The Poor Man's (TPM) HSM

DNSSEC and TPMs

Richard Lamb

ICANN 44th Meeting, June 2012

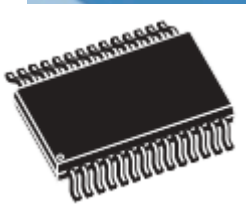
Prague, CZ

- PKCS11
- My modified dnssec-signzone (opensslrsa_link.c – direct pkcs11 – no engine)
- Only need C_Sign   C_GenerateKeyPair

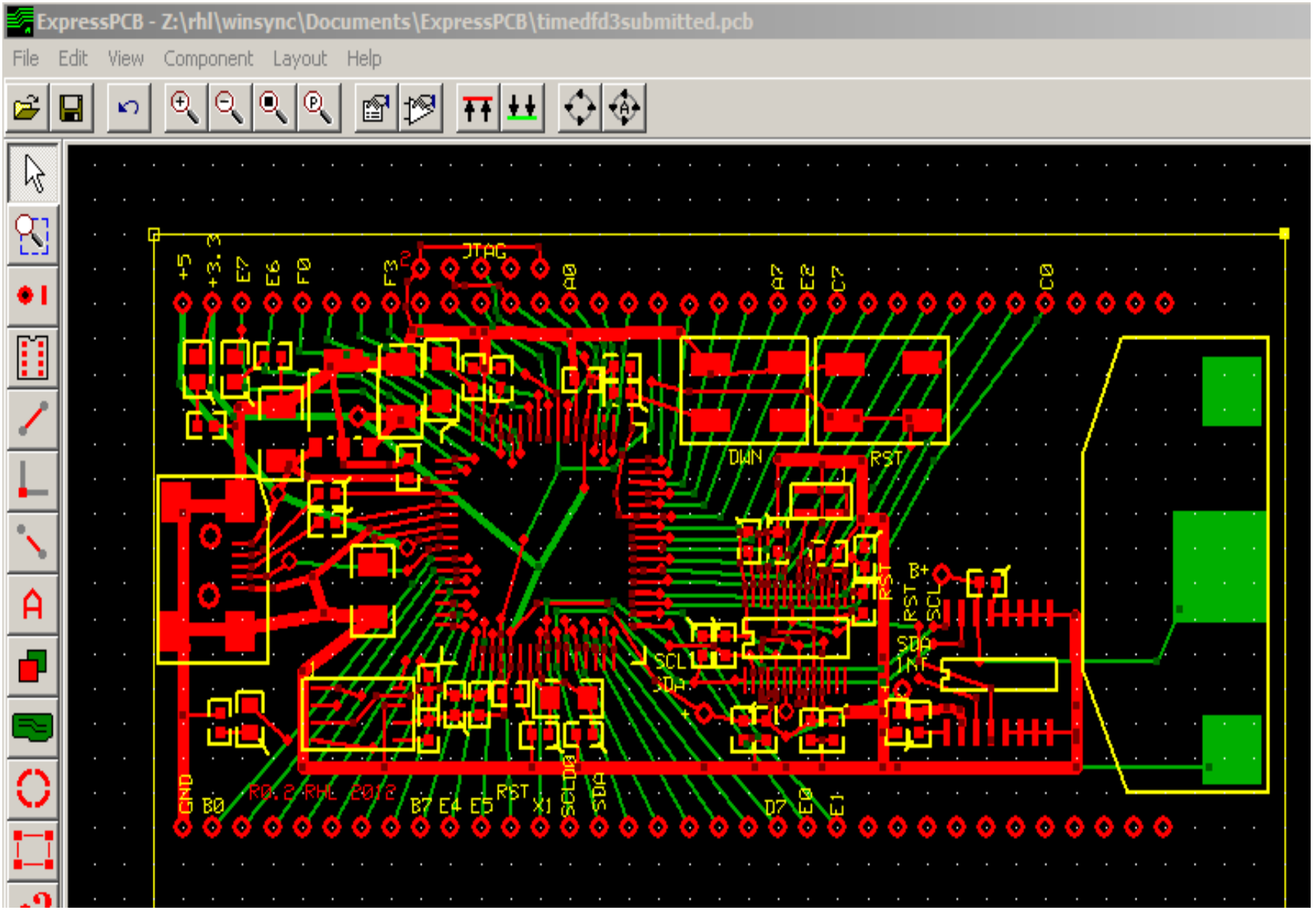
- Smartcard = 1 sig/sec
- OpenSC

- Open source PKCS11 for TPM =
  Opencryptoki and Trousers by IBM
- 1 1024 RSA sig/sec

