 생성하여 USIM에 저장한다.

단계 2. 사용자는 단말기의 MTM에 대한 인증을 수행한 후에, 사용자의 서브 루트키인 *UserKey*를 SRK 아래 생성하게 된다. 이때 *UserKey*는 CMK의 속성을 가지며, 이에 따라서 USIM으로부터 인증된 백업키인 PU_{bk}를 CMK의 인증 객체로 사용한다. 이 과정에서 이전을 위한 인증정보인 *migrationAuth*는 다음과 같이 연산되어 *UserKey*의 이전 인증 정보로 사용된다.

$$migrationAuth = H(tpmProof, H(PU_{bk}), H(PU_{UserKey}))$$

4.2.3.2. 백업 과정

백업 과정은 사용자의 서브 루트키인 *UserKey*를 외부에 백업하기 위해 백업키로 암호화 하는 과정이다. 본 과정에 앞서 이미 사용자는 USIM과 단말기를 검증하고, 소유자 인증을 수행하였다고 가정한다.

단계 1. 사용자는 이전 명령어를 수행하여 사용자 서브 루트키인 *UserKey*의 CMK 암호화 데이터의 생성을 MTM에 요청한다. 요청시에는 암호화 하고자 하는 대상 키인 *UserKey*와 백업키로써의 USIM으로부터 받은 PU_{bk}를 같이 제공한다.

단계 2. MTM은 사용자의 요청에 따라서 암호화 하고자 하는 대상 키인 *UserKey*의 migrationAuth를 검증한다. migrationAuth에 명시된 자신의 비밀값으로써의 *tpmProof*와 백업키 PU_{bk}, 그리고 백업 대상인 사용자 루트키인 $PU_{UserKey}$를 가지고 계산하여 *UserKey*의 migrationAuth를 다음과 같이 검증한다.

$$H(tpmProof, H(PU_{bk}), H(PU_{UserKey})) \stackrel{?}{=} migrationAuth$$

단계 3. 검증이 통과된 후에는 사용자 키를 백업키로 암호화 하여 *UserKey*에 대한 백업 데이터 *BackupData*를 생성한다.

$$BackupData = E_{PU_{bk}}[PR_{UserKey}]$$

생성된 *BackupData*는 네트워크 저장소나, USIM등의 별도의 저장소에 따로 보관하게 된다.

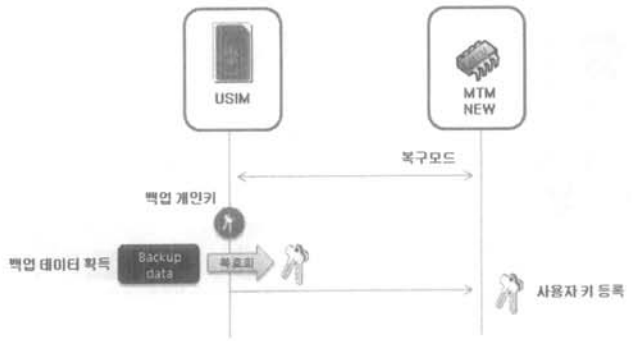
4.2.3.3. 복구 과정

복구 과정은 백업 데이터를 가지고 단말기에 사용자 키를 복구하는 과정이다. 이 과정을 위해서 단말기는 복구를 위한 특정한 상태로써 복구 모드가 되어야 한다.

단계 1. 먼저 사용자는 새로운 단말, 혹은 기존의 초기화된 단말기에 USIM을 삽입하고, 단말이 제공하는 복구 모드로 들어가게 된다.

단계 2. MTM은 복구 정보인 *BackupData*를 다른 사용자의 저장매체를 통해 제공받는다. 제공받은 후에는 *BackupData*를 USIM에 다시 전송한다. 만약 *BackupData*가 USIM에 저장된 경우에는 MTM에 전송할 필요는 없다.

단계 3. USIM은 전송된 백업 데이터를 자신의 백업 개인키로 복호한다.



(그림 9) 제안방식 3의 복구 과정

$$UserKey = D_{PR_{bk}}[BackupData]$$

복호된 *UserKey* 개인키는 MTM에 전송되어 사용자 루트키로써의 역할을 하게 되고, 기존에 암호화 되었던 사용자 데이터를 접근할 수 있게 된다.

5. 제안 방식 분석

본 논문에서는 백업 및 복구를 사용하여 사용자의 암호키를 이전하는 방안들로써 모바일 환경의 다양한 단말의 교체 상황에 대해 세 개의 방안으로 제안되었다. 각각의 교체 상황에 따라 적용할 수 있는 방안을 따로 제시하였다. 제안된 상황은 *UserKey*가 MTM 내부에서 생성되며 백업키로 암호화되어 백업 데이터를 생성하는 구조를 가지고 있다. 이 과정에서 백업 키의 관리는 USIM과 MTM, 그리고 외부의 신뢰 개체의 의해 이루어 질 수 있으며 백업 데이터는 USIM이나 단말기, 혹은 외부 신뢰 개체에 저장될 수 있다.

