유넷

TCLM & TMCLM V1.1
KCMVP 검증필 암호모듈 제품 소개서

목차

1. TCLM & TMCLM V1.1 개요

- **제품명**

- TCLM (TrustNET Crypto Library Module) for C V1.1 &
  TMCLM (TrustNET Mobile Crypto Library Module) for C V1.1

- **버전정보** : V 1.1

- **제품설명**

- 블록암호 알고리즘 및 블록 암호운영모드, 해시함수,
  메시지인증코드, 난수발생기, 공개키 암호, 전자서명 등의

국정원 암호 모듈 검증 적합

국정원 암호 모듈 검증 적합 판정으로 시스템 안전성과 구현 적합성을 검증 받았습니다.

- 암호관련 서비스를 소프트웨어 암호 라이브러리 형태로 구현한 암호모듈로서
  응용 프로그램과 연동되어 다양한 암호서비스 (기밀성, 무결성, 부인방지 등) 기능을
  지원한다.

- **검증대상 운영환경**

- Windows XP SP2, Windows 7, Windows 8, Windows 8.1, Windows 10 등
  검증대상 운영환경을 모두 지원한다.
- 모바일은 안드로이드 2.3 이상, iOS 6.1 이상 지원한다

2. TCLM & TMCLM V1.1 지원 알고리즘 & 검증필 목록

- 지원 검증대상 알고리즘

구분	보호함수	운영모드	키길이
블럭암호	ARIA	ECB, CBC, OFB, CFB128, CTR128	|K|=128,192,256
	HIGHT	ECB, CBC, OFB, CFB64, CTR64	|K|=128
	LEA	ECB, CBC, OFB, CFB128, CTR128	|K|=128,192,256
	SEED	ECB, CBC, OFB, CFB128, CTR128	|K|=128
해시함수	SHA224,256,384,512	-	-
HMAC	HMAC with SHA224,256,384,512	-	-
난수발생기	HASH-DRBG with SHA256	-	-
공개키 암호	RSAES-OAEP	-	|n|=2048, 3072
전자서명	RSA-PSS KCDSA	-	|n|=2048, 3072 |n|=2048

- 검증필 암호모듈 목록
  - https://www.nis.go.kr:4016/AF/1_7_3_3/list.do 내 **검증필 암호모듈 목록** 참조

연락처 Contact us

회사

- 전화 : 02-2088-3030
- 팩스 : 02-2088-3095
- 이메일 : info@unet.kr
- 주소 : 서울 영등포구 당산로41길11, W905호 (당산동4가, 당산 SK V1센터)

마케팅

- 전화 : 02-6748-0201
- 이메일 : mkt@unet.kr

영업

- 전화 : 02-6748-0207
- 이메일 : sales@unet.kr

기술

- 이메일 : support@unet.kr

고맙습니다

THANK YOU

UNET 유넷