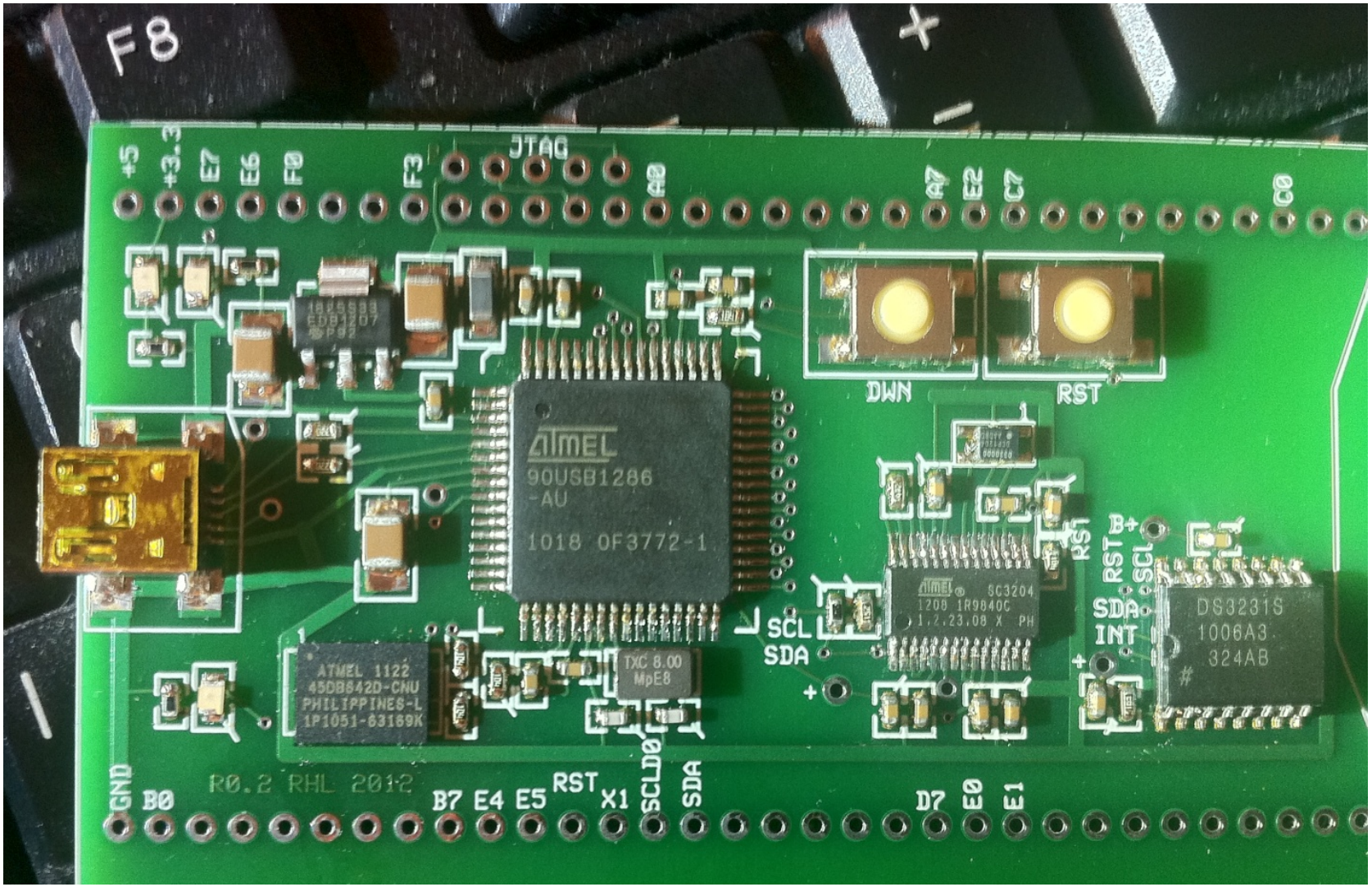
..or this (from .cr)

