Towards Set and Forget DNSSEC

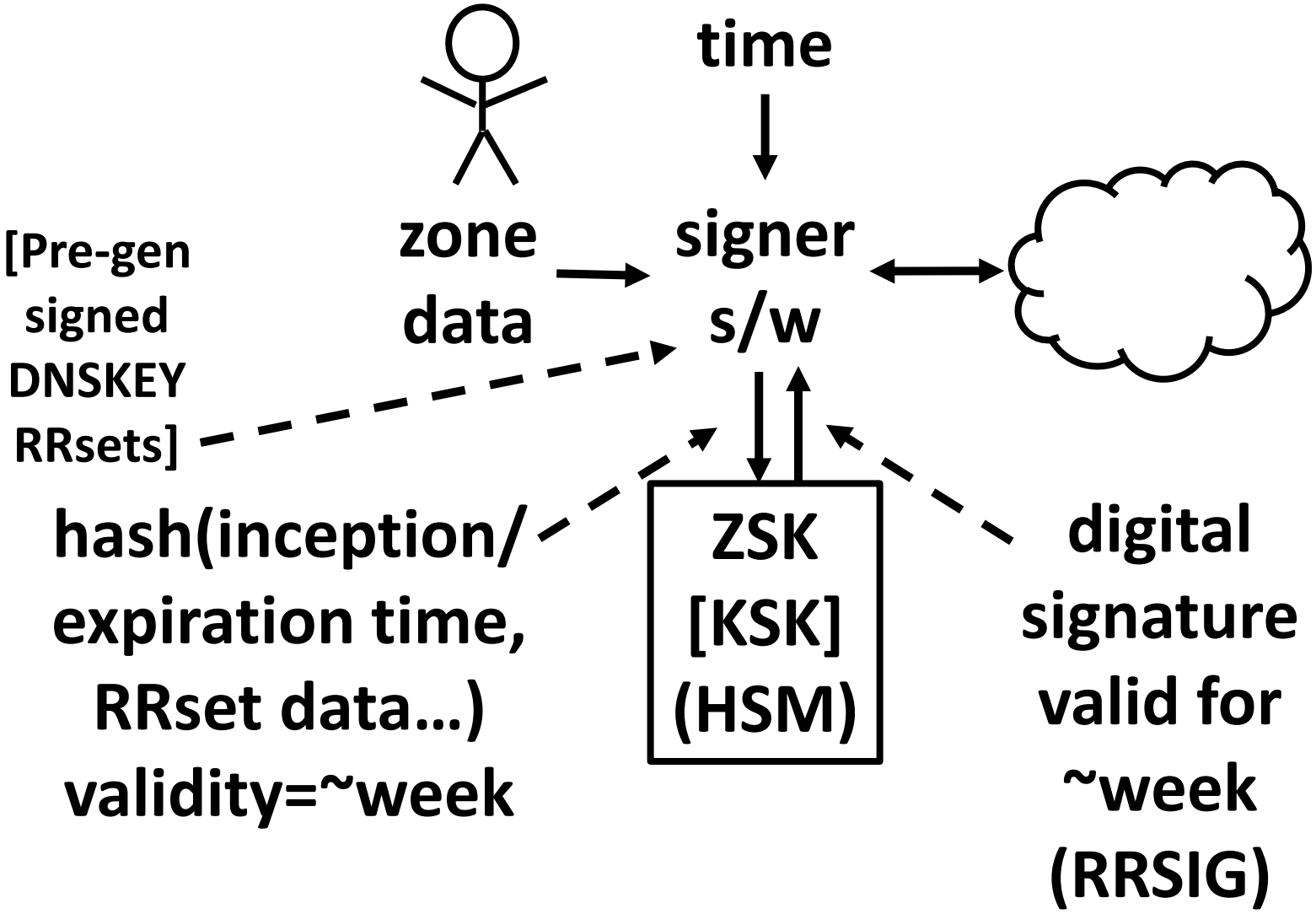
The beginning of the end of key management?

