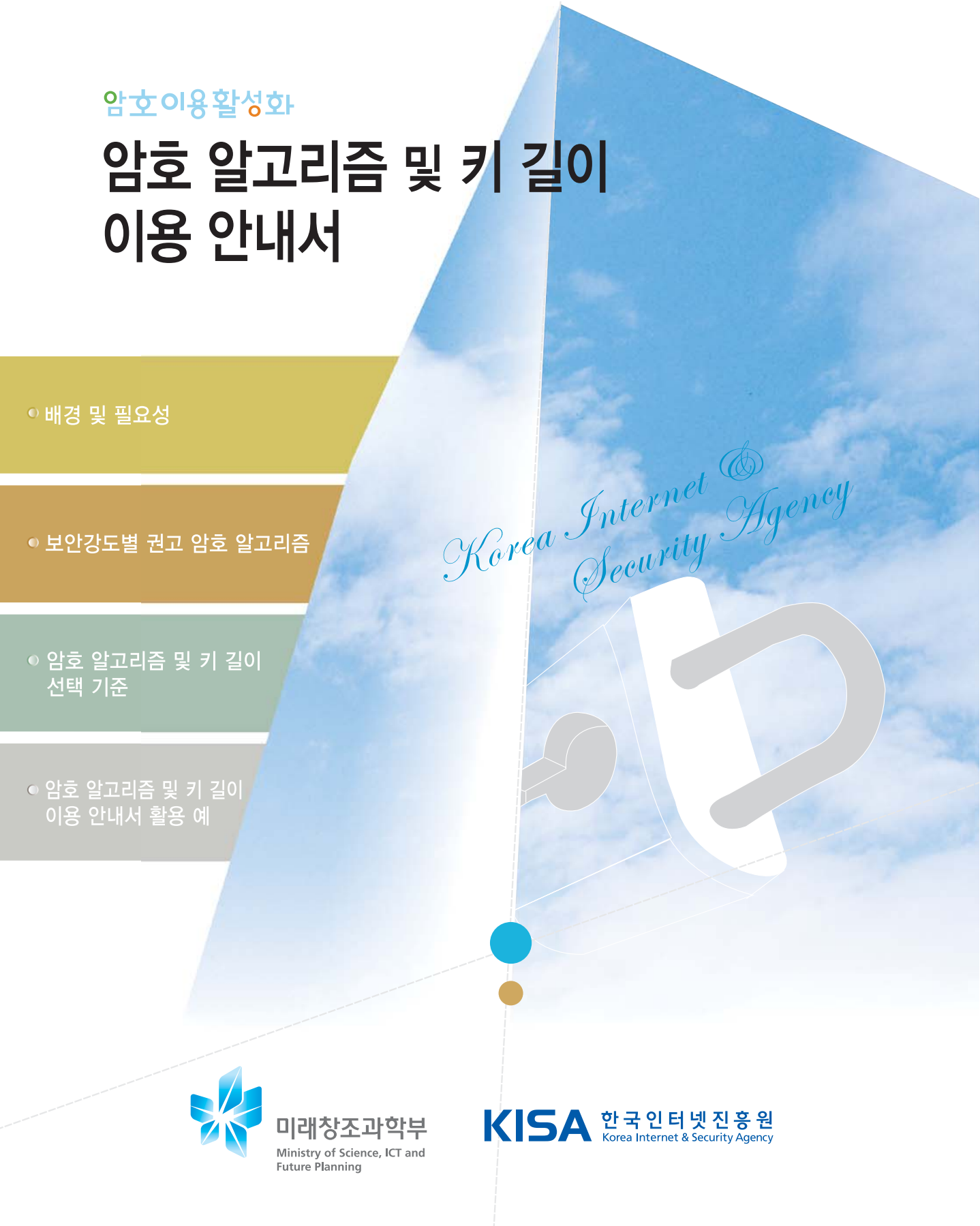
www.kisa.or.kr

암호이용활성화

암호 알고리즘 및 키 길이 이용 안내서

- 배경 및 필요성
- 보안강도별 권고 암호 알고리즘
- 암호 알고리즘 및 키 길이 선택 기준
- 암호 알고리즘 및 키 길이 이용 안내서 활용 예