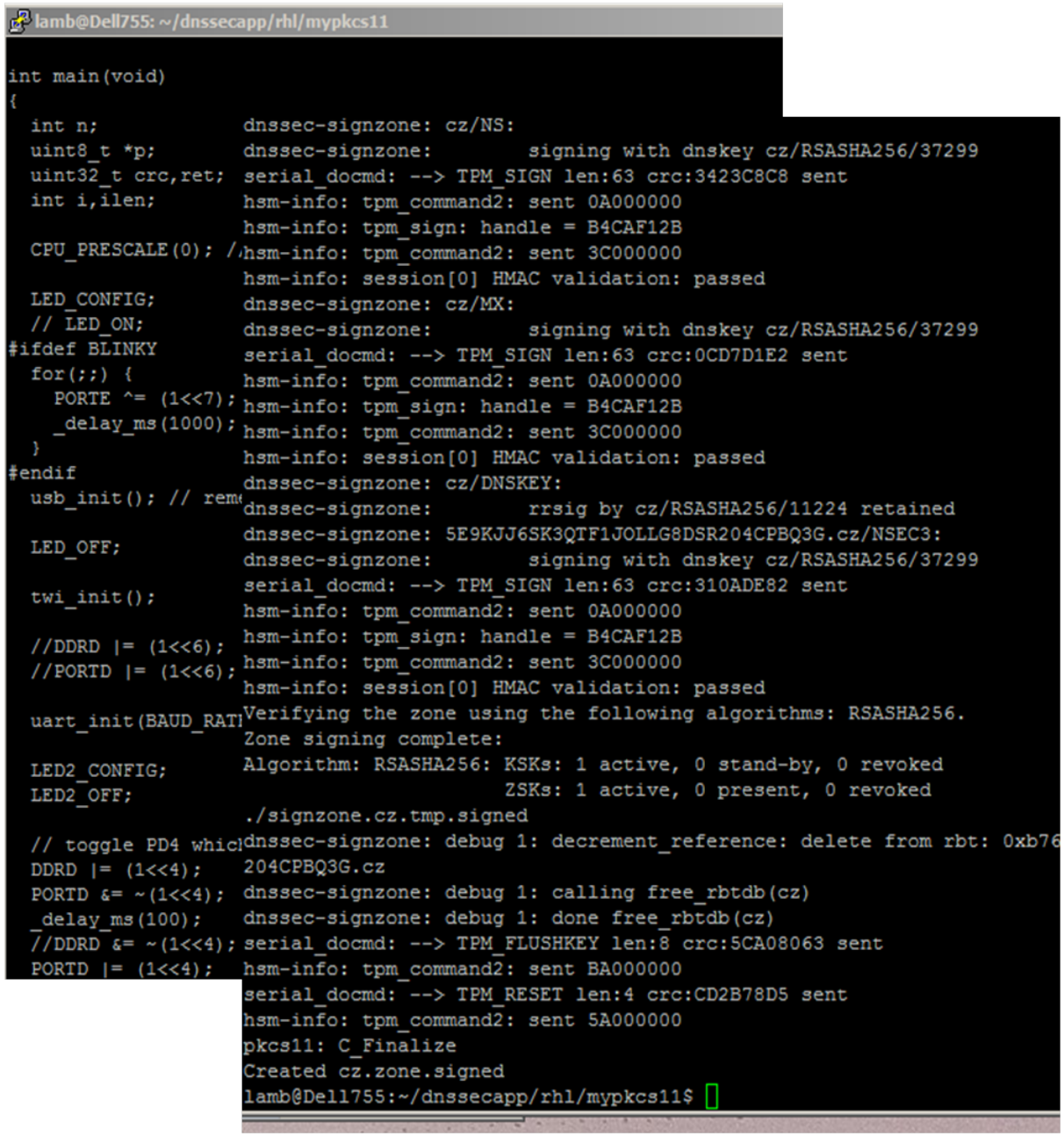


- ATMEL AT97SC3204 25 sig/sec??
- Generate keys inside TPM
- A certified RNG
- Private keys ALWAYS encrypted
- Infinite number of keys
- Backup support: TPM_CreateMigrationBlob
- RSA 2048/1024
- Got 5-10 sig/sec


