국정원 검증필암호모듈
CM-214-2027.10

RTCrypto v1.2
제품 소개서

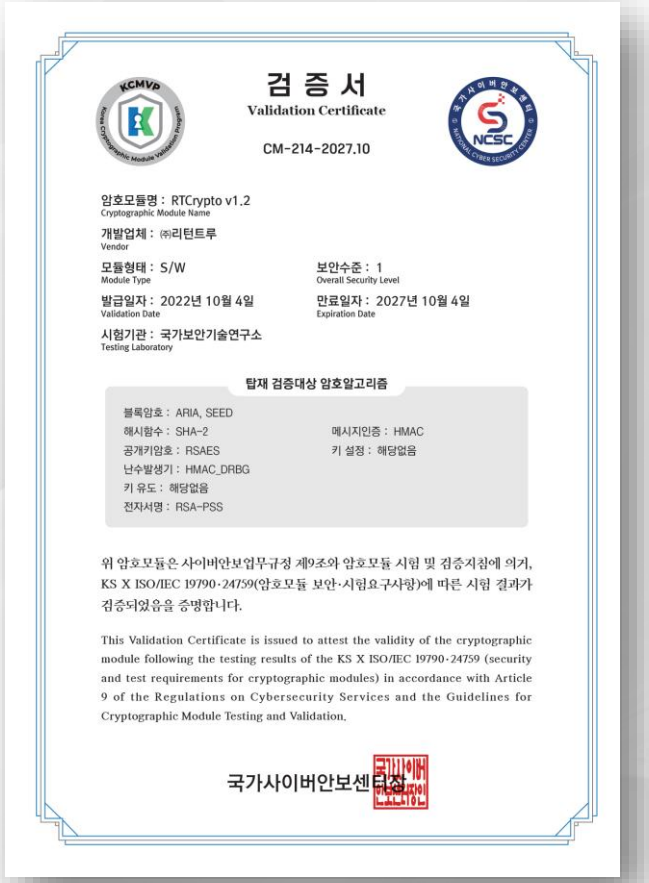
ReturnTrue
SOFTWARE DEVELOPMENT

주식회사 리턴트루

CONTENT

검증필암호모듈 개요

디지털 전환이 가속화되면서 기업과 기관은 각종 사이버 위협으로부터 중요한 정보를 안전하게 보호해야 하는 과제에 직면하고 있습니다. 이에 따라 국가 차원에서는 암호기술의 안정성과 신뢰성을 확보하기 위해 국가용 암호모듈 검증제도(KCMVP, Korea Cryptographic Module Validation Program)를 운영하고 있으며, 검증을 통과한 암호모듈만이 공공 및 금융 등 주요 분야에서 활용될 수 있습니다.



검 증 서
Validation Certificate

CM-214-2027.10

암호모듈명 : RTCrypto v1.2
Cryptographic Module Name

개발업체 : ㈜리턴트루
Vendor

모듈형태 : S/W
Module Type

보안수준 : 1
Overall Security Level

발급일자 : 2022년 10월 4일
Validation Date

만료일자 : 2027년 10월 4일
Expiration Date

시험기관 : 국가보안기술연구소
Testing Laboratory

탑재 검증대상 암호알고리즘

블록암호 : ARIA, SEED
해시함수 : SHA-2
메시지인증 : HMAC
공개키암호 : RSAES
키 설정 : 해당없음
난수발생기 : HMAC_DRBG
키 유도 : 해당없음
전자서명 : RSA-PSS

위 암호모듈은 사이버안보업무규정 제9조와 암호모듈 시험 및 검증지침에 의거, KS X ISO/IEC 19790·24759(암호모듈 보안·시험요구사항)에 따른 시험 결과가 검증되었음을 증명합니다.

This Validation Certificate is issued to attest the validity of the cryptographic module following the testing results of the KS X ISO/IEC 19790·24759 (security and test requirements for cryptographic modules) in accordance with Article 9 of the Regulations on Cybersecurity Services and the Guidelines for Cryptographic Module Testing and Validation.