(The Poor Man's HSM Part 2)

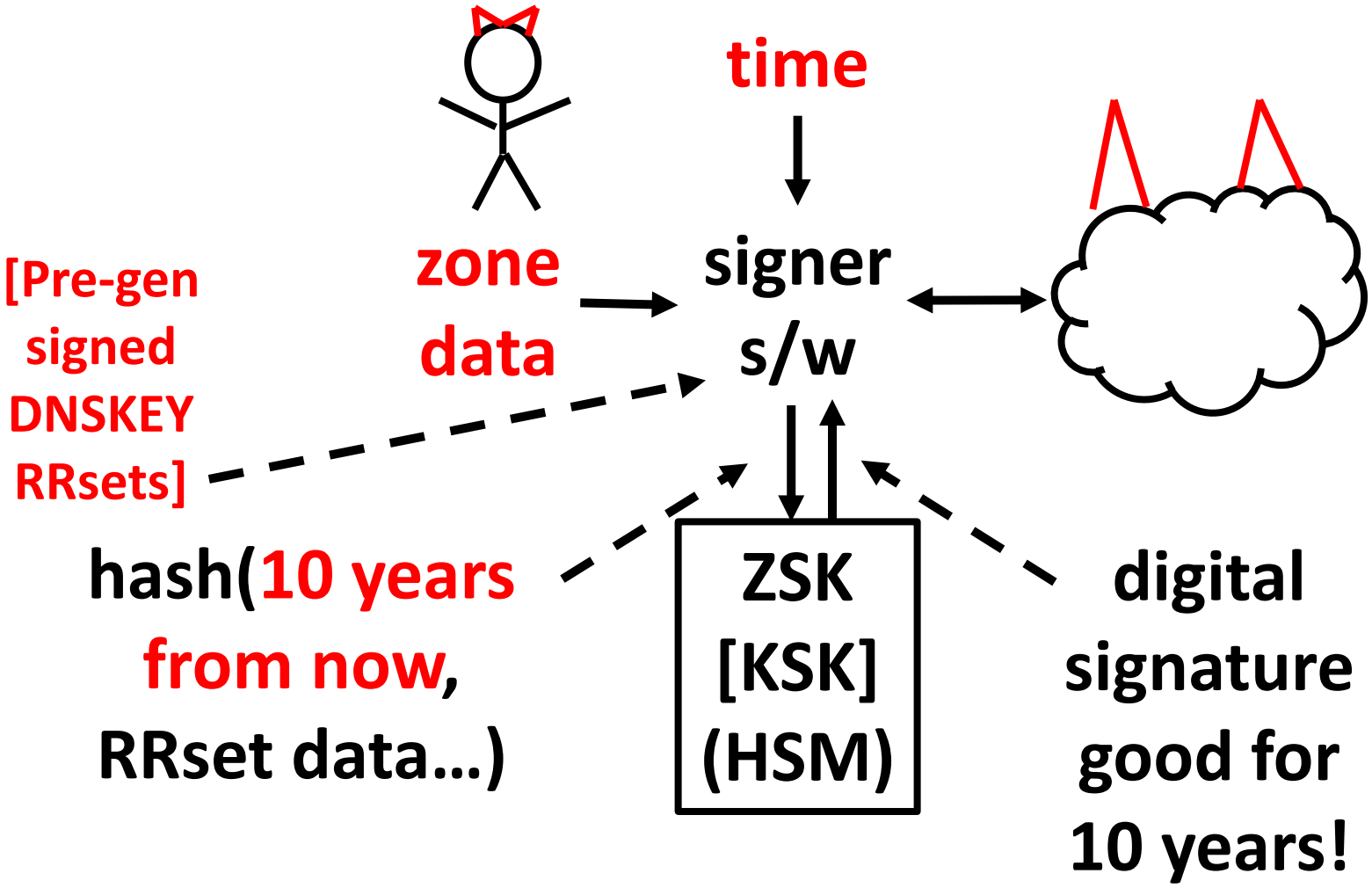
ccNSO Tech Day, 15 July 2013,
Durban, ZA,