ExpressPCB - Z:\rhl\winsync\Documents\ExpressPCB\timedfd3submitted.pcb
File Edit View Component Layout Help
+5
+3.3
E7
E6
F0
F3
JTAG
A0
A7
E2
C7
C0
DWN
RST
B+
SCL
SDA
INT
GND
B0
RD.2 RHL 2012
B7 E4 E5
RST
X1
SCL
SDA
D7
E0
E1


66
StoP
TEMP°F/°C
FUNCTION
TIMER/TOAST
BLACK&DECKER


F8
+5
+3.3
E7
E6
F0
F3
JTAG
A7
E2
C7
C0
DWN
RST
ATMEL
90USB1286
-AU
1018 0F3772-1
SCL
SDA
RST
B+
SCL
SDA
INT
DS3231S
1006A3
324AB
ATMEL 1122
45DB642D-CNU
PHILIPPINES-L
1P1051-63189K
TXC 8.00
MpE8
R0.2 RHL 2012
GND
B0
B7
E4
E5
RST
X1
SCLD0
SDA
D7
E0
E1


lamb@Dell755: ~/dnssecapp/rhl/mypkcs11
int main(void)
{
int n;
uint8_t *p;
uint32_t crc,ret;
int i,ilen;
CPU_PRESCALE(0); /
LED_CONFIG;
// LED_ON;
#ifdef BLINKY
for(;;) {
PORTE ^= (1<<7);
_delay_ms(1000);
}
#endif
usb_init(); // reme
LED_OFF;
twi_init();
//DDRD |= (1<<6);
//PORTD |= (1<<6);
uart_init(BAUD_RATI
LED2_CONFIG;
LED2_OFF;
// toggle PD4 whic
DDRD |= (1<<4);
PORTD &= ~(1<<4);
_delay_ms(100);
//DDRD &= ~(1<<4);
PORTD |= (1<<4);
dnssec-signzone: cz/NS:
dnssec-signzone: signing with dnskey cz/RSASHA256/37299
serial_docmd: --> TPM_SIGN len:63 crc:3423C8C8 sent
hsm-info: tpm_command2: sent 0A000000
hsm-info: tpm_sign: handle = B4CAF12B
hsm-info: tpm_command2: sent 3C000000
hsm-info: session[0] HMAC validation: passed
dnssec-signzone: cz/MX:
dnssec-signzone: signing with dnskey cz/RSASHA256/37299
serial_docmd: --> TPM_SIGN len:63 crc:0CD7D1E2 sent
hsm-info: tpm_command2: sent 0A000000
hsm-info: tpm_sign: handle = B4CAF12B
hsm-info: tpm_command2: sent 3C000000
hsm-info: session[0] HMAC validation: passed
dnssec-signzone: cz/DNSKEY:
dnssec-signzone: rrsig by cz/RSASHA256/11224 retained
dnssec-signzone: 5E9KJJ6SK3QTF1JOLLG8DSR204CPBQ3G.cz/NSEC3:
dnssec-signzone: signing with dnskey cz/RSASHA256/37299
serial_docmd: --> TPM_SIGN len:63 crc:310ADE82 sent
hsm-info: tpm_command2: sent 0A000000
hsm-info: tpm_sign: handle = B4CAF12B
hsm-info: tpm_command2: sent 3C000000
hsm-info: session[0] HMAC validation: passed
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
dnssec-signzone: debug 1: decrement_reference: delete from rbt: 0xb76
204CPBQ3G.cz
dnssec-signzone: debug 1: calling free_rbtdb(cz)
dnssec-signzone: debug 1: done free_rbtdb(cz)
serial_docmd: --> TPM_FLUSHKEY len:8 crc:5CA08063 sent
hsm-info: tpm_command2: sent BA000000
serial_docmd: --> TPM_RESET len:4 crc:CD2B78D5 sent
hsm-info: tpm_command2: sent 5A000000
pkcs11: C_Finalize
Created cz.zone.signed
lamb@Dell755:~/dnssecapp/rhl/mypkcs11$

Thank You