미래창조과학부
Ministry of Science, ICT and Future Planning

KISA 한국인터넷진흥원
Korea Internet & Security Agency

제 · 개정 이력

순번	제 · 개정일	제 · 개정 내역
1	2009. 04	– 암호 알고리즘 및 키 길이 이용 안내서 제정
2	2009. 10	– 기관명 변경
3	2013. 01	– 권고 대상 암호 알고리즘 추가 – RSA 공개키 암호 버전 설명 추가 – 해쉬함수 종류별 용도 설명 – 안전성 유지기간 관련 부가 설명 제시 – 개인정보 관련 암호 알고리즘 적용 예 추가

01

1. 배경 및 필요성

정보보호제품 및 시스템에 암호 알고리즘을 탑재·적용 하는 경우, 알고리즘의 종류나 키 길이 등은 해당 시스템의 안전성 수준을 만족할 수 있도록 선택해야한다. 이를 위해 미국, 일본, 유럽 등에서는 암호 알고리즘 및 키 길이에 대한 가이드라인을 제시하고 있다. 그러나 국내의 경우, 국산 암호 알고리즘의 활용비율이 높지만, 국산 암호 알고리즘을 포함한 『암호 알고리즘 및 키 길이 선택』 기준이 없어 이에 대한 개발이 필요하다.

이에, 본 안내서에서는 SEED, HIGHT, ARIA, KCDSA 등의 국산 암호 알고리즘을 포함해 보안강도에 따라 선택 가능한 암호 알고리즘의 종류와 키 길이, 유효기간을 소개한다.

※ 『안전성 수준』 이란 시스템이 어느 정도의 보안강도를 만족해야하는지를 의미함
※ 『보안강도』 란 암호 알고리즘이나 시스템의 암호키 또는 해쉬함수의 취약성을 찾아내는데 소요되는 작업량을 수치화한 것으로 80, 112, 128, 192, 256비트로 정의(80비트의 보안강도란 2^{80}번의 계산을 해야 암호키 또는 암호 알고리즘의 취약성을 알아낼 수 있음을 의미)

02

2. 보안강도별 권고 암호 알고리즘

미국, 일본, 유럽 및 국내에서는 <표 1>과 같은 암호 알고리즘의 이용을 권고한다.

〈표 1〉 국내외 권고 암호 알고리즘

분류		NIST(미국) (2012)	CRYPTREC(일본) (2011)	ECRYPT(유럽) (2011)	국내[1] (2012)
대칭키 암호 알고리즘		AES 2TDEA[2] 3TDEA[2]	AES 3TDEA Camellia Cipherunicorn-A Cipherunicorn-E Hierocrypt-3 Hierocrypt-L1 MISTY1 SC2000	AES 2TDEA 3TDEA KASUMI Blowfish1)[1]	SEED ARIA HIGHT
해쉬함수		SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256 SHA-384/512 RIPEMD-160	SHA-1 SHA-224/256 SHA-384/512 RIPEMD-128/160 Whirlpool	HAS-160 SHA-1 SHA-224/256 SHA-384/512
공개키 암호 알고리즘	키 공유용	DH ECDH MQV ECMQV	DH ECDH PSEC-KEM	ACE-KEM PSEC-KEM RSA-KEM	DH ECDH
	암 · 복호화용	RSA	RSAES-OAEP RSAES-PKCS1(v1.5)	RSAES-OAEP	RSAES-OAEP[3]
	전자 서명용	RSA DSA ECDSA	RSASSA-PSS RSASSA-PKCS1(v1.5) DSA ECDSA	RSASSA-PSS RSASSA-PKCS1(v1.5) DSA ECDSA	RSASSA-PKCS1(v1.5)[3] RSASSA-PSS[3] KCDSA ECDSA EC-KCDSA