국가사이버안보센터장

- **암호모듈 검증제도**는「사이버안보 업무규정」제9조와「전자정부 시행령」제69조 등에 따라 비밀로 분류되지 않은 중요 자료를 보호하기 위해 국가·공공기관에서 도입하는 **암호모듈의 안전성과 구현 적합성을 검증하는 제도**
- 검증필 암호모듈은 기본적인 암·복호화 기능 뿐만 아니라 암호가 안전하게 사용될 수 있도록 중요보안매개변수 관리 등 추가적인 보안기능도 탑재하여 **정보의 유출, 위·변조, 훼손 등을 방지**하기 위한 **기밀성·무결성·인증·부인방지 등의 기능을 제공**
- 국가정보원은 국가·공공기관 도입기준으로 **검증필 암호모듈 탑재를 필수로 요구**

국가 보안 표준 준수

- 국가정보원 KCMVP(국가용 암호모듈 검증제도) 인증 획득
- 공공·금융기관에서 요구하는 보안 규격 충족
- 국제 보안 표준과 호환성 보장

안전한 데이터 보호

- 데이터 암호화, 전자서명 등 핵심 보안 기능 제공
- 무결성 검증 및 안전한 난수 생성으로 정보 유출·위변조 방지

검증된 신뢰성과 확장성

- 국가 공인 검증 과정을 거쳐 보안성 입증
- 금융권, 공공기관 등 주요 분야에 바로 적용 가능
- 고객 요구에 맞춘 커스터마이징 지원

(주)리턴트루는 KCMVP를 3회 획득하였으며 한국인터넷진흥원의 암호모듈 컨설팅 사업을 2회 수행하였습니다.

암호모듈의 주요 기능 및 특징

주요 알고리즘 탑재 + 다양한 운영체제 지원 + 오랜 기간 안정성 확보 + 국내 최저비용

주요 기능

데이터 암호화/복호화	• 국가 표준 알고리즘 지원 (SEED, ARIA)
공개키 암호화	• 키 교환 및 전자서명을 위한 공개키 기반 암/복호화 기능 제공
전자서명/검증	• RSA 공개키 알고리즘 지원 (ECDSA 비검증으로 지원)
키 관리 기능	• 안전한 키 생성 기능 제공
메시지 인증 (MAC)	• 데이터의 무결성 및 인증을 위한 메시지 인증 코드 생성 및 검증 기능
난수 생성	• FIPS/KCMVP 기준 충족 난수 생성기 제공 (대칭키 생성)
인터페이스 지원	• C, JAVA 등 다양한 애플리케이션 연동 API 제공

특징

KCMVP 인증 획득	• 총 3회에 걸쳐 KCMVP 인증 획득
보안성 검증 완료	• 다양한 고객사에서 오랜 시간 사용됨으로 인한 안정성 및 보안성 검증 완료
다중 운영체제 지원	• Windows, Linux, HP, AIX, SUN 운영 환경을 지원하여 폭넓은 활용이 가능
안정적인 기술지원	• KCMVP 인증을 수행한 고급인력 직접 기술지원
맞춤형 지원	• 고객사의 요구에 맞는 프로세스에 해당하는 채널 암호화, 데이터 암복호화, 전자서명/검증 등에 대한 예제 프로그램 지원
비용 절감	• 국내 최저 금액으로 무제한으로 사용 가능

