情 報 保 護 學 會 誌
第 14 券 第 2 號, 2004. 4

NIST SP 800-57 키 관리 가이드라인 분석†

이 진 우*, 곽 진*, 양 형 규**, 원 동 호***

요 약

최근, 인터넷의 보급이 일반화되면서 네트워크를 통해 다양한 전자상거래 서비스가 활성화되고 있다. 이러한 서비스는 전송되는 정보의 기밀성(confidentiality), 인증(authentication), 무결성(integrity), 부인봉쇄(non-repudiation)등의 정보보안 서비스를 제공하기 위해 암호기술이 요구된다. 이러한 암호기술의 안전성은 공개되어 있는 암호 알고리즘에 의존하는 것이 아니라, 암호 알고리즘에 사용된 키에 의해 좌우된다. 또한, 암호통신을 이용하는 개체가 증가함에 따라, 효율적인 키 관리의 필요성도 함께 증가하고 있다. 이에 본 고에서는 키 관리의 전반적인 개요와 효율적이고 안전한 키 관리를 위해 2003년도에 NIST에서 발표된 SP(Special Publication) 800-57 키 관리 가이드라인을 분석한다.

Ⅰ. 서 론

유·무선 및 초고속 통신망 보급으로 시간과 공간의 제약을 극복하고, 암호 통신은 실생활과 같은 인터넷 뱅킹, 주식거래, 전자입찰, 전자상거래 등의 응용분야로 널리 확대되고 있다. 이러한 응용분야의 확대로 인해 기업간의 거래는 물론 개체간의 암호 통신이 활성화되고 있다. 암호 통신에서의 안전성은 통신에 사용되는 암호 알고리즘에 의존하는 것이 아니라, 암호 알고리즘에 사용되는 키에 의해 좌우된다. 또한, 암호 통신을 사용하는 개체가 증가함에 따라 암호 통신에 사용되는 키의 수가 증가되고, 이에 보다 효율적이고 안전하게 키를 다룰 수 있는 키 관리(key management)기술이 필요하다. 그러나, 아직까지 암호 시스템에서 효율적이고, 안전한 키 관리 기술을 위한 지침서와 관련 자료들은 미비한 실정이다. 이에 본 고에서는 2001년도에 NIST에서 발표된 키 관리 지침서 이후, 2003년도에 새로 발표된 NIST SP 800-57 키 관리 가이드 라인을 분석하고자 한다.

본 고의 구성은 다음과 같다. 제 2장에서는 키 관리 개요에 대하여 살펴보고, 제 3장에서는 NIST SP 800-57 키 관리 가이드 라인을 바탕으로 암호학적 서비스들의 정의 및 각 알고리즘을 권장하는 표준문서에 대해 살펴본다. 또한, 키 생명주기 및 키 관리 주기에 대해 분석하고, 암호 알고리즘에 사용 되는 여러 가지 암호학적 키의 고려사항 및 유효기간, 권장 키 사이즈에 대해 분석한다. 마지막으로 4장에서 결론을 맺는다.

Ⅱ. 키 관리 개요

키 관리는 키 및 키 재료(key material)의 생성, 등록, 인증, 말소, 분배, 설치, 저장, 보관, 취소, 파생, 파기 등과 같은 서비스의 관리를 총칭한다. 키 관리의 목적은 키를 이용하는 모든 과정에서 안전성을 보장하기 위한 모든 절차를 규정하는 것이며, 키 관리 절차는 사용된 알고리즘, 키의 의도적인 사용, 그리고 사용에 대한 보안정책에 의해 좌우된다. 또한 암호화 장비에서 발생하는 사항도 포함한다.

1. 키 관리 서비스

키 관리는 생성, 등록, 인증, 분배, 설치, 저장, 파생, 보관, 취소, 말소, 폐기 등의 기본적인 키 관리 서비스를 포함한다. 이러한 서비스는 키 관리 시스템에

† 본 연구는 대학 IT 연구센터 육성·지원 사업의 연구결과로 수행되었음
* 성균관대학교 정보통신공학부 정보통신보호연구실 ({jwlee, jkwak}@dosan.skku.ac.kr)
** 강남대학교 컴퓨터미디어 공학부 부교수 (hkyang@kns.kangnam.ac.kr)
*** 성균관대학교 정보통신공학부 정교수 (dhwon@dosan.skku.ac.kr)

의해 제공되거나 신뢰성 있는 제 3의 신뢰기관에 의해 제공될 수 있다. 이 때 신뢰기관은 모든 객체가 신뢰할 수 있도록 보안 요구사항을 만족시키는 범위 내에서 서비스를 제공해야 한다.

1.1 키 생성

키 생성은 암호학적으로 안전한 키를 생성하는 절차를 의미하며, 이 때 예측이 불가능하고 위조할 수 없는 랜덤 수(random number)를 사용해야 하며 재사용해서는 안 된다. 이는 하나의 키의 노출로 인해 그 키와 관련된 정보뿐만 아니라 노출된 키로부터 파생되었거나 관련되어 있는 다른 모든 키들에 대한 접근권한도 임의의 사용자에게 제공될 수 있기 때문이다.

1.2 키 등록

키 등록은 생성된 키를 정당한 사용자와 관련시키는 것으로 등록 기관(RA: Registration Authority)에 의해 이루어지며, 등록 기관은 키와 관련된 정보의 기록을 안전하게 유지해야 한다. 또한, 키 등록 기관은 키 등록뿐만 아니라 키를 말소시키는 역할도 수행한다.

1.3 키 인증서 생성

키 확인서는 보통 공개키와 객체의 연관성을 보장하는 인증서(certificate)라 하며 인증기관에 의해 생성된다. 인증기관(CA: Certification Authority)은 사용자로부터 키 인증에 대한 요구를 받은 경우 키 인증서를 생성한다.

1.4 키 분배

키 분배는 인가된 객체들 사이에 키 또는 키 재료가 안전하게 공유되는 것을 의미한다. 비대칭 암호 방식에서는 키를 분배하는 특정 메커니즘을 사용하고, 대칭 암호 방식에서는 키 전송 센터(KTC : Key transport center), 키 분배 센터 (KDC : Key distribution center)에 의해 분배가 이루어진다.

1.5 키 설치

키 설치는 키를 사용하기 전에 필요한 절차로 키 관리 시스템 내에서 안전하게 제공되어야 한다.

1.6 키 저장

키 저장은 키를 사용하거나 복구를 위한 백업을 위해 키를 안전하게 저장하는 것을 의미한다. 이 때, 키는 물리적으로 안전한 장치에 저장되는 것이 바람직하며, 저장된 키 재료에 대하여 기밀성 및 무결성을 제공하여야 한다. 키 저장은 키의 생명주기(key life-cycle)동안의 모든 상태(활성 준비, 활성, 활성 종료 등)에서 발생할 수 있다.

1.7 키 유도

키 유도는 원본 키(original key)로부터 파생(derivation key)를 유도하는 것으로 유도된 키가 원본 키를 노출시키지 않도록 하기 위해서 유도 연산은 역 변환이 불가능하고 예측 불가능해야 한다.

1.8 키 보관

키 보관은 키의 일반적인 사용이 중단된 이후, 그 키의 오용 등의 문제가 발생했을 경우 그러한 사실을 증명하는데 키가 사용될 수 있도록 하기 위해 이루어진다.

1.9 키 복구

키 복구는 합법적 상황에서 암호문을 복호화 하거나, 사용자가 자신의 비밀키를 분실했을 경우 등의 유사시에 허가된 사용자만이 복호화를 할 수 있는 기능을 제공하기 위해 수행된다.