※ 본 표에서는 국내외 암호 연구기관에서 발간하는 보고서에서 다루어지는 대표적인 암호 알고리즘들을 언급함

[1] 국내 : 국내 암호 알고리즘은 '검증대상보호함수(IT보안인증사무국)'와 국내 표준들을 기반으로 구성하며, 그 외의 암호 알고리즘을 사용할 경우, 국외 권고(안)을 참고하기를 권장함
[2] 2TDEA(3TDEA) : 두 개의 키가 다른(세 개의 키가 다른) TDEA(Triple Data Encryption Algorithm)
[3] PKCS#1 v2.0(RSA Cryptography Standard) 버전 이상에 포함된 알고리즘을 의미함

암호 알고리즘 및 키 길이 이용 안내서는 암호 알고리즘별 보안강도(80, 112, 128, 192, 256비트)를 기반으로 한다. 우선, 국내외에서 권고하는 암호 알고리즘을 보안강도에 따라 분류한다.

1) 대칭키 암호 알고리즘

암·복호화용 대칭키 암호 알고리즘의 보안강도에 따른 알고리즘 분류는 <표 2>와 같다.

〈표 2〉 보안강도에 따른 대칭키 암호 알고리즘 분류

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
80 비트 이상	AES-128/192/256 2TDEA 3TDEA	AES-128/192/256 3TDEA Camellia-128/192/256 MISTY1	AES-128/192/256 2TDEA 3TDEA KASUMI Blowfish1)[1]	SEED HIGHT ARIA-128/192/256
112 비트 이상	AES-128/192/256 3TDEA	AES-128/192/256 3TDEA Camellia-128/192/256 MISTY1	AES-128/192/256 Blowfish KASUMI 3TDEA	SEED HIGHT ARIA-128/192/256
128 비트 이상	AES-128/192/256	AES-128/192/256 Camellia-128/192/256 MISTY1	AES-128/192/256 KASUMI Blowfish	SEED HIGHT ARIA-128/192/256
192 비트 이상	AES-192/256	AES-192/256 Camellia-192/256	AES-192/256 Blowfish	ARIA-192/256
256 비트 이상	AES-256	AES-256 Camellia-256	AES-256 Blowfish	ARIA-256

※ 본 표에서는 국외 암호연구기관에서 권고하는 암호 알고리즘 중에서 국가적으로 다수 사용되지 않는 암호 알고리즘은 제외하였음

1) Blowfish : 32~448비트의 가변적인 키 길이를 제공하므로 각 보안강도 이상의 비트를 가질 경우 안전함

2) 해쉬함수

해쉬함수는 사용 목적에 따라 메시지인증/키유도/난수생성용과 단순해쉬(메시지 압축)/전자 서명용으로 나눠지며, 사용목적과 보안강도에 따라 <표 3>, <표 4>와 같이 분류된다.

☑ 메시지인증/키유도/난수생성용 해쉬함수

- 메시지 인증용 : 메시지의 위 · 변조를 확인하기 위해 해쉬함수 이용
- 키유도/난수생성용 : 안전한 키와 랜덤한 난수를 생성하기 위해 해쉬함수 이용

〈표 3〉 보안강도에 따른 메시지인증/키유도/난수생성용 해쉬함수 분류

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
80 비트 이상	SHA-1 SHA-224/256/384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-1 SHA-224/256 SHA-384/512
112 비트 이상	SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-1 SHA-224/256 SHA-384/512
128 비트 이상	SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-1 SHA-224/256 SHA-384/512
192 비트 이상	SHA-256/384/512	SHA-256/384/512	SHA-224/256/384/512 Whirlpool	SHA-256/384/512
256 비트 이상	SHA-256/384/512	SHA-256/384/512	SHA-256/384/512 Whirlpool	SHA-256/384/512

☑ 단순해쉬/전자서명용 해쉬함수

• 단순해쉬/전자서명용 : 패스워드의 안전한 저장이나 효율적인 전자서명 생성을 위해 메시지 압축 시 해쉬함수 이용

〈표 4〉 보안강도에 따른 단순해쉬/전자서명용 해쉬함수 분류

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
80 비트 이상	SHA-1 SHA-224/256/384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160[2] SHA-1[3] SHA-224/256/384/512
112 비트 이상	SHA-224/256/384/512	SHA-256/384/512	SHA-224/256/384/512 Whirlpool	SHA-224/256/384/512
128 비트 이상	SHA-256/384/512	SHA-256/384/512	SHA-256/384/512 Whirlpool	SHA-256/384/512
192 비트 이상	SHA-384/512	SHA-384/512	SHA-384/512 Whirlpool	SHA-384/512
256 비트 이상	SHA-512	SHA-512	SHA-512	SHA-512

