Festplattenverschlüsselung mit TPM 2.0

FrOSCon 2025

17. August 2025

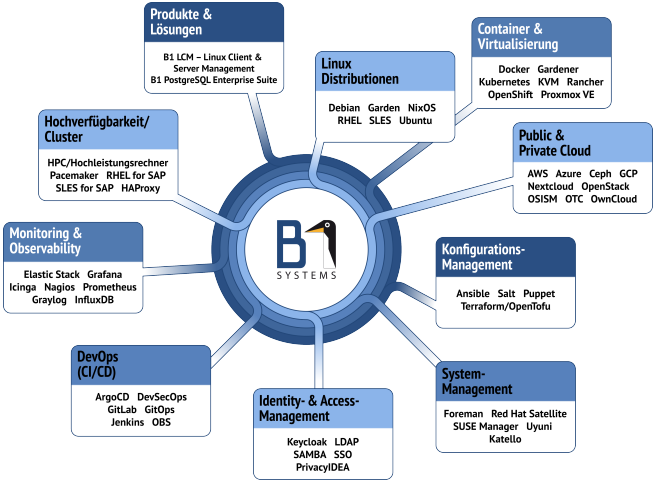
Susanne Schütze
Linux Consultant
B1 Systems GmbH
schuetze@b1-systems.de

Inhaltsverzeichnis

Vorstellung B1 Systems

- gegründet 2004
- spezialisiert auf Linux/Open Source-Themen
- national & international tätig
- ca. 150 Mitarbeiter:innen
- unabhängig von Soft- & Hardware-Herstellern
- Leistungsangebot:
  - Managed Service & Betrieb
  - Beratung & Consulting
  - Support
  - Training
  - Lösungen & Entwicklung
- Standorte in Rockolding, Köln, Berlin & Dresden

Schwerpunkte



whoami

- Susanne Schütze
- 41 Jahre
- Fachinformatikerin für Systemintegration
- bei B1 Systems GmbH seit Juli 2024
- berufliche Themen: Linux Client Management, Development, Ansible, Salt, etc.

Was ist der mysteriöse TPM?

- Abkürzung für „Trusted Platform Module“, spezifiziert von der Trusted Computing Group (TGC)
- herausragende Fähigkeit: mit Verschlüsselungskeys umgehen können und diese sicher speichern
- Möglichkeiten: Measured Boot über PCRs realisieren, Certificate Signing Requests, Random Number Generator, ...

TPM – ganz einfach?

kompliziert aufgebaut:

platform	System-Hersteller-Bereich
endorsement	TPM-Hersteller-Bereich und Privacy Owner, Sicherheitsbereich
storage	User-Bereich für Keys und Objekte
no hierachy / null	überlebt keinen Boot, berechnet Zufall, nur für temporäre Keys

Vorteile des TPM unter Linux

- der TPM kann nun auch unter Linux genutzt werden
- Festplatte kann mit dem TPM automatisch entschlüsselt werden
- TPM kann Passphrase für LUKS ersetzen
- Kernel, initrd und der Bootprozess können auf Änderungen überwacht werden
- Entschlüsselung kann gesperrt werden
- TPM ist unter Linux in aktiver Entwicklung

Spielwiese

- Ubuntu 24.04
- Virtuelle Maschine mit aktiviertem TPM 2.0
- benötigte TPM-Pakete:
  - `tpm2-tools`
  - `tpm2-abrmd`
  - `dracut`
- Root-Rechte
- bereits eingerichtete Festplatten-Verschlüsselung (zum Beispiel bei der Installation)

TPM-Erkennung überprüfen

Einhängepunkte für TPM 2.0:

`/dev/tpm0` TPM allgemein

`/dev/tpmrm0` Resource Manager, mit dem der Kernel mehrere User-Zugriffe auf den TPM steuert

TPM-Prüfung mit `systemd-cryptenroll`

```
# systemd-cryptenroll --tpm2-device=list
PATH        DEVICE      DRIVER
/dev/tpmrm0 MSFT0101:00 tpm_tis
```

LUKS-Header

Überblick LUKS-Header mit systemd-cryptenroll

```
# systemd-cryptenroll /dev/vda3
SLOT TYPE
   0 password
```