1.10 키 취소

키 취소는 키의 오용이 의심되거나 알려진 경우 키 취소는 키의 안전한 비 활성 상태를 유지하기 위해 이루어진다. 키 취소는 키 삭제라고도 하며, 유효기간이 만료된 키나 소유자의 환경이 변경된 경우 발생한다. 키가 취소된 후에는 단지 키와 관련된 정보의 복호화나 검증만을 위해 사용된다.

1.11 키 말소

키 말소는 키와 객체의 관계를 제거하는 것으로, 키 등록 기관에 의해 폐기 과정의 일부분으로 제공된다.

1.12 키 폐기

키 폐기는 더 이상 사용될 필요가 없는 키의 안전한 폐기를 위해 이루어진다. 키를 폐기한다는 것은 키와 관련된 모든 기록을 제거함으로써 폐기 후에 남아

있는 어떠한 정보를 가지고도 폐기된 키를 다시 복구시킬 수 없도록 하는 것을 의미한다. 또한, 이는 사용되는 키뿐만 아니라 보관된 모든 복사본에 대한 폐기도 포함한다. 보관된 키를 폐기할 때는 보관된 키에 의해 보호된 자료가 더 이상 필요 없는지의 여부를 사전에 판단 하여야한다.

Ⅲ. NIST SP 800-57 키 관리 가이드라인

본 장에서는 NIST SP 800-57 키 관리 가이드라인에서 정의하고 있는 정보보안 서비스, 암호알고리즘 및 기능, 규격에 대해 알아보고, 여러 가지의 암호학적 키의 유효기간 및 권장 키 사이즈에 대해 분석한다.

1. 정보보안 서비스

암호기술은 기밀성, 데이터 무결성, 인증, 부인방지와 같은 보안 서비스들을 제공한다. 그 정의는 다음 〔표 1〕과 같다.

정보보안 서비스들은 독립적으로 서비스가 제공되기도 하며, 보안 서비스들을 지원해주는 형태로 제공된다. 예를 들어, 암호학적 서비스들은 키 설정(key establishment), 랜덤 수 생성 서비스(random number generation services)들이 요구되며, 많은 어플리케이션들은 여러 가지의 보안 서비스들의 결합을 필요로 한다. 이에 보안 시스템을 설계하는 설계자들은 보안 시스템이 제공할 보안 서비스들을 고려하여 설계해야 한다. 암호 알고리즘들은 여러 가지의 보안 서비스들은 동시에 제공한다. 예를 들어, 전자 서명 알고리즘(digital signature algorithm)은 인증, 데이터의 무결성 및 부인방지 모두 제공한다.

〔표 1〕 정보보안 서비스

기밀성	비인가자가 부당한 방법으로 정보를 입수한 경우에도 정보의 내용을 알 수 없도록 하는 서비스
데이터 무결성	데이터가 전송 도중 또는 DB에 저장되어 있는 동안 악의의 목적으로 위조 또는 변조되는 것을 방지하는 서비스
인증	송·수신자가 상대방의 신원을 확인·식별하는 서비스
부인방지	송·수신 당사자가 각각 전송된 송수신 사실을 추후에 부인하는 것을 방지하는 서비스

2. 암호 알고리즘

2.1 암호 알고리즘의 분류

일반적으로 암호 알고리즘은 해쉬 알고리즘(hash algorithms), 대칭키 알고리즘(symmetric algorithms)과 비대칭키 알고리즘(asymmetric algorithms)으로 크게 세 가지로 분류되며, 키 관리 형태에 따라 대칭키와 비대칭키 알고리즘으로 분류되기도 한다. 해쉬 알고리즘은 키가 요구되지 않으며, 큰 메시지로부터 축소된 작은 메시지를 생성한다. 또한, MAC(message authentication code), 전자서명(digital signature), 키 설정(key establishment), 랜덤 수 생성(random number generation) 등 많은 암호화 과정의 구성요소로서 사용된다. 대칭키 알고리즘은 다른 말로 비밀키 알고리즘이라고 하며, 암호화키와 복호화키가 일치한다는 특징을 가지고 있다. 비대칭키 알고리즘은 공개키 알고리즘이라고도 불리며, 이 알고리즘은 대칭키 알고리즘과는 달리 공개키와 개인키 쌍이 존재하고, 공개키는 누구나 알 수 있으나, 공개키가 알려지더라도 개인키에 대한 어떠한 정보도 알 수 없다.

2.2 알고리즘의 기능

정보보안 서비스들을 제공하기 위하여 다수의 다른 알고리즘들이 사용되기도 하며, 같은 알고리즘이 다중 서비스를 제공하기 위해서 사용되어지기도 한다.

2.2.1 해쉬 함수

해쉬 함수는 임의의 길이의 입력 값을 고정된 작은 크기의 결과 값으로 생성하며, 해쉬 함수들은 다수의 보안 서비스들을 제공하기 위하여 다른 알고리즘들과 함께 사용된다. 예를 들어, 해쉬 함수는 전자서명을 하기 위해 전자서명 알고리즘과 함께 사용되며, 랜덤 수 생성기의 부분으로도 사용하고, 키 해쉬 메시지 인증 코드를 제공하기 위한 입력 값의 한 부분으로서 키와 함께 사용된다. NIST에서 권장하는 해쉬 함수 표준은 다음 〔표 2〕와 같다.

〔표 2〕 해쉬 함수 표준

FIPS 198	HMAC(Hash Message Authentication code)
FIPS 180-2	SHA-1, SHA-256, SHA-384, SHA-512

2.2.2 암·복호화 알고리즘

암호화 알고리즘은 데이터의 기밀성을 제공하기 위하여 사용된다. 암호문은 복호화 알고리즘을 통하여 평문으로 전환될 수 있다.

■ Advanced Encryption Standard(AES)

AES 알고리즘은 FIPS 197에 상술되어져있다. AES의 암호화와 복호화는 128비트 블록단위이며 128, 192, 256비트의 키가 사용된다. 각 다른 크기의 키를 갖는 AES의 명명법은 AES-x이고 x는 키 크기이다. 세 가지 키 크기 모두 연방정부 실용성에 적합하게 고려되었다.

■ Triple DES (TDES)

TDES는 ANSI X9.52에 정의되어 있으며, FIPS 46-3에서 채택되었다. TDES는 64비트 블록단위의 데이터를 암호화 복호화하고 56비트의 키를 사용한다.

NIST에서 권장하는 암·복호화 알고리즘 표준은 다음 〔표 3〕과 같다.

〔표 3〕 암·복호화 알고리즘 표준

FIPS 197	AES(Advanced Encryption Standard)
ANSI X9.52 FIPS 46-3	TDES(Triple DES), ANSI X9.52에 정의되어 있으며, FIPS 46-3에서 채택

2.2.3 MAC

MAC은 메시지 인증과 무결성을 제공하며, 검사합(checksum)을 이용하여 데이터의 변조 방지를 제공한다. 전자서명과 달리 특정 송·수신자간의 메시지 인증을 수행하기 위해 사용된다. NIST에서 권장하는 MAC 표준은 다음 〔표 4〕와 같다.

〔표 4〕 MAC 표준

SP 800-38B	MACs Using Block Cipher Algorithms
FIPS 198	MACs Using Hash Functions

2.2.4 전자서명 알고리즘

전자서명 알고리즘들은 인증, 무결성, 부인방지를 제공하기 위하여 사용되며 해쉬 알고리즘과 함께 이루어진다.