3) 공개키 암호 알고리즘

공개키 암호 알고리즘은 메시지 암·복호화, 전자서명, 키 공유 등을 위해 사용되며, 공개키 암호 알고리즘의 보안강도에 따른 분류는 <표 5>와 같다.

2) HAS-160 : 충돌저항성(안전성)이 112비트 보안강도를 제공하지 못하므로, 2010년도부터는 단순해쉬/전자서명용으로 사용하는 것을 권장하지 않음

3) SHA-1 : 충돌저항성(안전성)이 80비트 보안강도 이하를 제공하여(Crypto'05), 새로운 어플리케이션에 적용하는 것을 권장하지 않지만 현재 광범위하게 사용되므로 해쉬함수 보안강도 표에 추가하였음

〈표 5〉 보안강도에 따른 공개키 암호 알고리즘 분류

보안강도	인수분해 문제(비트)	이산대수 문제(비트)		타원곡선
		공개키	개인키	
80 비트	1024	1024	160	160
112 비트	2048	2048	224	224
128 비트	3072	3072	256	256
192 비트	7680	7680	384	384
256 비트	15360	15360	512	512

기반	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
인수분해 문제	RSA(암,전)	RSAES-OAEP(암) RSAES-PKCS1(v1.5)(암) RSASSA-PKCS1(v1.5)(전) RSASSA-PSS(전)	RSA-KEM(키) RSAES-OAEP(암) RSAES-PKCS1(v1.5)(암) RSASSA-PSS(전)	RSAES-OAEP(암) RSASSA-PSS(전) RSASSA-PKCS1 (v1.5)(전)
이산대수 문제	DH(키) DSA(전) MQV(키)	DH(키) DSA(전) PSEC-KEM(키)	ACE-KEM (키) DSA(전) PSEC-KEM(키)	DH(키) KCDSA(전)
타원곡선	ECDH(키) ECDSA(전) ECMQV(키)	ECDH(키) ECDSA(전)	ECDSA(전)	ECDH(키) ECDSA(전) EC-KCDSA(전)

(암) : 메시지 암/복호화용, (전) : 전자서명용, (키) : 키 공유 용

03

3. 암호 알고리즘 및 키 길이 선택 기준

암호 알고리즘 및 키 길이 선택 시, 암호 알고리즘의 안전성 유지기간과 보안강도별 암호 알고리즘 키 길이 비교표, 암호키의 사용 유효기간을 기반으로 암호 알고리즘 및 키 길이를 선택하도록 권장한다.

1) 보안강도별 암호 알고리즘 비교

대칭키 암호 알고리즘/공개키 암호 알고리즘/해쉬함수의 보안강도 비교표는 <표 6>와 같다.

〈표 6〉 보안강도별 암호 알고리즘 비교표

보안강도	대칭키 암호 알고리즘 (보안강도)	해쉬함수 (보안강도)	공개키 암호 알고리즘				암호 알고리즘 안전성 유지기간 (년도)
			인수분해 (비트)	이산대수		타원곡선 암호 (비트)	
				공개키 (비트)	개인키 (비트)		
80 비트	80	80	1024	1024	160	160	2010년까지
112 비트	112	112	2048	2048	224	224	2011년에서 2030년까지 (최대20년)

보안강도	대칭키 암호 알고리즘 (보안강도)	해쉬함수 (보안강도)	공개키 암호 알고리즘				암호 알고리즘 안전성 유지기간 (년도)
			인수분해 (비트)	이산대수		타원곡선 암호 (비트)	
				공개키 (비트)	개인키 (비트)		
128 비트	128	128	3072	3072	256	256	2030년 이후 (최대30년)
192 비트	192	192	7680	7680	384	384	
256 비트	256	256	15360	15360	512	512	