Überblick LUKS-Header mit cryptsetup (gekürzt)

```
# cryptsetup luksDump /dev/vda3
LUKS header information
...
Keyslots:
  0: luks2
        Key:        512 bits
        Priority:   normal
        Cipher:     aes-xts-plain64
        Cipher key: 512 bits
        PBKDF:      argon2id
        Memory:     82040
        Salt:       9a 9f b7 e2
...
```

Entschlüsselung an den TPM binden

LUKS-Key an TPM binden

```
1 # systemd-cryptenroll --tpm2-device=auto /dev/vda3
2 Please enter current passphrase for disk /dev/vda3: ••••
3 New TPM2 token enrolled as key slot 1.
```

LUKS-Key an TPM binden mit TPM-Pin

```
1 # systemd-cryptenroll --tpm2-device=auto --tpm2-with-pin=yes /dev/vda3
2 Please enter current passphrase for disk /dev/vda3: ••••
3 New TPM2 token enrolled as key slot 1.
```

Überflüssiger Slot?

Eine Gute Idee? – Löschen des überflüssigen Slots

```
# systemd-cryptenroll --wipe-slot=0 /dev/vda3
```

A Generell keine Gute Idee, da Updates dafür sorgen können, dass der TPM die Festplatte nicht mehr entschlüssen will ✓ Hängt mit PCRs zusammen.

B Zu diesem Zeitpunkt keine gute Idee, die Konfiguration der Crypttab fehlt ✓

C Slot 0 enthält das Passwort, das wird nicht mehr gebraucht. Reboot und fertig :) X so kann keiner mehr die Festplatte entschlüsseln

D Zu diesem Zeitpunkt keine gute Idee, die Konfiguration der Initramfs-Module fehlt. ✓

E Zu diesem Zeitpunkt keine gute Idee, die Konfiguration der Kernel-Commandline fehlt. ✓

Spaß mit der Crypttab – systemd-Version 255

/etc/crypttab

```
#dm_crypt-0 UUID=ede52a15-f515-4fed-838d-5433999f3f24 none luks
```

A Was auskommentiert ist, kann weggelassen werden (leere Datei). X

B Die Datei ist unnötig und wird nicht gebraucht. X

C Es genügt das Kommentarzeichen am Anfang der Zeile. ✓

D In der Datei fehlen die TPM-Optionen. X

Konfiguration /etc/crypttab

systemd-Version < 255

```
#
```

systemd-Version > 256

```
dm_crypt-0 UUID=ede52a15-f515-4fed-838d-5433999f3f24 none
↪  discard,tpm2-device=auto,tpm2-pin=yes
```

initramfs modifizieren mit dracut

Datei /etc/dracut.conf.d/tpm2-tss.conf anlegen

```
add_dracutmodules+=" tpm2-tss crypt "
```

Leerzeichen nach und vor den Anführungsstrichen vergessen?:

Fehler in der Dracut-Konfiguration

```
1 # dracut -f
2 /etc/dracut.conf.d/tpm2.conf:add_dracutmodules+="tpm2-tss crypt "
3
4 dracut[W]: <key>+=" <values> ": <values> should have surrounding white
  ↪  spaces!
5 dracut[W]: This will lead to unwanted side effects! Please fix the
  ↪  configuration file.
```

ab dracut-Version 103-3

initramfs modifizieren mit initramfs-Tools

/etc/initramfs-tools/modules erweitern

```
1 rng_core
2 tpm
3 tpm_tis_core
4 tpm_tis
```

initramfs neu bauen

```
# update-initramfs -u
```

Kernel-Optionen in Grub

Datei `/etc/default/grub`: `GRUB_CMDLINE` anpassen

nur TPM:

```
GRUB_CMDLINE_LINUX="rd.auto rd.luks=1
↪ rd.luks.options=tpm2-device=auto"
```

TPM mit PIN:

```
GRUB_CMDLINE_LINUX="rd.auto rd.luks=1
↪ rd.luks.options=tpm2-device=auto,tpm2-pin=yes"
```

Update Grub

```
1 # update-grub # Debian
2 # grub2-mkconfig -o /boot/grub2/grub.cfg # Fedora
```

TPM und PCR

cryptsetup luksDump 1

```
# cryptsetup luksDump /dev/vda3
...
Keyslots:
  0: luks2
    Key:        512 bits
    Priority:   normal
    Cipher:     aes-xts-plain64
    Cipher key: 512 bits
    PBKDF:      argon2id
...
  1: luks2
    Key:        512 bits
     ...
```

cryptsetup luksDump 2

```
Tokens:
  0: systemd-tpm2
    tpm2-hash-pcrs:   7
    tpm2-pcr-bank:    sha256
    tpm2-pubkey: (null)
    tpm2-pubkey-pcrs:
    tpm2-primary-alg: ecc
...
    tpm2-policy-hash:
...
    tpm2-pin:         false
    tpm2-pcrlock:     false
    tpm2-salt:        false
    tpm2-srk:         true
    Keyslot:    3
```

Was sind PCRs?