첫 번째로 사용자의 의도적인 단말의 교체 상황에 대해서 CMK와 MTM 기반의 사용자 키 백업 및 복구 방안을 제안하였다. 이 방법은 사용자의 백업 키가 MTM 내부에 존재하는 경우이다. 이 경우에는 백업 과정이 MTM 내부에서 일어나게 되므로, 별도의 추가적인 메커니즘이 필요하지 않다. 그리고 생성된 암호화 데이터는 단말기의 키 트리 저장소에 저장이 되며, 추후에 MTM에 의해 손쉽게 복호될 수 있다. 복구를 위해서는 사용자가 MTM에 대한 소유자 인증을 수행한 후, 단말기의 *UserKey* 백업 데이터를 복호하게 된다. 백업키는 MTM의 관리 하에 있으므로 인증된 사용자에 의해 복구 과정이 일어날 수 있다.

두 번째로 단말의 분실 및 손상에 따른 교체 상황에 대해서 CMK와 외부 신뢰 기관을 사용한 백업 및 복구 방안을 제안하였다. 이 방법은 사용자의 백업 키가 외부의 신뢰 개체에의해 관리되는 경우이다. MTM 내부의 *UserKey*를 외부의 백업 키로 암호화하여 보관하게 되는데, 이 과정은 MTM이 사용자의 인증정보인 *Auth Value*와 백업키를 사용하여 이중 암호화되기 때문에, 외부 객체에 의한 안전한 백업데이터 관리가 가능하다.

마지막으로 단말의 MTM 모듈 손상에 따른 교체 상황에 대해서 CMK와 USIM을 사용한 키 백업 및 복구 방안을 제안하였다. 이는 사용자의 백업 키가 사용자 인증 모듈인 USIM에 저장되어 있는 경우이다. 이 경우에는 MTM 내부의 *UserKey*를 USIM의 사용자 암호키로 암호화 하여 보관하는 방법이다. 이 경우에는 USIM이 복구에 대한 복구키를 가지고 있는 개체로써 매우 중요하게 된다.

제안방식은 요구사항에 따라 다음 <표 2>와 같이 분석할 수 있다. 기본적으로 기밀성과 무결성의 경우에는 백업키와 백업데이터를 고려할 수 있다. 이는 각각이 저장되는 USIM이나 MTM의 안전성을 따라간다고 할 수 있다. 상용화 솔루션으로써 BitLocker은 사용자가 관리하는 부분이 크며, 복구에 있어 사용자가 복구 암호를 잘 관리해야 하고, Active Directory라는 인증 서버를 두어야 원격 관리가 가능하다. 복구를 위한 인증에 관해서는 백업키의 소유 개체에 대한 인증을 수행하는 것으로 볼 수 있다. 이에 따라서 제안방식 2, 3은 각각의 개체에 대한 인증으로 제공되고, 제안방식 1은 사용자의 MTM에 대한 소유자 인증 이외에 별도의 복구 메커니즘을 위한 추가적인 인증이 필요하다. BitLocker의 경우 윈도우 운영체제의 로그온이나 부팅시의 복구모드에서 복구 암호를 입력해야 한다. 사실상의 인증은 윈도우 운영체제의 사용자 계정과 연결되어 있다. 효율성 측면에서는 MTM을 백업 키와 백업 데이터의 저장소로 사용하는 방법이 외부 개체와의 통신이 없으므로 가장 효율적이며, USIM을 사용하는 방법 그리고 외부 신뢰 개체를 사용하는 것은 별도의 추가적인 암호 통신을 요구하므로 상대적으로 효율성이 부족하다고 분석된다. BitLocker의 경우에서는 디스크를 다른 곳으로 옮기기 위해 추가적인 복호과정이 요구된다. 이는 암호화를 통한 안전성에 비해 사용자의 편의성 및 효율성이 저하되는 부분이 있을 수 있지만, BitLocker은 모바일 환경이 아닌 일반 환경이라는 점을 고려할 필요가 있다. 백업에 대한 완전성 측면에서는 백업키와 데이터가 외부 개체에 의해 관리되는 제안방식 3이 완전성을 제공할 수 있으며, 제안방식 1, 2의 경우에는 사용자에 의해 관리되는 데이터로 인해 잠재적인 분실 가능성이 존재하게 된다. BitLocker도 다양한 복구 메커니즘을 가지고 있지만, 사용자에 의해 분실되거나, 저장 매체가 손상되는 경우에는 복구하기 어려운 점이 있다.