※ 만약 2009년에 80비트 보안강도의 암호 알고리즘을 적용하였을 경우, 2010년 이후에는 80비트 보안강도의 암호 알고리즘이 안전하지 않으므로 이를 계속 사용하는 것은 권장하지 않음
▶ 112비트 이상의 보안강도를 제공하는 암호 알고리즘으로 암호화 또는 재-해쉬를 적용하여 안전성을 강화하기를 권장함

2) 암호키 사용 유효기간

암호 알고리즘 키 사용 유효기간이란 암호키를 사용할 수 있는 기간을 말한다. 즉, 암호 알고리즘에 사용되는 키의 사용 유효기간은 송신자가 암호키를 사용하는 기간(예, 암호화 과정)과 수신자가 받은 메시지와 관련된 암호키를 사용하는(예, 복호화 과정)기간을 포함한다. <표 7>에서는 NIST[4]의 키 관리 권고안을 기반으로 암호키의 사용 유효기간을 제시한다.

〈표 7〉 암호키 사용 유효기간(NIST 권고안)

키 종류		사용 유효기간	
		송신자 사용기간	수신자 사용기간
대칭키 암호 알고리즘	비밀키	최대 2년	최대 5년[5]
공개키 암호 알고리즘	암호화 공개키	최대 2년	
	복호화 개인키	최대 2년	
	검증용 공개키	최소 3년	
	서명용 개인키	최대 3년	

4) NIST Special Publication 800-57, Recommendation for Key Management-Part 1: General(Revision 3)

5) 수신자의 경우 송신자가 전송한 암호화된 데이터를 수신 한 후 필요시에 복호화 할 수 있으므로 송신자보다 오랜 기간 동안 비밀키를 사용할 수 있음

04

4. 암호 알고리즘 및 키 길이 이용 안내서 활용 예

☑ 주민등록번호 및 계좌번호 등의 정보를 저장하는 경우

- 주민등록번호 및 계좌번호 등의 정보를 안전하게 암호화하기 위해 다음과 같은 방법으로 암호 알고리즘을 선택하여 적용할 수 있다.

1

〈표 6〉에서 현재 2013년 기준으로 안전하게 사용할 수 있는 보안강도(비트)확인

- 보안강도 : 112비트 이상

2

주민등록번호 및 계좌정보 암호화에 필요한 안전한 암호 알고리즘이란 데이터 암·복호화가 가능한 양방향 암호 알고리즘인 대칭키 암호알고리즘이므로 〈표 2〉에서 보안강도 112비트 이상을 제공하는 알고리즘을 확인

- AES, SEED, ARIA-128/192/256 등이 존재
- 국내 암호 알고리즘을 고려한다면 SEED, ARIA-128/192/256 선택 가능

3

〈표 7〉을 참조하여 키 사용 유효기간을 설정(NIST 권고)

- 송신자용 암/복호화 비밀키 : 최대 2년
- 수신자용 암/복호화 비밀키 : 최대 5년

- 주민등록번호 및 계좌정보 등 금융정보 암호화를 위해서는 보안강도 **112비트 이상**을 제공하는 대칭키 알고리즘들 중 국내 암호 알고리즘을 사용한다면, SEED, HIGHT, ARIA-128/192/256 암호 알고리즘 중 선택하여 적용
- 비밀키 유효기간은 송신자용 최대 **2년**, 수신자용 최대 **5년**으로 설정하기를 권장

비밀번호 및 바이오 정보를 저장하는 경우

- 비밀번호 및 바이오 정보를 안전하게 암호화하기 위해 다음과 같은 방법으로 암호 알고리즘을 선택하여 적용할 수 있다.