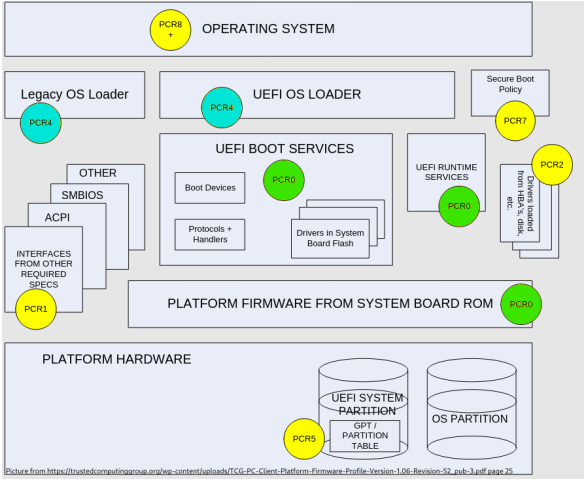
- PCR steht für *Platform Configuration Register*
- Ablage für gehashte Werte in SHA1 oder SHA256
- Werte beziehen sich zum Beispiel auf secure-boot-policy, kernel-initrd, kernel-boot, kernel-config, ...
- Integrität überprüfen

PCR – Übersicht

PCR Ausgabe

```
# systemd-analyze pcrs
NR NAME                SHA256
 0 platform-code       8612f3867faeb0fdadcdad675d95202ba256d1be3aeddc
 1 platform-config     a7eac3ef0871d29a2fb02312786d17f73ef743eb790035
 2 external-code       f1fa93cc54736b2e79a00f4d0ba566abb5d08dff9de70d
 3 external-config     3d458cfe55cc03ea1f443f1562beec8df51c75e14a9fcf
 4 boot-loader-code    30e68a8980f5cbd2cdb82dd5cdd46bae6cc90188dac07d
 5 boot-loader-config  28ff65fd8161c8ab7e909591816be3de4c07ef5af06ed8
 6 host-platform       3d458cfe55cc03ea1f443f1562beec8df51c75e14a9fcf
 7 secure-boot-policy  6dc6aeabe4d8207dad5a99dea56dc1ba5fca17a678c73a
 8 -                   016a167e0c5690c26b4d3c33f8a4fad08655e42b7c11c0
 9 kernel-initrd       516a9ca2c7f7b4786cb800c692caa137471a5809f58eed
10 ima                 9592ad63436356ecafe2c10fadccd4bc51a77b50e69194
11 kernel-boot         0000000000000000000000000000000000000000000000
...
14 shim-policy         306f9d8b94f17d93dc6e7cf8f5c79d652eb4c6c4d13de2
```

PCRs im UEFI Mapping



PCR-Slots und ihre Bedeutung 1/3

PCR	manpage-name	Used by	Measured Objects	changed by
0	platform-code	UEFI-boot	SRTM, BIOS, Host Platform Extensions, Embedded Option ROMs and PI Drivers	firmware updates
1	platform-config	UEFI-boot	Core system firmware data/host platform configuration; typically contains serial and model numbers	basic hardware/ CPU/ RAM replacements
2	external-code	UEFI-boot	UEFI driver, application Code	pluggable hardware
3	external-config	UEFI-boot	UEFI driver, application Configuration, Data	pluggable hardware
4	boot-loader-code	UEFI-boot/ Bootloader	UEFI Boot Manager Code (usually the MBR) and Boot Attempts	bootloader updates
5	boot-loader-config	UEFI-boot/ Bootloader	Boot Manager Code Configuration, Data (for use by the Boot Manager Code), GPT/Partition Table	GPT/Partition Table updates

