TechLab 2000
R & D Company

TEACUP

Key Management System

SECURE PKI

TEACUP is designed to be the core element of Public Key Infrastructure (PKI). It supports integrated functionality of Certificate Authority (CA) and Registration Authority (RA), which makes it optimal and efficient solution for small and medium PKI installations. TEACUP encompass highest class security solutions. It's correctness and fidelity is proved by the certification according to Common Criteria EAL4 level with high security function strength. Basing on that Internal Polish Security Agency approved TEACUP for systems with up to "Secret" level informations. TEACUP is unique composition of hardware component (HSM++), dedicated application, data base, cryptographic key tokens and PC workstation together with optional WWW, SCEP and LDAP servers. All the most important data and operations are always performed in hardware component, which is more than a HSM in that it "understands" information it processes. Cryptographic keys never never leaves in plain the hardware components. Moreover CA private key is stored on smartcards with split knowledge schema. Cryptographic algorithms are fed with true random bitstring coming from thermal noise. Despite its high-end security TEACUP is still easy to operate due to wizard based PC application.

IMPORTANT

- CA & RA FOR PKI
- CERTIFIED TO "SECRET" LEVEL
- DEEPLY EXAMINED PROTECTIONS
- EASY TO OPERATE

KEY FEATURES

- Split knowledge mechanism for CA private key storage
- Hardware components employs tamper resistance & evidence
- Cryptographic keys held on smartcards and USB tokens
- Smartcard readers with locks (only the owner can get the card back)
- HSM++ equipped with own PIN-pad and display for local management and PIN entry
- „Panic" button disarms the device
- Dedicated interface for maintenance
- Embedded security controller with battery backup
- Mechanisms for hardware and software integrity verification
- State management of HSM++: operational, transport, in-danger, dead
- Hardware true random bitstring generator
- Secure (encrypted and authenticated) software upgrade technology
- Easy to operate in spite of high security
- Versatile solution because of Public Key Infrastructure (PKI)
- Easy adaptable for new solutions

CURRENT APPLICATIONS

- CA and RA for encrypting analog telephones CYGNUS: Silver, Gold, Platinum)
- CA and RA for encrypting ISDN telephones CYGNUS: Diamond, Titanium, Titanium+
- CA and RA for encrypting GSM telephones CYGNUS
- CA and RA for encrypting plug-in REA for two-way radio
- CA and RA for encrypting ISDN NT2 terminals: ONYX1001, AGATE-P, AGATE-T
- CA with LDAP and RA via SCEP for VPN routers NEFRYT

TEACUP Key Management System

HSM++ SECURITY	
TAMPER PROOF	▪ robust mechanical design
TAMPER EVIDENT, INTEGRITY CHECK	▪ mechanical, electronic sensors ▪ encrypted and signed software ▪ individual per HSM++ cryptographic key for integrity check
CRYPTOGRAPHIC KEYS PROTECTION	▪ generation based on true random bit generator (RBG) ▪ secure media with PIN ▪ split knowledge (2/8 schema, CA keys only)
DATA PROTECTION	▪ exported data is signed, sensitive additionally encrypted
SOFTWARE UPGRADE	▪ Secure Upload technology (TechLab's 2000 proprietary)
CRYPTOGRAPHY ALGORITHMS	
ASYMMETRIC	▪ RSA 1024 – 4096 bits (PKCS#1)
SYMMETRIC	▪ AES: key 256 bits, block 128 bits (FIPS 197) ▪ IDEA: key 128 bits, block 64 bits
DIGEST	▪ SHA-1 and SHA-256 (FIPS 180-2)
RSA OPERATIONS RATES FOR 2048 BITS KEYS	
KEY GENERATION	▪ typically 33 s but usually unnoticeable due to background operation
SIGNATURE GENERATION	▪ 90 ms
SIGNATURE VERIFICATION	▪ 15 ms
DATA FORMATS	
PUBLIC KEY CERTIFICATES	▪ X.509 v3 (DER coded X.690)
CERTIFICATES REVOCATION LISTS (CRLS)	▪ X.509 v2 (DER coded X.690)
SIGNATURE	▪ PKCS#1_v1_5
CERTIFICATES AND CRLS DIRECTORY	▪ LDAP
REMOTE CERTIFICATES REQUESTS	▪ SCEP
INTERFACES	
APPLICATION	▪ USB 2.0 full-speed
AUDIT	▪ USB 2.0 full speed
ACCEPTABLE MEDIA	
INFINEON SLE66CX322P WITH CARDOS/M4.01A (SIEMENS)	▪ CA and user keys
INFINEON SLE66CX322P WITH SETEC SETCOS 4.4.1 (SETEC)	▪ CA and user keys
SECURE USB DEVICE	▪ user keys
PC REQUIREMENTS	
SYSTEM	▪ Windows XP

Śniadeckich 10/1, 00-656 Warszawa, Poland, tel/fax: +48 22 625 53 19
office@tl2000.com.pl www.tl2000.com.pl