■ DSA

DSA 전자서명 알고리즘은 FIPS 186-2에서 정의하고 있다.

■ RSA

ANSI X9.31과 PKCS#1에서 상술된 RSA 알고리즘은 FIPS 186-2에서 전자서명의 계산을 위하여 채택되었다.

■ ECDSA

ANSI X9.62에 상술되어있는 타원 곡선 전자서명 알고리즘은 FIPS 186-2에서 전자서명의 계산을 위해 채택되었다. ANSI X9.62에서는 최소의 키 사이즈에 대하여 상술되어 있다. ECDSA는 키 사이즈의 두 배 길이의 디지털 서명을 생성한다. 권장하는 타원 곡선 전자서명 알고리즘은 FIPS 186-2에서 제공한다.

NIST에서 권장하는 전자서명 알고리즘 표준은 다음 〔표 5〕와 같다.

〔표 5〕 전자서명 알고리즘 표준

FIPS 186-2	DSA
ANSI X9.31	RSA
ANSI X9.62	ECDSA

2.2.5 키 설정 알고리즘

키 설정 알고리즘들은 통신하는 개체들 사이에서 키들을 설치하기 위하여 사용되어진다. 키 설정은 키 전송과 키 동의로 나뉘어진다.

키 동의 과정동안 설정되는 키 자료들은 전송되지 않고, 키 자료 계산을 위해 필요한 정보가 개체간에 교환된다. 일반적으로 키 동의 기법은 비대칭키 기술을 사용하며 키 전송 기법은 대칭키/비대칭키 기법 모두 사용한다.

■ 이산대수 키 동의 스킴

유한체 상에서 연산하는 이산대수 문제의 어려움에 기반한 키 동의 스킴들은 ANSI X9.42에 정의되었다.

■ RSA 전송

RSA 키 전송 스킴들은 ANSI X9.44에 정의되었다.

■ 타원곡선 키 동의/키 전송

타원 곡선 상에서 이산대수 문제의 어려움에 기반한 타원 곡선 키 동의와 키 전송 스킴들은 ANSI X9.63에 정의 되어있다. 11개의 키 동의 스킴들 중 7개가 채택되어졌다.

■ Key Wrapping

key wrapping은 대칭키 알고리즘을 사용한 키 암호화키에 의한 키의 암호화이다.

NIST에서 권장하는 키 설정 알고리즘 표준은 다음 〔표 6〕과 같으며, SP800-56에서 자세히 정의하고 있다.

〔표 6〕 키 설정 알고리즘 표준

ANSI X9.42	Discrete Log Key Agreement Schemes Using Finite Field Arithmetic
ANSI X9.44	RSA Key Transport
ANSI X9.63	Discrete Log Key Agreement Schemes Using Elliptic Curve Arithmetic

2.2.6 랜덤 수 생성기

랜덤 수 생성기는 키 생성 재료의 생성을 위해서 요구되어진다. RNG(Random number generator)는 결정적과 비결정적 두 분류로 정의되어 진다. 결정적 RNG는 랜덤 수를 생성하기 위해 키 생성 재료와 암호학적 알고리즘들을 사용하며, 일반적으로 pseudo random number generate라 불려진다. 비 결정적 RNG는 예측 불가능한 물리적 소스에 의존하여 결과를 생성한다. pseudo random number generation 알고리즘은 다양한 암호학적 어플리케이션들에 사용하기 위해 FIPS 186-2, ANSI X9.31, ANSI X 9.62에서 정의되어 있다. NIST에서 권장하는 랜덤 수 생성기 표준은 다음 〔표 7〕과 같다.

〔표 7〕 랜덤 수 생성기 표준

FIPS 186-2 ANSI X9.31 ANSI X9.62	Random Number Generation

3. 암호학적 키 분류 및 유효기간

본 장에서는 암호 시스템에 사용되는 여러 가지의 키를 분류하여 정의하고, 키의 보안사항 및 유효기간에 대해 알아본다.

3.1 키의 사용

암호 시스템에서 사용되는 키들은 하나의 목적으로만 사용해야만 한다. 키는 각각의 목적에 맞게 사용되어야 하며, 그 키가 다른 목적으로 사용된다면 여러 가지 공격에 노출될 위험이 존재하게 된다. 만약, 키가 노출되었거나, 사용의 의심스러운 경우 즉시 키의 사용을 제한하여야 한다.

3.2 키의 분류 및 유효기간

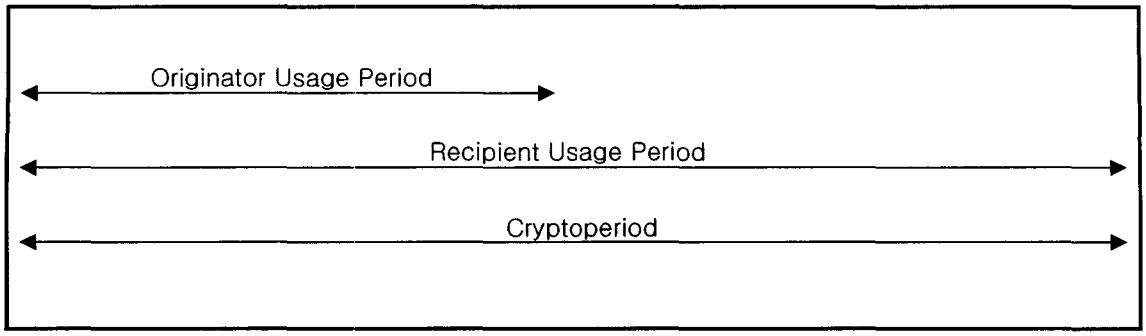
키는 각 알고리즘에 따라 분류되며, 키의 유효기간은 정당한 개체가 정의된 키를 가지는 합법적인 키의 기간으로 다음과 같은 보안요구사항을 만족하여야 한다.

① 공격 가능한 키에 의해 보호된 정보를 제한
② 주기(lifetime)가 추측된 알고리즘의 사용을 제한
③ 노출된 키의 사용 제한
④ 물리적, 논리적 공격이 가능한 시간을 제한
⑤ 공격자에 의해 정보가 노출되지 않도록 기간을 제한

키의 유효기간에 영향을 미치는 요소로는 암호 시스템 동작환경 또는 작업 환경 등을 들 수 있다. 일반적으로 키를 보호하기 위해 사용된 키 암호화 키는 암호통신에 사용되는 키 보다 오랜 기간의 유효기간이 요구되며, 공개키·개인키 쌍에서 각 키들은 서로 다른 유효기간을 가지게 된다. 대칭키의 유효기간은 키의 생성자가 사용하는 키의 기간과 수신자가 사용하는 키의 기간으로 구성된다. 생성자의 사용 기간은 키가 암호학적 처리에 사용될 때부터 사용되지 않을 때까지이다. 다음 〔그림 1〕은 일반적인 대칭키의 유효기간을 나타내고 있다.

각 알고리즘에 사용되는 여러 가지의 키들의 정의 및 고려사항, 유효기간은 다음과 같다.

■ Private signature key : 비대칭키 알고리즘의 키쌍 중에 개인키로서 일반적인 서명을 생성할 때 사용되는 키



〔그림 1〕 대칭키 유효기간

① 고려사항 : 개인 서명키의 유효기간은 공개 서명 검증키의 유효기간보다 짧다.
② 유효기간 : FIPS의 승인된 알고리즘과 키의 크기, 키 저장과 사용 환경의 안전성이 키의 유효기간에 영향을 미친다. 최대 키의 유효기간은 3년이다.