1

〈표 6〉에서 현재 2013년 기준으로 안전하게 사용할 수 있는 보안강도(비트) 확인

▶ 보안강도 : 112비트 이상

2

비밀번호 및 바이오 정보 암호화에 필요한 일방향 암호 알고리즘은 단순해쉬/전자서명용 해쉬함수이므로 〈표 4〉에서 보안강도 112비트 이상을 제공하는 알고리즘을 확인

▶ SHA-224/256/384/512 등이 존재하며, 이 중에서 선택 가능

- 비밀번호 및 바이오정보에 대해서는 보안강도 112비트 이상을 제공하는 해쉬함수 중 SHA-224/256/384/512 암호 알고리즘 중 선택

대칭키 암호 알고리즘을 적용하여 2025년까지 사용하고자 하는 경우

- 시스템 개발자가 메시지 기밀성을 제공하기 위해 대칭키 암호 알고리즘을 시스템에 적용하여 2025년까지 안전하게 사용하고자 할 경우, 개발자는 다음과 같은 방법으로 암호 알고리즘을 선택하여 적용할 수 있다.

1

〈표 6〉에서 현재 2013년 기준으로 대칭키 암호 알고리즘을 2025년까지 안전하게 사용하기 위한 보안강도(비트) 확인

▶ 보안강도 : 112비트 이상

2

〈표 2〉에서 보안강도 112비트 이상을 제공하는 대칭키 암호 알고리즘 확인

▶ AES, SEED, HIGHT, ARIA-128/192/256 등이 존재

▶ 국내 암호 알고리즘을 고려한다면 SEED, HIGHT, ARIA-128/192/256 선택 가능

3

〈표 7〉을 참조하여 키 사용 유효기간을 설정(NIST 권고)

▶ 송신자용 암/복호화 비밀키 : 최대 2년

▶ 수신자용 암/복호화 비밀키 : 최대 5년

- 보안강도 **112비트 이상**을 제공하는 알고리즘들 중 국내 암호 알고리즘 사용한다면, SEED, HIGHT, ARIA-128/192/256 암호 알고리즘 중 선택을 권장
- 비밀키 유효기간은 송신자용 **최대 2년**, 수신자용 **최대 5년**으로 설정하기를 권장

공개키 암호 알고리즘을 적용하여 2035년까지 사용하고자 하는 경우

- 시스템 개발자가 메시지 기밀성을 제공하기 위해 공개키 암호 알고리즘을 시스템에 적용하여 2035년까지 안전하게 사용하고자 할 경우, 개발자는 다음과 같은 방법으로 암호 알고리즘을 선택하여 적용할 수 있다.

1

〈표 6〉에서 현재 2013년 기준으로 공개키 암호 알고리즘을 2035년까지 안전하게 사용하기 위한 보안강도(비트) 및 공개키/개인키 길이 확인

- 보안강도 : 128비트 이상
- 인수분해 기반 알고리즘의 경우, 공개키/개인키 길이 : 3072비트 이상
- 이산대수 기반 알고리즘의 경우, 공개키/개인키 길이 : 3072/256비트 이상
- 타원곡선 기반 알고리즘의 경우, 공개키/개인키 길이 : 256비트 이상

2

〈표 5〉에서 공개키 암호 알고리즘 종류를 확인

※이산대수/타원곡선 기반의 권고 알고리즘 중, 암/복호화용은 없음

- RSAES-OAEP 선택

3

〈표 7〉을 참조하여 키 사용기간을 설정(NIST 권고)

- 송/수신자용 암/복호화 공개키/개인키 : 최대 2년

- 보안강도 **3072비트 이상**을 제공하는 **공개키/개인키**를 갖는 RSAES-OAEP 선택 사실, 2013년 기준으로 안전한 암호 알고리즘은 2048비트 이상이지만 향후 활용될 시기를 고려해서 3072비트 이상의 보안강도를 제공하는 암호 알고리즘을 사용하기를 권장함
- 공개키/개인키 유효기간은 **최대 2년**으로 설정하기를 권장

미래창조과학부
Ministry of Science, ICT and Future Planning
427-700 경기도 과천시 관문로 47(중앙동, 과천청사 4동)
대표전화 : 국번없이 1335 www.msip.go.kr

KISA 한국인터넷진흥원
Korea Internet & Security Agency
138-950 서울특별시 송파구 중대로 109번지 대동빌딩
Tel: 02-405-5114 Fax: 02-405-5119 www.kisa.or.kr