Richard Lamb, slamb@xtcn.com

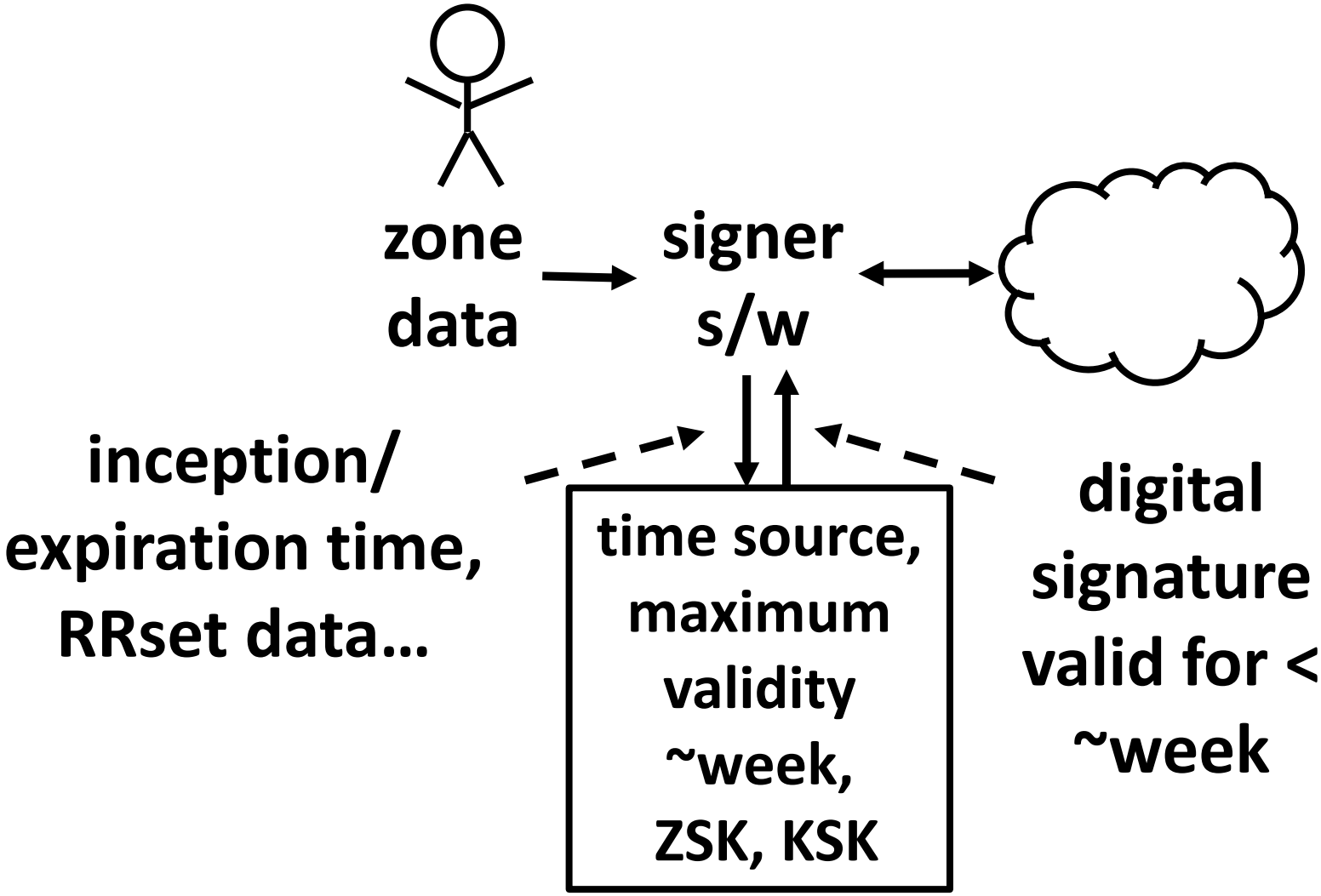
Typical Signer
(I am not a graphic artist!)