- Public signature verification key : 비대칭키 알고리즘의 키쌍 중에 공개키로서 일반적인 서명을 검증할 때 사용되는 키
  ① 고려사항 : 공개 서명 검증키의 유효기간은 개인 서명키의 유효기간보다 길다. 일반적으로 검증키는 개인키가 서명에 사용된 후 검증하는데 사용되므로 유효기간이 길다. 비교적 작은 안전성을 요구한다.
  ② 유효기간 : 최대 유효기간은 10년이다.

- Symmetric authentication key : 대칭키 알고리즘에서 개체의 인증 또는 메시지 소스 및 저장된 데이터를 정보의 무결성을 보장하기 위한 키
  ① 고려사항 : 하나의 키를 사용하며, 키의 노출은 정보를 바로 노출시킨다. MACs은 인증을 위해 사용되며, 한번 적용한 정보는 다시 복수 할 수 없다.
  ② 유효기간 : FIPS의 승인된 알고리즘과 키의 크기, 키 저장과 사용 환경의 안전성이 키의 유효기간에 영향을 미친다. 최대 키의 유효기간은 2년까지이다.

- Private authentication key : 비대칭키 알고리즘의 키쌍 중에 개인키로서 정보의 무결성, 개체의 인증 또는 메시지 소스 및 저장된 데이터를 보장하기 위한 키
  ① 고려사항 : 개인 인증키는 여러 번에 걸쳐 사용되며, 이에 상응하는 공개키는 신뢰기간의 인증을 받는다. 대부분의 경우, 인증 개인 키의 유효기간은 관련된 공개키의 유효기간과 같다.
  ② 유효기간 : 인증된 정보의 중요성에 따라 다르지만, 유효기간은 1-2년이다.

- Public authentication key : 비대칭키 알고리즘의 키쌍 중에 공개키로서 정보의 무결성, 개체의 인증 또는 메시지 소스 및 저장된 데이터를 보장하기 위한 키
  ① 고려사항 : 공개 인증키의 유효기간은 개인 인증키의 유효기간과 같다.
  ② 유효기간 : 인증된 정보의 중요성에 따라 다르지만, 유효기간은 1-2년이다.

- Symmetric data encryption key : 대칭키 알고리즘에서 정보의 기밀성을 적용하기 위한 키
  ① 고려사항 : 대칭 데이터 암호화 키는 짧은 데이터를 암호화하거나, 통신세션에 사용되는 키이다. 암호화하는 데이터의 크기에 따라 키의 유효기간이 달라지며, 비교적 다른 키에 비해 짧은 유효기간을 가진다. 대칭키의 노출은 바로 정보의 노출이 됨을 주의하여야 한다.
  ② 유효기간 : 암호화되는 정보의 양이 많으면 몇 일에서 몇 주 정도의 유효기간을 가지며, 정보의 양이 적으면 최대 한달 정도의 유효기간을 가진다.

- Symmetric key wrapping key : 대칭키 알고리즘을 사용하여 다른 키를 암호화하는 키로, 키 암호화 키(key encryption key)라고도 한다.
  ① 고려사항 : 대칭키 암호화 키는 키의 크기에 따

라 유효기간이 다르다.

② 유효기간 : 큰 수의 키들을 암호화하는데 사용하는 키 암호화 키는 몇 일에서 몇 주일 정도의 유효 기간을 지니며, 작은 수의 키를 암호화하는데 사용하는 키 암호화 키는 최대 한 달까지의 유효기간을 가진다.

- Random number generation key : 대칭키 알고리즘 또는 해쉬 함수와 함께 랜덤수를 생성하기 위한 비밀키
  ① 고려사항 : 키가 사용되는 양에 따라 키의 유효기간이 다르다.
  ② 유효기간 : 한 달에서 최대 두 달 사이의 기간을 가지는 게 적합하다.

- Symmetric master key : 대칭 마스터 키는 다른 대칭키들(data encryption key, key Wrapping key, authentication key)을 유도하기 위한 키
  ① 고려사항 : 적합한 키의 유효기간은 마스터 키로부터 유도된 키들의 사용이나 특성에 좌우된다. 마스터 키로부터 유도된 키들의 유효기간은 비교적 짧으며, 통신의 세션 등에 사용된다. 같은 마스터 키로 유도된 키들은 보통 다른 목적으로 사용된다.
  ② 유효기간 : 사용환경이나 인증된 정보의 중요성에 따라 다르지만 일반적으로 1년의 유효기간을 가진다.

- Private key transport key : 비대칭키 알고리즘의 키쌍 중에 개인키로서 비대칭키 알고리즘에서 복호화 하기 위한 키들을 위해 사용된다. 키 전송키는 보통 키 설정(key wrapping key, data encryption key 또는 MAC key) 을 위해 사용된다.
  ① 고려사항 : 개인 키 전송키는 여러 번에 걸쳐 사용된다. 개인 키 전송키는 때때로 키들을 복호화 하는데 필요하기 때문에 이에 상응하는 공개키 보다 길다.
  ② 유효기간 : 아래와 같은 요인에 따라 키의 유효기간이 달라지며, 최대 2년까지이다.
  - 승인된 FIPS 알고리즘의 사용과 키의 크기
  - 키에 의해 암호화된 정보의 크기
  - 키의 저장과 사용환경

- Public key transport key : 비대칭키 알고리즘의 키쌍 중에 공개키로서 비대칭키 알고리즘에서 암호화하기 위한 키들을 위해 사용된다. 키 전송키는 보통 키 설정(key wrapping key, data encryption key 또는 MAC key)을 위해 사용된다.
  ① 고려사항 : 공개키 전송키의 유효기간은 암호연산에 키가 사용될 때의 기간이며, 개인키 전송키에 비해 키의 유효기간이 짧다.
  ② 유효기간 : 최대 2년의 유효 기간을 가진다.

- Symmetric key agreement key : 키 동의키는 키 설정(key wrapping key, data encryption key 또는 MAC key) 그리고 다른 키 자료(Initialization Vectors)를 위해 사용된다.
  ① 고려사항 : 대칭 키 동의키는 여러 번 사용되며, 키의 유효기간은 다음과 같은 요소에 의해 달라진다.
  - 기본적인 안전성 요소
  - 키 설정에 사용되는 키의 크기와 특성
  - 키 동의 알고리즘과 사용되는 프로토콜
  - 대칭 키 동의 키 는 대칭 키 설정에 사용된다.
  ② 유효기간 : 아래와 같은 사항에 따라 1-2년의 키 유효기간을 가진다.
  - NIST에 사용된 알고리즘
  - FIPS 140-2에서 요구된 장치
  - SP 800-37에서 정의된 안전레벨

- Private static key agreement key : 비대칭키 알고리즘의 키쌍 중에 개인키로서 키 동의키는 키 설정(key wrapping key, data encryption key 또는 MAC key) 그리고 다른 키 자료(Initialization Vectors)를 위해 사용된다.