PCR-Slots und ihre Bedeutung 2/3

PCR	manpage-name	Used by	Measured Objects	changed by
6			Host Platform Manufacturer Specific	
7	secure-boot-policy	UEFI-boot	SecureBoot state	Secure-Boot, - Certificates updates
8	grub	UEFI-boot/ Bootloader	Commands and kernel command line	Kernel commandline
9	kernel-initrd	grub/Kernel	All files in initrd (including kernel image)	changes or updates initrd-file
10	ima	IMA	Integrity Measurement Architecture of the Linux Kernel & runtime state of IMA Project	IMA runtime state
11	kernel-boot	systemd-stub/ systemd-pcrphase	All components of unified kernel images (UKIs), Boot phase strings	UKI image changes and boot-process

PCR-Slots und ihre Bedeutung 3/3

PCR	manpage-name	Used by	Measured Objects	changed by
12	kernel-config	systemd-stub	Kernel command line, system credentials, system configuration images	Kernelcommands, system-credentials, system configuration
13	sysexts	systemd-stub	All system extension images for the initrd	initrd system extension updates
14	shim-policy	shim	"MOK" certificates and hashes	Secure-Boot-Certificates updates
15	system-identity	systemd-cryptsetup-@.service/ systemd-pcrmachine.-service/ systemd-pcrfs@.service	Root file system volume encryption key/ Machine ID/ File system mount point, UUID, label, partition UUID label of root file system and /var/	LUKS key changes/ machine-id/ file system and mountpoint updates
16	debug			
23	application-support			

Updates und PCRs?

User 1:

Hilfe ich kann meine Festplatte nicht mehr entschlüsseln.

User 2:

same, same

User 3:

Was bedeute die Fehlermeldung:

```
1 Please Enter Passphrase for Disk
2 *****
3 Please Enter Passphrase for Disk
4 *****
5 [FAILED] Failed to start Cryptography Setup for Disk
6 [DEPEND] Dependency failed for Local Encrypted Volumes
```

Ursache: Das Paket `shim-signed` wurde upgedated; Folge: anderer Hash in PCR 7.

Lösungen für verwendete PCRs 1/3

Hashsumme im PCR 7 updaten

```
# systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=7 --wipe-slot=2
↪  /dev/vda3
```

Keine PCRs verwenden

```
# systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs='' --wipe-slot=2
↪  /dev/vda3
```

Lösungen für verwendete PCRs 2/3

Andere PCRs verwenden

```
# systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=17,18
↪  --wipe-slot=2 /dev/vda3
```

Keine PCRs verwenden und stattdessen eine TPM-Pin

```
# systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=''
↪  --tpm2-with-pin=yes --wipe-slot=2 /dev/vda3
```

Lösungen für verwendete PCRs 3/3

Zusätzlichen Recovery-Key verwenden

```
# systemd-cryptenroll --recovery-key /dev/vda3
```

Zusätzlich Passwörter zum Entschlüsseln verwenden

```
# systemd-cryptenroll --password /dev/vda3
```

Wenn's dem TPM zu viel wird ...

Anfragen an den TPM können als *Dictionary Attack* gewertet werden. Zur Verhinderung wird `da-lockout` genutzt, das den Zugriff auf den TPM sperrt.

Lockout-Mode-Erkennung

```
# tpm2 getcap properties-variables
TPM2_PT_PERMANENT:
  ownerAuthSet:              0
  endorsementAuthSet:        0
  lockoutAuthSet:            0
...
  inLockout:                 1
  tpmGeneratedEPS:           1
...
TPM2_PT_LOCKOUT_COUNTER: 0x0
TPM2_PT_MAX_AUTH_FAIL: 0x3
TPM2_PT_LOCKOUT_INTERVAL: 0x3E8
TPM2_PT_LOCKOUT_RECOVERY: 0x3E8
...
```

da-lockout aufheben

da-lockout aufheben

```
# tpm2_dictionarylockout --clear-lockout
```

da-lockout Authentifizierungsversuche erhöhen

```
# tpm2_dictionarylockout --setup-parameters --max-tries=5
```

Den gesamten TPM beim nächsten Systemstart zurücksetzen

```
# echo 5 > /sys/class/tpm/tpm0/ppi/request
```

Auszug aus Manpage zu systemd-cryptenroll

man systemd-cryptenroll

```
...
CREDENTIALS
   systemd-cryptenroll supports the service credentials logic as implemented by
   ↪  ImportCredential=/LoadCredential=/SetCredential= (see systemd.exec(5) for details).
   ↪  The following credentials are used when passed in:

   cryptenroll.passphrase, cryptenroll.new-passphrase
    May contain the passphrase to unlock the volume with/to newly enroll.
   Added in version 256.

   cryptenroll.tpm2-pin, cryptenroll.new-tpm2-pin
    May contain the TPM2 PIN to unlock the volume with/to newly enroll.
   Added in version 256.
...
```

Welcher Befehlstyp verbirgt sich hinter `cryptenroll.tpm2-pin`?