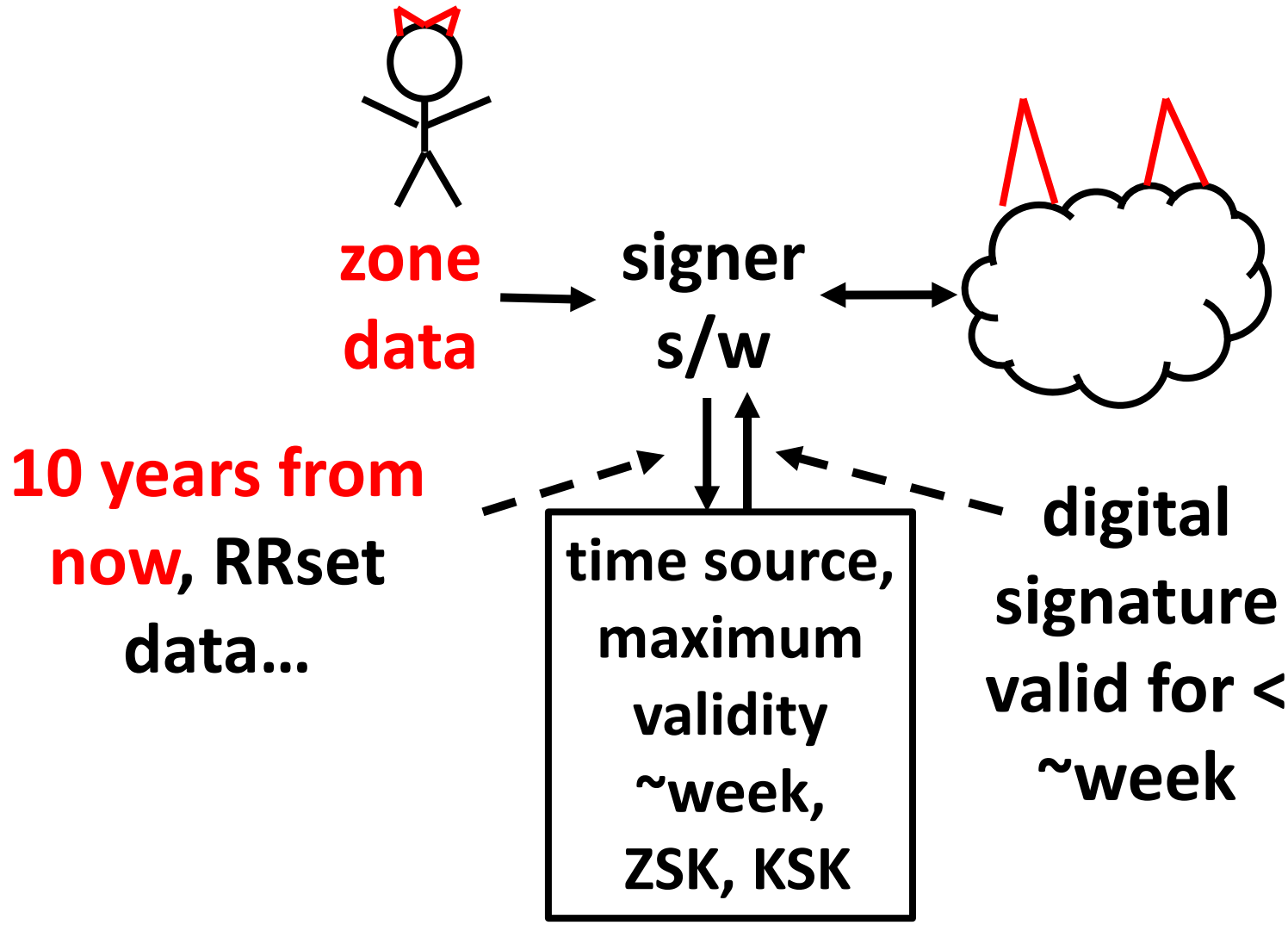
Compromise: not if but when



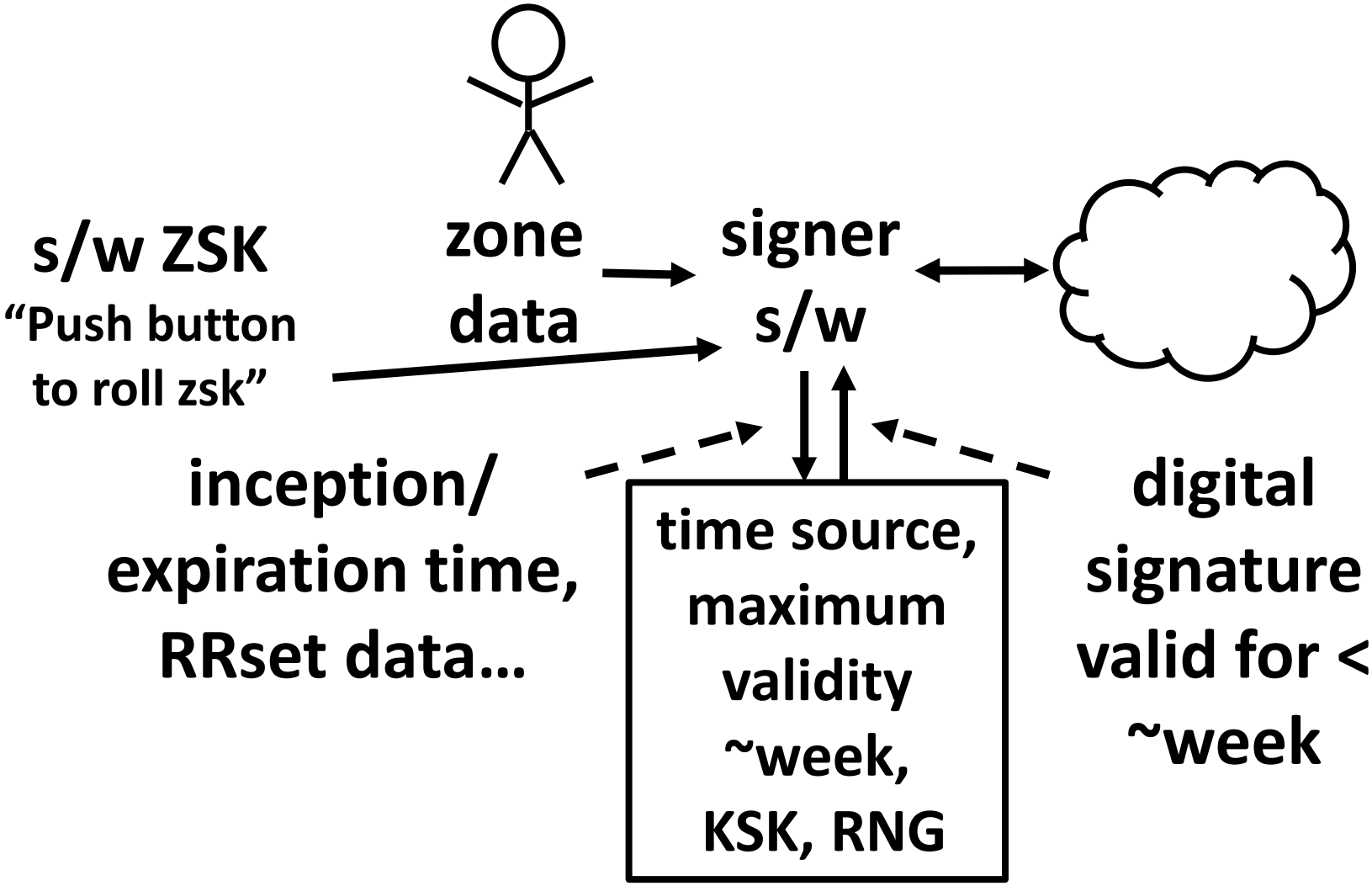
Safe Signer


zone
data
signer
s/w
inception/
expiration time,
RRset data…
time source,
maximum
validity
~week,
ZSK, KSK
digital
signature
valid for <
~week

Can always recover w/o dealing with parent (no KSK roll)