  ① 고려사항 : 개인 고정 키 동의키는 여러 번에 걸쳐 사용되며, 대칭키 동의키의 경우와 같이 요소에 따라 키 유효기간은 달라진다.
  ② 유효기간 : 개인 고정 키 동의키와 그와 상응된 공개키는 같은 유효기간을 가지며, 아래와 같은 사항에 따라 1-2년의 키 유효기간을 가진다.
  - NIST에 사용된 알고리즘
  - FIPS 140-2에서 요구된 장치
  - SP 800-37에서 정의된 안전레벨

- Public static key agreement key : 비대칭키 알고리즘의 키쌍 중에 공개키로서 키 동의키는 키 설정(key wrapping key, data encryption key 또는 MAC key) 그리고 다른 키 자료(Initialization Vectors) 을 위해 사용된다.
  ① 고려사항 : 공개 고정 키 동의키의 유효기간은 관련된 개인 고정 키 동의키의 유효기간과 같다.
  ② 유효기간 : 공개 고정키 동의키의 유효기간은 개인 고정 키 동의키와 같다.

- Private ephemeral key agreement key : 비대칭키 알고리즘의 키쌍 중에 개인키로서 키 설정시 단 한번만 사용되는 키
  ① 고려사항 : 개인 일회용 키 동의키는 키 설정에서 사용되는 비대칭키 쌍의 개인 키 요소이다. 개인 일회용 키 동의키는 대칭키 혹은 키 재료를 설정하는데 사용된다.
  ② 유효기간 : 개인 일회용 키 동의키는 한번 사용되는 키이며, 개인 일회용 키 동의키의 유효기간은 키 동의가 수행되는 동안이다.

- Public ephemeral key agreement key : 비대칭키 알고리즘의 키쌍 중에 공개키로서 키 설정시 단 한번만 사용되는 키
  ① 고려사항 : 공개 일회용 키 동의키는 설정에서 오직 한번 사용되는 비대칭키의 공개키 요소이다.
  ② 유효기간 : 오직 한번만 사용되며, 공개 일회용 키 동의 키는 키 동의가 수행되는 동안만 유효기간을 가진다.

- Symmetric authorization key : 대칭키 암호기법을 이용하여 개체의 권한을 주기 위해 사용되는 키
  ① 고려사항 : 대칭 인가키의 유효기간은 아래와 같은 방식에 따라 달라진다.
  - 적절한 암호방식의 사용
  - 적절한 키 보호 메커니즘의 사용
  ② 유효기간 : 아래와 같은 사항에 따라 최대 2년의 키 유효기간을 가진다.
  - 키의 저장과 사용환경의 안전성
  - FIPS에서 승인된 알고리즘과 키 크기 사용
  - 권한 과정 처리의 중요성

- Private authorization key : 비대칭키 알고리즘의 키쌍 중에 개인키로서 개체의 권한을 주기 위해 사용되는 키
  ① 고려사항 : 개인 인가키의 유효기간은 아래와 같은 방식에 따라 달라진다
  - 적절한 암호방식의 사용
  - 적절한 키 보호 메커니즘의 사용
  ② 유효기간 : 아래와 같은 사항에 따라 최대 2년의 키 유효기간을 가진다.
  - 키의 저장과 사용환경의 안전성
  - FIPS에서 승인된 알고리즘과 키 크기 사용
  - 권한 과정 처리의 중요성

- Public authorization key : 비대칭키 알고리즘의 키쌍 중에 공개키로서 개체의 권한을 검증하기 위해 사용되는 키
  ① 고려사항 : 공개 인가 키의 유효기간 길이는 안전성의 관점에서 보면, 관련된 개인 인가 키 동의키에 비해 중요하지 않다.
  ② 유효기간 : 공개 인가 키의 유효기간은 개인 인가 키와 같으며, 키의 유효기간은 최대 2년이다.

4. 키 생명주기 및 키 관리 주기

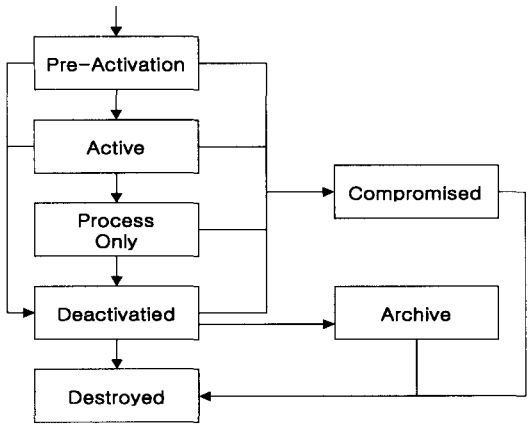
본 장에서는 키 생명주기에 따라 각 상의 키 상태를 살펴보고, 키 생명주기에 바탕을 둔 키 관리 주기를 알아본다. 암호학적 키 생명주기(key lifecycle)는 키 생성부터 키 파괴에 이르기까지 여러 가지의 상태(states)로 구성되어 있다.

다음 [그림 2]는 키 생명주기를 나타내고 있다.

- Pre-activation state : 키가 생성되지만, 아직 활성(active)되지는 않은 상태

- Active state : 이 상태의 키는 정보를 보호하기 위해 암호학적으로 적용할 경우(암호화) 또는 보호된 정보를 처리 할 경우(복호화, 전자 서명의 검증)에 사용될 수 있는 활성 상태

- Process only state : 보호된 정보를 처리할 수는 있으나, 정보를 보호하기 위해 암호학적으로는 적용할 수 없는 상태



〔그림 2〕 키 생명주기

- Deactivated state : 이 상태의 키는 암호학적인 처리나 적용이 이루어지는 것이 아니라, 키의 백업이 되는 상태

- Archive state : 보호된 정보를 저장하기 위한 상태

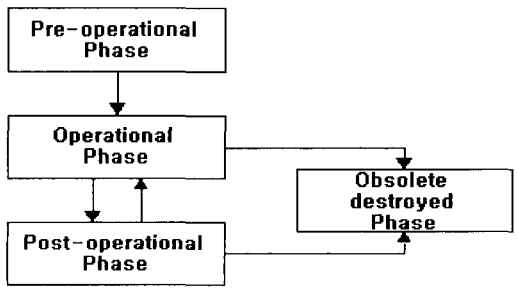
- Compromised state : 키의 무결성이나 기밀성이 의심스러운 경우의 상태이다. 모든 상태와 연관되며, 키가 의심스러운 경우에는 폐기·파괴가 이루어지는 전 단계의 상태

- Destroyed state : 키의 파괴 상태

4.1 Pre-operational Phase

키는 아직 생성되지 않았거나, 비 활성 상태를 말한다.

다음 〔그림 3〕은 키 관리 주기를 나타내며 그 각각의 상태는 다음과 같다.



〔그림 3〕 키 관리 주기

■ 사용자 등록

사용자는 자신의 ID의 고유 비밀 값(secret value : password, PIN, HMAC key)을 부여받으며, 키 등록 시에 사용자 인증을 위하여 사용된다. 사용자 등록을 하는 동안 개체는 보안 영역의 인가된 일원이 된다. 초기 키 생성 재료의 취득 혹은 생성, 교환을 포함한다.

■ 시스템 초기화

시스템 초기화는 보안 작동을 위해 알고리즘 선택, 허가받은 사용자의 인증, 도메인 파라미터 정책(domain parameter policies)들을 정의하고, 시스템 전반적인 사항을 준비한다. 시스템 초기화는 보안 운영을 위해 시스템을 설정·설치하는 것을 포함한다.

■ 사용자 초기화

사용자 초기화는 초기화 소프트웨어나 하드웨어를 통해서 이루어진다. 사용자 등록에서 얻게되는 초기 키 생성 재료의 설치나 사용을 포함한다.