검증받은 알고리즘 및 운영 환경

KCMVP 검증 받은 모듈

운영환경	운영환경 상세	라이브러리	추가 제공 모듈
Windows	Windows 10 (32/64bit)	**RTCrypto_W32.dll** **RTCrypto_W64.dll**	RTCryptoEx_W32.dll RTCryptoEx_JNI_W32.so RTCryptoEx_W64.dll RTCryptoEx_JNI_W64.so
Linux	Linux 64bit	**libRTCrypto_L64.so**	libRTCryptoEx_L64.so libRTCryptoEx_JNI_L64.so
HP-UX	HP-UX 11.31 64bit	**libRTCrypto_H64.sl**	libRTCryptoEx_H64.so libRTCryptoEx_JNI_H64.so
AIX	AIX 7.1 64bit	**libRTCrypto_A64.so**	libRTCryptoEx_A64.so libRTCryptoEx_JNI_A64.so
Solaris	Solaris 11.1 64bit	**libRTCrypto_S64.so**	libRTCryptoEx_S64.so libRTCryptoEx_JNI_S64.so

- 암호모듈을 사용하는 환경에 따라 **인증 받은** 모듈과 전자서명값이 포함된 서명된 파일 제공 (RTCrypto_000.dat)
- RTCryptoEx_000.dll 파일은 암호모듈을 사용하는 기관에서 쉽고 편리하게 암호모듈을 개발하기위해 제공되는 추가 모듈
- Java에서 암호모듈을 사용하기위한 JNI 모듈은 별도로 제공

KCMVP 검증 받은 알고리즘

분류	알고리즘/운영모드	참조표준
블록암호	ARIA-CBC,CTR |K|=128,192,256	KSX1213
	SEED-CBC,CTR |K|=128	TTAS.KO-12.0004
공개키암호	RSAES-OAEP |n|=2048 |hash| = SHA256	ISO/IEC 18033-2
전자서명	RSASSA-PSS |n|=2048 |hash| = SHA256	ISO/IEC 14888-2 ISO/IEC 14888-3 TTAS.KO-12.0001/R1 TTAS.KO-12.0015
해시함수	SHA-256	ISO/IEC 10118-3 Amd 1
	SHA-512	
메시지 인증코드	HMAC SHA-256	ISO/IEC 9797-2
	HMAC SHA-512	
난수발생기	HMAC_DRBG_SHA-256	ISO/IEC 18031

- 암호모듈을 구매 시 검증필 받은 알고리즘 전체 사용 가능
- 운영환경 및 알고리즘을 확인 후 구매 결정 필요
- 검증대상 외의 알고리즘은 필요시 비검증대상으로 지원 가능 (문의)

암호모듈 적용 시 기대 효과

"보안성·신뢰성·효율성을 확보하여 비즈니스 경쟁력 강화"