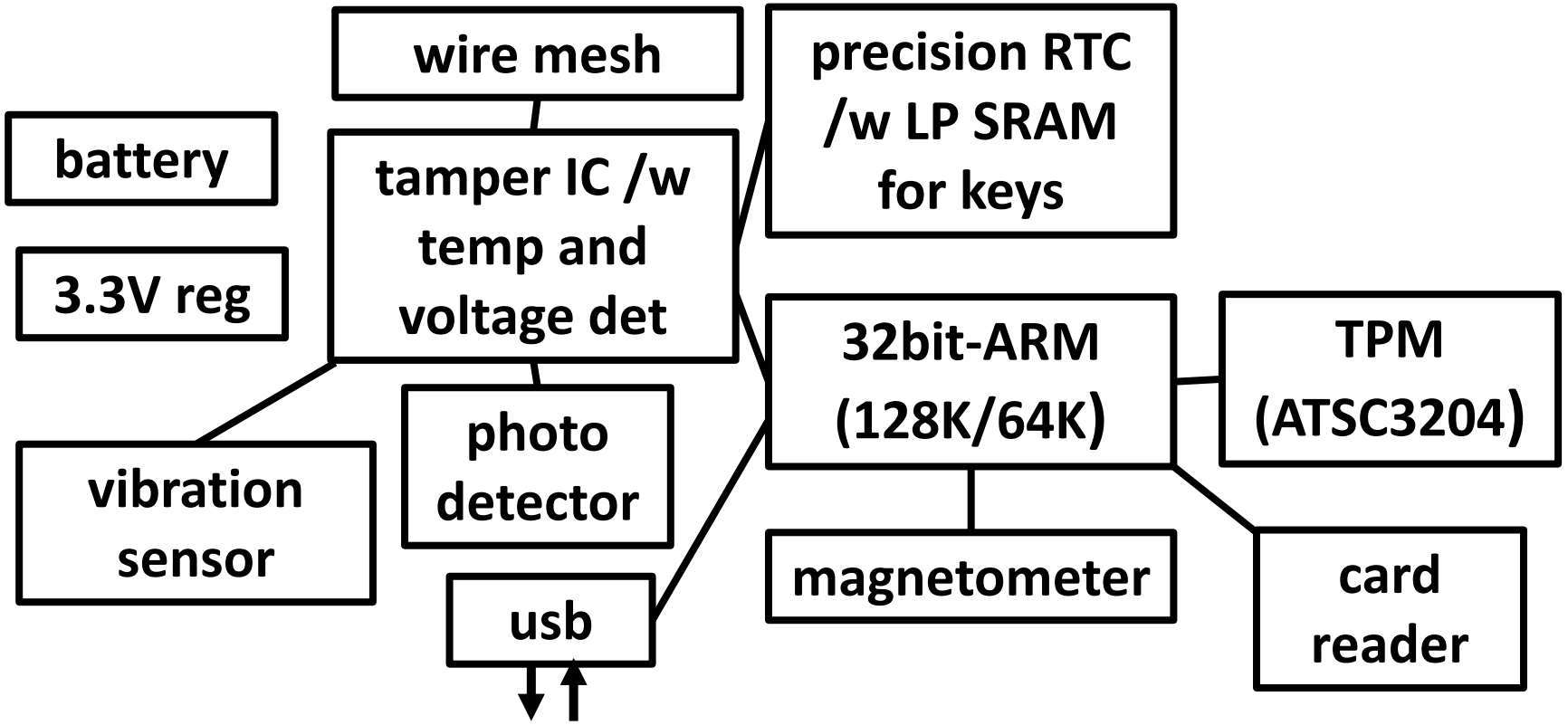


Further simplification



Problem: HSM's do not work this way

- Nothing stopping me from building it – we have the technology




H1
H2
J1
B1
B2
GND
H4
R0.6 (C) KLW 2013
CRYPTOBAT

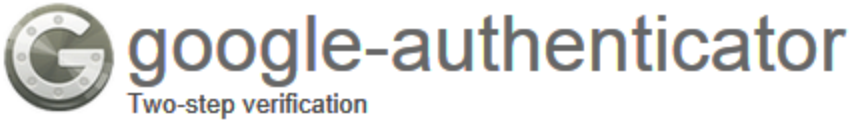

37
1
60A

Features

- **Tamper IC (STM1404) “supports” FIPS 140-2 level 4**
- **TPM ~20 1024 RSA/sec**
- **RNG**
- **2-factor M-of-N using built-in card reader or Google Authenticator Token for setting parameters (e.g., max validity), key generation, backup/migration**
- **Remote M-of-N capability**
- **modified BIND 9.9.2 RRSIG interface or pkcs11 driver**
- **2048bit RSA keyed firmware loader**
- **Tamper protected precision temperature compensated RTC (PCF2127)**
- **Low cost**

Authentication example

```
# screen /dev/ttyUSB0 115200
> version
Cryptobat firmware version 0.60.51D8207C (c) KLW rst:software
rtt:2296/4294967295     rstc: sr:00010300 mr:00000001
> date
Y:13 M:07 D:06 h:14 m:14 s:02 ok
1373120042
> colist
> coadd lamb
***write***read
Added CO: lamb
Secret: HZ5KNVA3KA3UYD2U
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/lamb?secret=HZ5KNVA
3KA3UYD2U
> colist
 |lamb| not present
> cologin lamb 192498
checkpin: del=0
 CO lamb Ok
> colist
 |lamb| present
> setmaxval 3600
 Configuration disabled
```



Cont..


```
> coadd jakob
***write***read
Added CO: jakob
Secret: 7MZDTPOU4JWESYFO
....
> colist
 |lamb| present
 |jakob| not present
> cologin jakob 061612
 Failed
> cologin jakob 107712
 CO jakob Ok
> colist
 |lamb| present
 |jakob| present
> setmaxval 3600
 Maximum validity period set to +3600 seconds
> coreset
> colist
 |lamb| not present
 |jakob| not present
> date
Y:13 M:07 D:06 h:14 m:20 s:07 ok
1373120407
```

Domain name: ABCC.
Token Key:
K4RYBJKUEZCUZU4A

Signing using modified dnssec-signzone

```
# bind-9.9.2-P2/bin/dnssec/dnssec-signzone -s now -e +300 -v 5 -x -o testzone -k Ktestzone.+008+35407 testzone Ktestzone.+008+58968
dnssec-signzone: debug 3: pkcs11_parse: Start
dnssec-signzone: debug 3: pkcs11: pkcs11_login: start
dnssec-signzone: debug 3: pkcs11: pkcs11_initlib Start
C_GetFunctionList+1636:
C_Initialize+1519:
serial_init+1872:Openned /dev/ttyUSB0
|> v2on|
|TWI_ConfigureMaster()|
|Using CKDIV = 1 and CLDIV/CHDIV = 158 CWGR=00019E9E|
C_GetSlotList+1414:
C_OpenSession+1430:
dnssec-signzone: debug 3: pkcs11: C_Login 1
C_Login+1394:
dnssec-signzone: debug 3: pkcs11: pkcs11_parse Ktestzone.+008+35407
C_FindObjectsInit+816:
C_FindObjects+943:          MATCHED 00000002
C_FindObjectsFinal+844:
C_FindObjectsInit+816:
C_FindObjects+943:          MATCHED 00000003
C_FindObjectsFinal+844:
C_GetAttributeValue+1014:
C_GetAttributeValue+1014:
dnssec-signzone: testzone/NSEC:
dnssec-signzone:               signing with dnskey testzone/RSASHA256/58968
dnssec-signzone: testzone/DNSKEY:
dnssec-signzone:               signing with dnskey testzone/RSASHA256/35407
dnssec-signzone: debug 3: pkcs11: rick_thsm doing pkcs11_RSA_sign TIMED
C_SignInit+673:
writecryptolcmd: |tpmloadkey| 559
```