■ 키 자료 설치

키 생성 재료 설치의 보안은 시스템 보안에 있어 중요하다. 이 단계 동안의 키 생성 재료는 개체의 소프트웨어, 하드웨어, 어플리케이션, 암호모듈 혹은 다양한 기술들을 사용하기 위한 장치를 위해 설치된다.

■ 키 설정

키 설정은 사용자가 사용할 키 생성과정과 분배과정이 이루어진다. SP 800-56에 명시되어 있다.

① 공개/개인키 쌍의 생성과 분배 : 공개/개인 키 쌍은 전자 서명과 키 설정 알고리즘들에 사용된다. FIPS 140-2에서 검증된 암호 모듈을 사용하여 생성된 키 쌍들이 요구되며, 키 쌍 생성시 모든 접근이 통제된다.

비밀 서명, 인증과 인가 키들은 다른 개체들에게 분배되어져서는 안된다. 서명, 인증과 인가 키들 보다도 공개키와 비밀키의 분배는 고정이든 임시적이든 키의 형태에 독립적이어야 한다.

② 대칭키 생성과 분배 : 대칭 키들은 생성되어진 후, 공개 키 전송 메커니즘을 사용하거나, 사전 분배를 사용하여 분배된다. 데이터나 다른 키들의 암호화/복호화, MAC의 계산에 사용된 대칭 키들은 입증된 방법으로 결정되어야만 한다. 키들은 랜덤 하게 생성되어지고, 키 동의 메커니

즘에 의해 결정되어야만 한다.

③ 그 외의 키 자료 생성과 분배 : 키들은 다른 키 생성 재료와 연관되어 생성 되거나 사용되어진다.

- Domain Parameters : 도메인 파라미터들은 공개/비밀키 쌍을 생성하거나 전자 서명들을 계산하기 위해 특정 공개키 알고리즘에 의해서 사용된다. 일반적으로 도메인 파라미터들은 오랜 시간동안 사용자들의 통신에 사용된다. 도메인 파라미터들은 신뢰되는 개체나 개체 자신들에 의해 우선적으로 검증되어야만 한다. 도메인 파라미터의 검증은 FIPS 186-3, SP 800-56에 정의되어있다.

- Initialization Vectors : 초기 벡터들은 암호화·복호화 및 인증을 위해 몇 가지 모드 연산에 의해 사용되어진다. IV의 기준은 SP 800-38A에 정의되어 있다.

- Shared Secrets : 분산된 비밀들은 키 동의 과정 동안(SP 800-56)에 계산되어지고, 그 후에 키 생성 재료를 유도하는데 사용된다. 분산된 비밀들은 적합한 키 동의 스킴에 의해 생성되어지지만 분배되어서는 안된다.

- Secret and Public Seeds : Seeds는 의사 난수 생성기를 초기화하는데 사용된다. seed의 선택 기준은 입증된 의사 난수 생성기의 설계 명세서에 의해 제공되어야 한다.

- Intermediate Result : 중간 결과 값은 암호 알고리즘을 사용한 계산 도중에 일어난다. 이러한 결과는 분배되어져서는 안 된다.

4.2 Operational Phase

키는 active 또는 process only 상태이며, 키의 유효기간 동안 사용된 키 자료들은 계속해서 저장되어진다. 키 생성 재료의 백업은 키 복구를 위하여 제공된다. 그러나, 모든 키들을 백업 해야하는 것은 아니다.(부록 〔표 3, 4〕 참고)

■ 일반적인 저장

① 안전한 암호학적 디바이스(Device)나 모듈(Module)에 저장

② 즉시 접근 가능한 저장 매체에 저장
(ex: 하드디스크, 스마트 카드)

③ 백업(Backup)저장 : 키 자료의 백업은 독립적으로 이루어져야 하며, 키 복구를 위해 안전한 저장 매체에 저장해야 한다.

■ 키 대체(Key Replacement) : 키의 대체는 키의 무결성이나, 기밀성이 의심스러운 경우, 그리고 키의 유효기간이 만기에 가까워 졌을 때 이루어진다.

4.3 Post-Operational Phase

Post-operational 상태동안에 키 자료는 더 이상 암호학적으로 사용가능하지는 않지만, 단순 키 접근은 가능하다.

■ Archive Storage

모든 키 생성 재료는 기록 보관되어져야할 필요는 없다. 저장된 키 생성 재료는 새롭게 저장된 암호화 키 하에서 재 암호화되어질 필요가 있다. 저장된 데이터는 활동중인 데이터로부터 구분되어 저장되어져야 하며, 저장된 데이터의 다중 복사물은 각 다른 것들로부터 구분되어 저장되고 가용할 수 있어야만 한다.(부록 〔표 5, 6〕 참고)

4.4 Obsolete/Destroyed Phase

이 상태에서는 키 자료가 더 이상 사용 가능하지 않다. 저장된 모든 키의 기록을 삭제된다.

5. NIST 권장 키 사이즈 및 알고리즘

AES, TDES와 같은 블록 암호 알고리즘의 경우에는 블록 사이즈도 안전성과 매우 밀접한 관계를 가지고 있지만, 일반적인 암호 알고리즘들은 키 사이즈에 비례하여 서로 다른 안정성을 제공하게 된다. 이에 본 장에서는 이산대수 문제의 공격방법, 타원 곡선 이산대수 문제의 공격방법 그리고 미래의 양자 암호 시스템을 고려하여 서로 다른 알고리즘의 NIST 권장 키 사이즈들을 살펴보며, 2035년 이 후 까지 NIST에서 권장하는 알고리즘과 최소 키 사이즈에 대해 년도 별로 알아본다. 위의 〔표 8〕은 알고리즘별 각 안전성을 고려하여 권장 키 사이즈를 나타내고 있으며, 〔표 9〕는 2003년부터 년도별로 권장하는 알고리즘 및 최소 키 사이즈를 정리한 것이다.

〔표 8〕 NIST 권장 키 사이즈

Bit of security	Symmetric key algs	Hash function (collision)	Hash function (no collision)	DSA, D-H, MQV	RSA	Elliptic Curves
80	2TDES	SHA-1		L=1024 N=160	k=1024	f=160
112	3TDES			L=2048 N=224	k=2048	f=224
128	AES-128	SHA-256		L=3072 N=256	k=3072	f=256
160			SHA-1			
192	AES-192	SHA-384		L=7680 N=384	k=7680	f=384
256	AES-256	SHA-512	SHA-256	L=15360 N=512	k=15360	f=512
384			SHA-384			
512			SHA-512			

〔표 9〕 년도별 NIST 권장 알고리즘 및 키 사이즈

Years	Symmetric key algs (Encryption &MAC)	Hash function (collision)	Hash function (no collision)	DSA, D-H, MQV	RSA	Elliptic Curves
2003-2015	2TDES 3TDES AES-128 AES-192 AES-256	SHA-1 SHA-256 SHA-384 SHA-512	SHA-1 SHA-256 SHA-384 SHA-512	L=1024 N=160	k=1024	f=160
2016-2035	3TDES AES-128 AES-192 AES-256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-256 SHA-384 SHA-512	L=2048 N=224	k=2048	f=224
After 2035	AES-128 AES-192 AES-256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-256 SHA-384 SHA-512	L=3072 N=256	k=3072	f=256

Ⅳ. 결 론

본 고에서는 NIST에서 2003년도에 발표된 SP 800-57 키 관리 가이드라인을 분석함으로써, 전반적인 키 관리 개념 및 키 관리를 위한 다양한 암호학 적 키의 정의를 알아보고, 각각의 키에 대한 고려사항과 키의 유효기간에 대해 분석하였다. 또한, NIST에서 권장하는 키 사이즈 및 년도별 권장 알고리즘, 최소 키 사이즈에 대하여 살펴보았다.