보안성 강화

- 국가검증(KCMVP) 기준 충족 → 공공·금융기관 보안 요건 만족
- 데이터 암호화 및 무결성 보장으로 정보 유출·위변조 방지

신뢰성 확보

- 국가 공인 인증으로 대외 신뢰도 상승
- 시스템 및 서비스의 안정성과 지속 가능성 보장

규제 대응 및 인증 용이

- 공공조달, 금융권 사업 참여에 필수 요건 충족
- 각종 보안 관련 규제 및 감사 대응 용이

운영 효율성 및 비용 절감

- 표준화된 모듈 적용으로 개발/검증 비용 절감
- 국내 최저 가격으로 도입 비용 및 유지보수 비용 절감

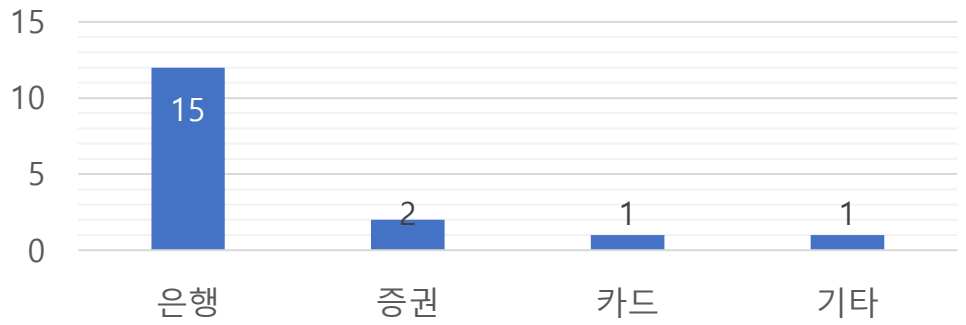
비즈니스 경쟁력 강화

- 보안 인증 기반으로 신규 사업·고객사 확보 용이
- 차별화된 보안 가치 제공 → 매출 확대 기여

주요 레퍼런스

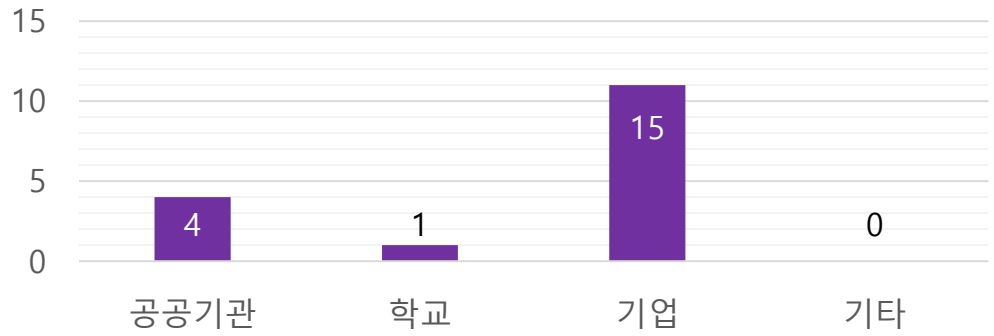
금융기관

금융결제원 · NH투자증권 · 우정사업본부 · 신한금융투자 · KB국민은행 · K bank · 수협 · DGB대구은행 · 우리은행 · LOTTECARD · IBK기업은행 · KEB 하나은행 · SBI 저축은행 · NH Bank · 신한은행 · MG새마을금고 · iM뱅크 · kakaobank · BNK 부산은행



공공, 학교, 기업

FUJITSU · KEPCO · AlphaBit · KAC 한국공항공사 · STRIX · TS 한국교통안전공단 · duplex · LOCKIN · 극동대학교 FAR EAST UNIVERSITY · Nable Communications · KRX 한국거래소 · REMTECH · koscom · COSOSYS · 지란지교에스앤씨 · KOREAN AIR · KORNEC · NNE · Nable · ENlighten



도입 절차 및 지원 체계

표준화된 도입 절차와 전문 기술 지원 체계를 통해 안정적 구축과 신속한 운영을 보장

암호모듈 도입(구매) 절차

견적 의뢰	• 유선 또는 메일을 통한 문의 • 고객 환경에 맞는 견적 • 메일을 통한 발주	온라인
계약 및 모듈 전달	• 라이선스 방식 (서버, 클라이언트 대수 제한 없음) • 메일을 통한 모듈 전달	국내 최저가격
개발 및 기술지원	• 암호모듈을 개발한 개발자가 기술지원 수행 • 계약이 따라 온/오프라인 기술지원	고급 인력
하자/유지 보수	• 1년간 무상 유지보수 • 1년 이후 별도 계약을 통한 유상 유지보수 (업데이트된 암호모듈 갱신 등)	지속/안전성

기술 지원 체계

컨설팅 지원	• 암호화 적용을 위한 컨설팅 지원 • 중요정보 암호화 관련 기술문의 대응 • 데이터 암호화, 채널 암호화 관련 기술 문의 지원
샘플 제공	• RTCrypto 암호모듈을 사용하기 위한 알고리즘 선택 지원 • 선택된 알고리즘에 해당하는 API 예제 파일 제공 및 가이드 제공
기술 지원	• API 적용 시 오류 등에 대한 원인 분석 • API 사용 문의 기술 지원

국정원 검증필암호모듈
CM-214-2027.10

감사합니다

제품 및 기술 문의

- 이상준 대표이사
- 031-784-8280
- joonir@rtruesoft.kr

ReturnTrue
SOFTWARE DEVELOPMENT

주식회사 리턴트루