Cont…

```
|> tpmloadkey|
|***write|
|***read|
|***write|
|***read|
|tpm_loadkey: handle = 3285047210  hex: 0xC3CDD7AA|
|ok: key loaded handle=C3CDD7AA|
C_SignInit+728:|ok: key loaded handle=C3CDD7AA|
C_SignInit+736:tpmhandle:C3CDD7AA hsmhandle:00000003
dnssec-signzone: debug 3: pkcs11: pkcs11_RSA_sign TimedSign C_Sign 1
C_Sign+748:
|> tpmtimedsign|
| checking expiration time 1373120022 < 1373123348 and algorithm 8|
| computing hash of 468 bytes:|
|***write|
|***read|
|tpm_sign: handle = C3CDD7AA|
|***write|
|***read|
|ok: signature|
| 69 35 47 56 E5 0E A6 B2 26 29 50 59 40 1C FD 4E |…
|DONE|
C_Sign+782:signature:
```

Cont…

```
dnssec-signzone: testzone/SOA:
dnssec-signzone:    signing with dnskey testzone/RSASHA256/58968
dnssec-signzone: testzone/NS:
dnssec-signzone:    signing with dnskey testzone/RSASHA256/58968
dnssec-signzone: www.testzone/NSEC:
dnssec-signzone:    signing with dnskey testzone/RSASHA256/58968
dnssec-signzone: www.testzone/A:
dnssec-signzone:    signing with dnskey testzone/RSASHA256/58968
Verifying the zone using the following algorithms: RSASHA256.
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 present, 0 revoked
testzone.signed
dnssec-signzone: debug 3: pkcs11: pkcs11_logout: C_Logout 1
C_Logout+1402:
C_CloseSession+1470:
|> tpmflush C3CDD7AA|
|***write|
|***read|
|> tpmreset|
|***write|
|***read|
C_CloseSession: done
dnssec-signzone: debug 3: pkcs11: pkcs11_logout: done
C_Finalize+1504
```