A eine Variable X

B Ersatz für die Umgebungsvariable `TPM2-PIN` ✓

C systemd-Direktive X

D eine Variable von `systemd-creds` X

E ein Credential, das innerhalb einer systemd-Unit verwendet werden kann ✓

Was ist systemd-creds?

man systemd-creds

```
DESCRIPTION
   systemd-creds is a tool for
   ↪ listing, showing, encrypting and decrypting unit credentials.
   ↪ Credentials are limited-size binary or textual objects that may be
   ↪ passed to unit processes. They are primarily used for passing
   ↪ cryptographic keys (both public and private) or certificates, user
   ↪ account information or identity information from the host to
   ↪ services.

   Credentials are configured in unit files via the ImportCredential=,
   ↪ LoadCredential=, SetCredential=, LoadCredentialEncrypted=, and
   ↪ SetCredentialEncrypted= settings, see systemd.exec(5) for details.
```

Optionen sind `list`, `cat`, `encrypt`, `decrypt`, `user`, `system`

Was macht die Option `list` bei `systemd-creds`?

A listet alle bekannten Credentials auf X

B listet alle Dateien des Verzeichnisses der Umgebungsvariable `$CREDENTIALS_DIRECTORY` auf ✓

C gibt die Stärke der vorhandenen Credentials aus X

D gibt die Sicherheitsstärke der vorhandenen Credential-Dateien je nach Speicherort aus ✓

E macht nichts, weil `$CREDENTIALS_DIRECTORY` nicht gesetzt ist ✓

Was macht die Option `list` bei `systemd-creds`? – Demo

DEMO

Was macht die Option `list` bei `systemd-creds`? – Manpage

Option `list` aus der `systemd-creds` Manpage

```
list
    Show a list of credentials passed into the current execution context.
        This command shows the files in the directory referenced by the
    ↪   $CREDENTIALS_DIRECTORY environment variable, and is
    ↪   intended to be executed from within service context.
    Along with each credential name, the size and security state is shown.
        The latter is one of "secure" (in case the credential is backed
    ↪   by unswappable memory, i.e. "ramfs"), "weak" (in case it is
    ↪   backed by any other type of memory), or "insecure" (if having
    ↪   any access mode that is not 0400, i.e. if readable by anyone but
    ↪   the owner).
    Added in version 250.
```

Wie funktioniert `systemd-creds` mit `systemd-cryptenroll`?

- es ist keine Dokumentation zu finden
- es sind kein Beispiel zu finden
- systemd-Repo auf GitHub
  - Tests durchgesehen
  - Pull-Request durchsucht

Eine vage Idee

Test aus #31370 PR (unvollständig)

```
#Add PIN to TPM2 enrollment
NEWPIN=1234 systemd-cryptenroll --unlock-tpm2-device=auto --tpm2-device=auto
  ↪  --tpm2-with-pin=yes "$IMAGE"

#Add PIN to TPM2 enrollment, through systemd-creds
systemd-run -p SetCredential=TPM2_PIN:4321 -p DynamicUser=1 -E PIN=1234
  ↪  --unit=testsuite-70-cryptenroll-creds.service --wait systemd-cryptenroll
  ↪  --unlock-tpm2-device=auto --tpm2-device=auto --tpm2-with-pin=yes
  ↪  "$IMAGE"
```

Eine vage Idee, die nicht funktioniert

Aber ...

- PR wurde geschlossen, weil schon implementiert über `systemd-ask-password-agent`
- im restlichen Code kein Test, der das Verhalten prüft
- im Code von `systemd-cryptenroll` ist ersichtlich, dass `systemd-ask-password` genutzt wird (in C geschrieben)