〈표 2〉 키 백업 및 복구 방식 분석

	BitLocker	제안방식 1	제안방식 2	제안방식 3
백업키의 기밀성	사용자 관리	MTM의 안전성	외부 신뢰기관의 안전성	USIM의 안전성
백업 데이터의 기밀성	제공	제공	제공	제공
무결성	외부 저장소	MTM 및 단말 저장소의 안전성	외부 신뢰기관의 안전성	USIM의 안전성
인증	윈도우 로그온	MTM의 사용자 인증이 외에 추가 인증 필요	백업 키에 대한 소유자 인증	USIM의 소유자 인증
효율성	다양한 복구 메커니즘 제공	별도의 외부 객체와 통신이 필요 없음	추가적인 외부 신뢰기관과의 암호 통신 필요	추가적인 USIM과 MTM간의 통신 필요
백업 키의 보관	사용자 관리 및 MS 인증서버	MTM의 키 트리에 존재	외부 신뢰기관에 존재	USIM에 존재
백업 키의 분실 가능성	있음	있음	없음	있음
완전성	인증 서버 및 저장매체 손상 가능성 존재	단말기에 대한 분실 가능성 존재	제공	USIM에 대한 분실 가능성 존재

5. 결 론

신뢰 컴퓨팅은 향후 유비쿼터스 환경에서 중요한 보안 기술로 그 역할을 할 것이다. 신뢰 컴퓨팅은 기존의 소프트웨어 기반의 보안 아키텍처와 다르게 하드웨어 보안 모듈을 사용한 신뢰를 기반으로 하는 보안 프레임 워크이다. 이러한 신뢰 컴퓨팅은 향후 컴퓨팅 환경이 모바일 환경으로 이동함에 따라, 모바일 환경에서의 주요한 보안 프레임 워크로 그 기능을 할 것임은 자명한 사실이다

본 장에서는 안전한 모바일 환경을 위해 신뢰 컴퓨팅을 적용하는 것에 따른 단말의 이동성에 대한 문제점을 지적하고, 그에 대한 해결 방안으로 사용자 루트 암호키의 백업과 복구를 통해 단말의 교체시에 사용자가 사용하던 데이터들을 안전하게 관리하는 방안에 대해서 분석하였다. 이를 위해 TCG의 CMK를 응용하여 외부 신뢰 기관이나 USIM을 MA/MSA로 활용하여 사용자 루트 암호키를 안전하게 암호화하여 MTM 외부에 저장하는 방안을 제시하였다.

점차 증가하고 있는 보안 위협 속에 신뢰 컴퓨팅은 그 해결 방안을 제시할 수 있는 보안 기술로 부각되고 있다. 향후 신뢰 컴퓨팅을 적용하기 위한 보다 많은 연구가 필요할 것이다.

참 고 문 헌

[1] A. K. Ghosh, Tara M. Swaminatha, "Software security and privacy risks in mobile e-commerce," Communications of the ACM, Vol 44, No 2, pp.51-57, 2001.

[2] E. Gallery, C. J. Mitchell, "Trusted Mobile Platforms," Foundations of Security Analysis and Design IV, LNCS 4677, pp.282-323, 2007.

[3] J. Lindqvist, Laura Takkinen, "Privacy Management for Secure Mobility," WPES'06, 2006.

[4] Ulrich Kuhn, Klaus Kursawe, Stefan Lucks, "Secure Data Management in Trusted Computing," CHES 2005, LNCS 3659, pp.324-338, 2005.

[5] 김무섭, 신진아, 박영수, 전성익, "모바일 플랫폼용 공통보안핵심 모듈 기술," 정보보호학회지, 제 17권, 제 3호, pp.7-17, 2006.

[6] 김영수, 박영수, 박지만, 김무섭, 김영세, 주홍일, 김명은, 김학두, 최수길, 전성익, "신뢰 컴퓨팅과 TCG 동향," 전자통신동향분석, 제 22권 제 1호, pp.83-96, 2007.

[7] Trusted Computing Group, "Backgrounder," 2006.

[8] Trusted Computing Group, "Mobile Trusted Module Specification General Overview FAQ," 2007.

[9] Trusted Computing Group, "Mobile Phone Work Group Use Cases," 2005.

[10] Trusted Computing Group, "TCG TPM Specification Version 1.2 Revision 103," 2007

[11] Trusted Computing Group, "TCG Specification Architecture Overview," Revision 1.4, 2007.

[12] Microsoft, "Windows Vista BitLocker Drive Encryption: Technical Overview", http://technet.microsoft.com/en-us/windowsvista/ aa906017.aspx

강 동 완

e-mail : lupin428@gmail.com

2007년 순천향대학교 정보기술공학부 졸업(학사)

2009년 순천향대학교 대학원 컴퓨터학과 (공학석사)

2009년~현 재 한국정보호진흥원 연구원

관심분야 : TPM, 키 관리, 네트워크 보안

전 성 익

e-mail : sijun@etri.re.kr

1987년~2001년 한국전자통신연구원 책임연구원

2001년~2009년 한국전자통신연구원 무선보안응용연구팀장

2009년~현 재 한국전자통신연구원 SW서비스연구팀 책임연구원

관심분야 : 운영체제, 실시간 시스템, 스마트카드, USIM, TPM 등 정보보호 기반 기술 등

이 임 영

e-mail : imylee@sch.ac.kr

1981년 홍익대학교 졸업(학사)

1986년 오사카대학 통신공학전공(공학석사)

1989년 오사카대학 통신공학전공(공학박사)

1985년~1994년 한국전자통신연구원 선임연구원

1994년~현 재 순천향대학교 컴퓨터학부 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안