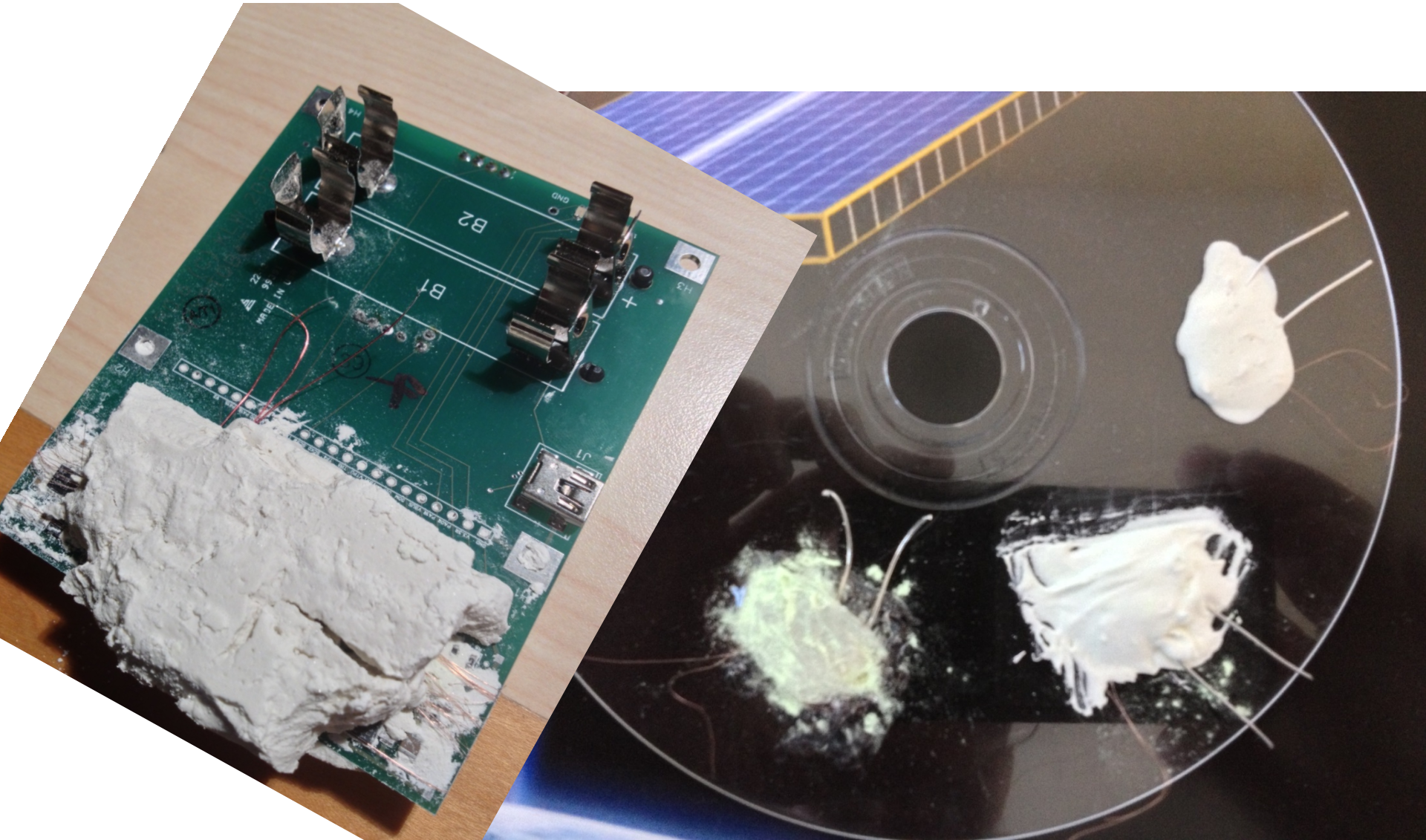
Cont…validity period too long

```
# bind-9.9.2-P2/bin/dnssec/dnssec-signzone -s now -e +3700 -v 5 -x -o testzone -k Ktestzone.+008+35407 testzone Ktestzone.+008+58968
dnssec-signzone: debug 3: pkcs11: pkcs11_login: start
dnssec-signzone: debug 3: pkcs11: pkcs11_initlib Start
C_GetFunctionList+1636:
C_Initialize+1519:
serial_init+1872:Openned /dev/ttyUSB0
|> v2on|
|TWI_ConfigureMaster()|
|Using CKDIV = 1 and CLDIV/CHDIV = 158 CWGR=00019E9E|
C_GetSlotList+1414:
C_OpenSession+1430:
dnssec-signzone: debug 3: pkcs11: C_Login 1
C_Login+1394:
dnssec-signzone: debug 3: pkcs11: pkcs11_parse Ktestzone.+008+35407
C_FindObjectsInit+816:
C_FindObjects+943:          MATCHED 00000002
C_FindObjectsFinal+844:
C_FindObjectsInit+816:
C_FindObjects+943:          MATCHED 00000003
C_FindObjectsFinal+844:
C_GetAttributeValue+1014:
C_GetAttributeValue+1014:
dnssec-signzone: testzone/NSEC:
dnssec-signzone:               signing with dnskey testzone/RSASHA256/58968
dnssec-signzone: testzone/DNSKEY:
dnssec-signzone:               signing with dnskey testzone/RSASHA256/35407
dnssec-signzone: debug 3: pkcs11: rick_thsm doing pkcs11_RSA_sign TIMED
C_SignInit+673:
writecryptolcmd: |tpmloadkey| 559
|> tpmloadkey|
|***write|
|***read|
|***write|
|***read|
|tpm_loadkey: handle = 1815518807  hex: 0x6C369E57|
|ok: key loaded handle=6C369E57|
```

Cont…

```
C_SignInit+728:|ok: key loaded handle=6C369E57|
C_SignInit+736:tpmhandle:6C369E57 hsmhandle:00000003
dnssec-signzone: debug 3: pkcs11: pkcs11_RSA_sign TimedSign C_Sign 1
C_Sign+748:
|> tpmtimedsign|
| checking expiration time 1373123496 < 1373123422 and algorithm 8|
|fail: RRSIG expiration time exceeds HSM policy|
C_Sign+782:signature:
dnssec-signzone: fatal: dnskey 'testzone/RSASHA256/35407' failed to sign data: ran out
of space
C_Finalize+1504:
C_CloseSession+1470:
|> tpmflush 6C369E57|
|***write|
|***read|
|> tpmreset|
|***write|
|***read|
C_CloseSession: done
```

I’ll have some ZnS with that please (gamma ray scintillation detector)



Thanks to Jakob Schlyter, Frederico Neves, Roy Arends, David Miller, and so many others