본고의 연구 결과는 키 관리 시스템 개발자에게 다양한 암호 알고리즘별 키의 고려사항 및 유효기간, 권장 키 사이즈 정보를 제공함으로써 키 관리 시스템 설계 시 유용한 지침서로 활용될 것이다. 그러나, 본 SP 800-57에서 안전성을 고려하여 키의 사이즈를 권장하였으나, 정확히 어떠한 공격방법들로부터 안전한 키 사이즈 및 알고리즘인지에 관한 사항은 미흡하며, 많은 부분이 제외되어 있다.

향후, 다른 키 관리 요소별 표준들과 상호 보안을 통하여 암호 알고리즘별 연산량 및 검증된 안전성 분석 방법을 고려한 키 관리 및 키 사이즈에 관한 연구가 필요하다.

참 고 문 헌

[1] ANSI X9.31, Digital Signatures Using reversible Public Key Cryptography for the Financial Services Industry (rDSA), 1998.

[2] ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using discrete Logarithm Cryptography, 2001.

[3] ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation, July, 1998.

[4] ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998.

[5] FIPS 46-3, Data Encryption Standard (DES), October 25, 1999.

[6] FIPS 140-2 Security Requirements for Cryptographic Modules, May 25, 2001

[7] FIPS180-2 Secure Hash Standard (SHS), August 2002.

[8] FIPS186-2 Digital Signature Standard (DSS), June 2000.

[9] FIPS197 Advanced Encryption Standard (AES), November 2001.

[10] HAC, Handbook of Applied Cryptography, Menezes, van Oorschot and Vanstone, CRC Press, 1996.

[11] SP 800-38 Special Publication 800-38, Recommendation for Block Cipher Modes of Operation, December, 2001.

[12] EKE S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-based protocols secure against dictionary attacks," in IEEE Symposium on Research in Security and Privacy, pp. 72-84, May, 1992.

[13] IEEE P1363, "Standard Specifications For Public Key Cryptography", IEEE, 2001.

[14] ANSI X9.44 (Draft), Public Key Cryptography for the Financial Services Industry: Agreement the Key Transport Using Factoring- Based Cryptography, December, 2003.

[15] NIST SP 800-56 (Draft), Recommendation On Key Establishment Schemes, 2003.

[16] P. Kocher, "Timing attacks on implementation of Diffie-Hellman, RSA, DSS and other systems", In Advances in Cryptography-CRYPT '96, LNCS 1109, pp. 104-113, 1996.

[17] E. Biham, A. Shamir, "Differential cryptoanalysis of DES-like cryptosystems", Journal of Cryptology, pp. 3-72, 1991.

[18] M. Matsui, "Linear cryptanalysis method for DES cipher", In Advances in Cryptography-EUROCRYPT'93, LNCS 765, pp. 386-397, 1994.

[19] D. Bleichenbacher, M. Joye, and J.J Quisquater, "A new and optimal chosen-message attack on RSA-Type cryptosystems", Information and Communications Security, LNCS 1334, pp. 302-313, 1997.

[20] NIST, "Escrowed Encryption Standard", Federal Information Processing Standards Publication 185, 1994.

[21] FIPS 198, The Keyed-Hash Message Authentication code(HMAC), March 2002

부 록

〔표 1〕 암호학적 키 종류별 보안 가이드라인

Key Type	Security Service	Security Protection	Association Protection	Validity Assurance	Period of Protection
Private signature key	Authentication; Integrity; Nonrepudiation	Integrity; Confidentiality	Usage or application; Domain parameters; Public signature verification key		The cryptoperiod of the key and until the private key is destroyed
Public signature verification key	Authentication; Integrity; Nonrepudiation	Archive; Integrity;	Usage or application; Key pair owner Domain parameters; Private signature key; Signed data	For association with signing private key	As long as signed data may need to be verified
Symmetric authentication key	Authentication; Integrity	Archive; Integrity; Confidentiality	Usage or application; Other authorized entities; Authenticated data		As long as the authenticated data may need to be authenticated and until the key is destroyed
Private authentication key	Authentication; Integrity	Integrity; Confidentiality	Usage or application; Public authentication key; Domain parameters		The cryptoperiod of the key and until the key is destroyed
Public authentication key	Authentication; Integrity	Archive; Integrity	Usage or application; Key pair owner; Authenticated data; Private authentication key; Domain parameters	For association with private key	As long as the authenticated data may need to be authenticat
Symmetric data encryption key	Confidentiality	Archive; Integrity; Confidentiality	Usage or application; Other authorized entities; Encrypted data		The cryptoperiod of the key and the lifetime of the data and until the key is destroyed

〔표 1〕 암호학적 키 종류별 보안 가이드라인(계속)

Key Type	Security Service	Security Protection	Association Protection	Validity Assurance	Period of Protection
Symmetric key wrapping key	Support	Archive; Integrity; Confidentiality	Usage or application; Other authorized entities; Encrypted keys		The cryptoperiod of the key and until the key is destroyed
Symmetric RNG key	Support	Integrity; Confidentiality	Usage or application		Until no longer needed to generate or reconstruct random numbers and until destroyed
Symmetric master key	Support	Archive; Integrity; Confidentiality	Usage or application; Other authorized entities; Derived keys		The cryptoperiod of the key, the lifetime of any keys derived using this key, and until the key is destroyed
Private key transport key	Support	Archive; Integrity; Confidentiality	Usage or application; Encrypted keys; Public key transport key; Domain parameters		As long as the transported key needs to be decrypted and until destroyed
Public key transport key	Support	Integrity	Usage or application; Key pair owner; Private key transport key; Domain parameters	Yes	The cryptoperiod of the key
Symmetric key agreement key	Support	Archive; Integrity; Confidentiality	Usage or application; Other authorized entities		The cryptoperiod of the key, until no longer needed to determine a key, and until destroyed

〔표 1〕 암호학적 키 종류별 보안 가이드라인(계속)

Key Type	Security Service	Security Protection	Association Protection	Validity Assurance	Period of Protection
Private static key agreement key	Support	Archive: Integrity: Confidentiality	Usage or application: Domain parameters: Public static key agreement key		The cryptoperiod of the key, until no longer needed to determine a key, and until destroyed
Public static key agreement key	Support	Archive: Integrity	Usage or application: Key pair owner: Domain parameters: Private static key agreement key	Yes	Until no longer needed to determine a key
Public ephemeral key agreement key	Support	Integrity	Key pair owner: Private ephemeral key agreement key: Usage or application: Domain parameters	Yes	Until the key agreement process is complete
Symmetric authorization keys	Authorization	Integrity: Confidentiality	Usage or application: Other authorized entities		The cryptoperiod of the key and until the key is destroyed
Private authorization key	Authorization	Integrity: Confidentiality	Usage or application: Public authorization key: Domain parameters		The cryptoperiod of the key and until the key is destroyed
Public authorization key	Authorization	Integrity	Usage or application: Key pair owner: Private authorization: Domain parameters	Yes	The cryptoperiod of the key or As long as the authorization needs to be verified

〔표 1〕 암호학적 키 종류별 보안 가이드라인(계속)

Key Type	Security Service	Security Protection	Association Protection	Validity Assurance	Period of Protection
Private ephemeral key agreement key	Support	Integrity; Confidentiality	Usage or application; Public ephemeral key agreement key; Domain parameters;		Until the key agreement process is complete; the ephemeral key is destroyed after the key agreement process is complete

