The Poor Man’s (TPM) HSM
DNSSEC and TPMs

Richard Lamb

ICANN 44th Meeting, June 2012
Prague, CZ
• PKCS11
• My modified dnssec-signzone
  (opensslrsa_link.c – direct pkcs11 – no engine)
• Only need C_Sign  C_GenerateKeyPair
• Smartcard = 1 sig/sec
• OpenSC
• Open source PKCS11 for TPM = Opencryptoki and Trousers by IBM
• 1 1024 RSA sig/sec
..or this (from .cr)

Offline Laptop with TPM

Sign ZSKs with KSK

Generate KSK

Secure Off-line Environment

Transport public half of ZSKs

Transport KSK signed DNSKEY RRsets

Online/off-net DNSSEC Signer with TPM

Unsigned zone

Sign zones with ZSK

Generate ZSKs

Signed zone

Signed zones with ZSK

Offline/signed zone

Online/unsigned zone

Transport KSK signed DNSKEY RRsets

Secure Off-line Environment
• ATMEL AT97SC3204 25 sig/sec??
• Generate keys inside TPM
• A certified RNG
• Private keys ALWAYS encrypted
• Infinite number of keys
• Backup support: TPM_CreateMigrationBlob
• RSA 2048/1024
• Got 5-10 sig/sec
int main(void)
{
    int n;
    uint8_t *p;
    uint32_t crc, ret;
    serial_docmd: --> TPM_SIGN len:63 crc:3423C8C8 sent
    int i, llen;
    hash-info: tpm_command2: sent OA000000
    hash-info: tpm_sign: handle = B4CAF12B
    CPU_FRESCALE(0); /hash-info: tpm_command2: sent 3C000000
    hash-info: session[0] HMAC validation: passed
    LED_CONFIG;
    // LED_ON;
    dnssec-signzone: cz/MX:
    // #ifdef BLINKY
    serial_docmd: --> TPM_SIGN len:63 crc:0CD7D1E2 sent
    for (;;) {
        hash-info: tpm_command2: sent OA000000
        hash-info: tpm_sign: handle = B4CAF12B
        delay_ms(1000);
    }
    #endif
    hash-info: session[0] HMAC validation: passed
    usb_init(); // rem
    dnssec-signzone: cz/DNSKEY:
    rsig by cz/RSASHA256/11224 retained
    dnssec-signzone: 8E5KJ76K3QTF1JOJ968DSR204CPQ3G.CZ/NSEC3:
    LED_OFF;
    dnssec-signzone: --> TPM_SIGN len:63 crc:310ADE82 sent
    hash-info: tpm_command2: sent OA000000
    hash-info: tpm_sign: handle = B4CAF12B
    hash-info: tpm_command2: sent 3C000000
    hash-info: session[0] HMAC validation: passed
    twi_init();
    Verifying the zone using the following algorithms: RSASHA256.
    Zone signing complete:
    Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
    ZSKs: 1 active, 0 present, 0 revoked
    /signzone.cz.tmp.signed
    // toggle PD4 when
    dnssec-signzone: debug 1: decrement_reference: delete from rbt: 0xb7e6
    DDRD |= (1<<4); 204CPQ3Q6.CZ
    PORTD &= ~(1<<4);
    serial_docmd: --> TPM_FLUSHKEY len:8 crc:5CA08063 sent
    hash-info: tpm_command2: sent EA000000
    serial_docmd: --> TPM_RESET len:4 crc:CD2B78D5 sent
    hash-info: tpm_command2: sent SA000000
    pkcs11: C_Finalize
    Created cz.zone.signed

Thank You