〔표 2〕 암호학적 키 관련 종류별 보안 가이드라인

Crypto. Information Type	Security Service	Security Protection	Association Protection	Validity Assurance	Period of Protection
Domain parameters	Depends on key assoc. with the params.	Archive; Integrity	Usage or application; Private and public keys	Yes	Until no longer needed to generate keys, or verify signatures
Initialization vectors	Depends on algorithm	Archive; Integrity	Protected data		Until no longer needed to process the protected data
Shared secrets	Support	integrity; Confidentiality	Usage or application; Public authorization key; Domain parameters		Until no longer needed to generate keying material, and the shared secret is destroyed
Secret seeds	Support	Confidentiality; Integrity	Usage or application		Until no longer needed to generate keying material and the shared secret is destroyed
Public seeds	Support	Archive; Integrity	User or application; Generated data		Until no longer needed to process generated data
Other public information	Support	Archive; Integrity;	User or application; Other authorized entities; Data processed using the nonce		Until no longer needed to process data using the public information

〔표 2〕 암호학적 키 관련 종류별 보안 가이드라인(계속)

Crypto. Information Type	Security Service	Security Protection	Association Protection	Validity Assurance	Period of Protection
Intermediate results	Support	Confidentiality: Integrity	Usage or application		Until no longer needed and the intermediate results are destroyed
Key control information (e.g., IDs, purpose)	Support	Archive: Integrity	Key		Until the associated key is destroyed
Random number	Support	integrity: Confidentiality			Until no longer needed, and the random number is destroyed
Password	Authentication	Archive Integrity: Confidentiality	Usage or application: Owning entity		Until replaced or no longer needed to authenticate the entity
Audit information	Support	Archive: Integrity: Access authorization	Audited events: Key control information		Until no longer needed

〔표 3〕 암호학적 키 종류별 백업 가이드라인

Type of Key	Backup?
Public authentication key	OK: its presence in a public-key certificate that is available elsewhere may be sufficient.
Symmetric data encryption key	OK
Symmetric key wrapping key	OK
Random number generation key	Not necessary and may not be desirable, depending on the application.
Symmetric master key	OK
Private key transport key	OK
Public key transport key	OK: presence in a public-key certificate available elsewhere may be sufficient.
Symmetric key agreement key	OK
Private static key agreement key	No, unless needed for reconstruction during key recovery. However, when ephemeral information (e.g., a privateephemeral key agreement key) is used in a key agreement scheme, knowledge of the private static key agreement key and any public keys will not be sufficient.
Public static key agreement key	OK: its presence in a public-key certificate that is available elsewhere may be sufficient.
Private ephemeral key agreement key	No
Public ephemeral key agreement key	No, unless needed for reconstruction during key recovery
Symmetric authorization key	OK
Private authorization key	OK
Public authorization key	OK: its presence in a public-key certificate that is available elsewhere may be sufficient.
Private signature key	No (in general): non-repudiation would be in question. However, it may be warranted in some cases - a CA' s signing private key, for example. When required, any backed up keys must be stored under the owner' s control.
Public signature verification key	OK: its presence in a public-key certificate that is available elsewhere may be sufficient.
Symmetric authentication key	OK
Private authentication key	OK, if required by an application.

〔표 4〕 암호학적 키 관련 종류별 백업 가이드라인

Type of Keying Material	Backup?
Domain parameters	OK
Initialization vector	OK, if necessary
Shared secret	No
Secret seed	No
Public seed	OK, if required for the validation of domain parameters
Other public information	OK
Intermediate results	No
Key control information(e.g. IDs, purpose, etc)	OK
Random number	OK
Passwords	OK
Audit information	OK

〔표 5〕 암호학적 키 종류별 저장 가이드라인

Type of Key	Archive?	Retention period(minimum)
Private signature key	No	
Public signature verification key	OK	Until no longer required to verify data signed with the assoc. private key
Symmetric authentication key	OK	Until no longer needs to authenticate data
Private authentication key	No	
Public authentication key	OK	Until no longer required to verify the authenticity of data that was authenticated with the assoc. private key
Symmetric data encryption key	OK	Until no longer needed to decrypt data encrypted by this key
Symmetric key wrapping key	OK	Until no longer needed to decrypt keys encrypted by this key
Random number generation key	No	
Symmetric master key	OK, if needed to derive other keys for archived data	Until no longer needed to derive other keys
Private key transport key	OK	Until no longer needed to decrypt keys encrypted by this key
Public key transport key	No	
Symmetric key agreement key	OK	
Private static key agreement key	OK if needed to reconstruct keying material	Until no longer needed to reconstruct keying material

〔표 5〕 암호학적 키 종류별 저장 가이드라인(계속)

Type of Key	Archive?	Retention period(minimum)
Public static key agreement key	OK if needed to reconstruct keying material	Until no longer needed to reconstruct keying material
Private ephemeral key agreement key	No	
Public ephemeral key agreement key	No	
Symmetric authorization key	No	
Private authorization key	No	
Public authorization key	No	

〔표 6〕 암호학적 키 관련 종류별 저장 가이드라인

Type of Key	Archive?	Retention period(minimum)
Domain parameters	OK	Until all keying material, signatures and signed data using the domain parameters are removed from the archive
Initialization vector	OK: normally stored with the protected information	Until no longer needed to process the protected data
Shared secret	No, unless needed to validate or reconstruct derived keying material for archived information	Until no longer needed to validate or reconstruct derived keying material for archived information.
Secret seed	No	
Public seed	OK	Until no longer needed to process generated data
Other public information	OK	Until no longer needed to process data using the public information
Intermediate results	No	
Key control information (e.g. IDs, purpose, etc)	OK	Until the associated key is removed from the archive
Random number	No	
Passwords	No, unless used to detect the reuse of old passwords	Until no longer needed to detect password reuse
Audit information	OK	

〈著 者 紹 介〉

이 진 우(Jinwoo Lee)
학생회원

2003년 2월 : 성균관대학교 정보통신공학부 졸업(공학사)
2003년 3월~현재 : 성균관대학교 컴퓨터공학과 석사과정

곽 진(Jin Kwak)
학생회원

2008년 8월 : 성균관대학교 바이오메카트로닉스 공학과 졸업(공학사)
2003년 2월 : 성균관대학교 대학원 전기전자 및 컴퓨터 공학부 졸업(공학석사)
2003년 3월~현재 : 성균관대학교 정보통신공학부 박사과정

양 형 규(Hyungkyu Yang)
정회원

1983년 2월 : 성균관대학교 전자공학과 졸업(공학사)
1985년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학석사)
1984년 12월~1991년 2월 : 삼성전자 선임 연구원
1995년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학박사)
1995년 3월~현재 : 강남대학교 컴퓨터미디어공학부 부교수

원 동 호(Dongho Won)
종신회원

1976년~1988년 : 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~2003년 : 한국전자통신연구소 전임 연구원, 일본 동경공대 객원연구원, 성균관대학교 교학처장, 전기·전자 및 컴퓨터공학부장, 정보통신대학원장, 국무총리실 정보화추진위원회 자문위원, 한국정보보호학회 이사, 부회장, 수석부회장, 회장
현재 : 성균관대학교 정보통신공학부 교수, 성균관대학교 연구지원처장, 한국정보보호학회 명예회장, 정통부지정 정보보호인증기술연구센터 센터장