Auszug Manpage systemd-ask-password

```
systemd-ask-password
  --credential=
      Configure a credential to read the password from - if it exists.
          This may be used in conjunction with the ImportCredential=,
      ↪   LoadCredential= and SetCredential= settings in unit files. See
      ↪   systemd.exec(5) for details. If not specified, defaults to
      ↪   "password". This option has no effect if no credentials
      ↪   directory is passed to the program (i.e. $CREDENTIALS_DIRECTORY
      ↪   is not set) or if the no credential of the specified name exists.
          Added in version 249.
```

systemd-ask-password hilft, das Credential beim User abzufragen, aber damit kann es nicht an systemd-cryptenroll übergeben werden

systemd-cred im Zusammenhang mit TPM – Fehler

Dateiname und Credential-Name müssen gleich sein – aber keine Fehlermeldung

```
$ echo -n test | systemd-creds encrypt --name=cryptenroll.passphrase -
↪ luks.pass.cred
```

Versuch, die Systemd-Creds mit der Unit zusammen zu nutzen

```
1 # systemd-run -p
  ↪ LoadCredential=cryptenroll.passphrase:/root/cryptenroll.passphrase
  ↪ -p SetCredential=cryptenroll.new-tpm2-pin:4321
  ↪ --unit=systemd-cryptsetup@root.service --wait systemd-cryptenroll
  ↪ --tpm2-device=auto --tpm2-with-pin=yes /dev/vda3
2 # systemd-cryptsetup@root.service: Failed to set up credentials:
  ↪ Protocol error
```

systemd-creds in Zusammenhang mit TPM

systemd-creds init und encrypt sowie decrypt

```
1 $ systemd-creds setup
2 $ echo -n GPN23 | systemd-creds --system encrypt
  ↪  --name=cryptsetup.tpm2-pin - cryptsetup.tpm2-pin
3 $ systemd-creds decrypt --name=cryptsetup.tpm2-pin --system
  ↪  cryptsetup.tpm2-pin
```

Setzt mit systemd-creds definierte Passphrase

```
# systemd-run -p SetCredential=cryptenroll.passphrase:test -p
  ↪  SetCredential=cryptenroll.new-tpm2-pin:4321 systemd-cryptenroll
  ↪  --tpm2-device=auto --tpm2-with-pin=yes /dev/vda3
```

Konfigurationsfehler?

Kernel kennt die TPM-Einstellungen nicht

```
localhost kernel: Unknown kernel command line parameters "splash
↪ BOOT_IMAGE=/vmlinuz-6.8.0-49-generic tpm2-pin=yes", will be passed
↪ to user space.
```

X

User tss ist nicht bekannt

```
localhost systemd-udevd[278]:
↪ /usr/lib/udev/rules.d/60-tpm-udev.rules:3 Unknown user 'tss',
↪ ignoring.
```

X Ubuntu24.04

Konfigurationsfehler?

Kein Unified Kernel Image verwendet

```
systemd[1]: systemd-tpm2-setup-early.service - TPM2 SRK Setup (Early)
↪  was skipped because of an unmet condition check
↪  (ConditionSecurity=measured-uki).
```

X

Konfigurationsfehler?

```
1 systemd-cryptsetup[513]: WARNING:esys:src/tss2-esys/api/Esys_StartAuthSession.c:391
  ↪  :Esys_StartAuthSession_Finish() Received TPM Error
2 systemd-cryptsetup[513]: ERROR:esys:src/tss2-esys/api/Esys_StartAuthSession.c:136:E
  ↪  sys_StartAuthSession() Esys Finish ErrorCode (0x0000098e)
3 systemd-cryptsetup[513]: Failed to unseal secret using TPM2: State not recoverable
4 systemd-cryptsetup[513]: Set cipher aes, mode xts-plain64, key size 512 bits for
  ↪  device /dev/disk/by-uuid/6b563880-9b80-4b25-a317-267617bbd26c.
5 systemd-cryptsetup[513]: WARNING:esys:src/tss2-esys/api/Esys_StartAuthSession.c:391
  ↪  :Esys_StartAuthSession_Finish() Received TPM Error
6 systemd-cryptsetup[513]: ERROR:esys:src/tss2-esys/api/Esys_StartAuthSession.c:136:E
  ↪  sys_StartAuthSession() Esys Finish ErrorCode (0x0000098e)
7 systemd-cryptsetup[513]: Failed to unseal secret using TPM2: State not recoverable
8 systemd-cryptsetup[513]: TPM2 operation failed, falling back to traditional
  ↪  unlocking: State not recoverable
```

✓

TPM-Fehlercodes entschlüsseln

Was bedeutet der Fehlercode `0x0000098e`?

A authorization HMAC failed ✓

B BlueScreen of Death X

C steht in der Manpage unter Exit Codes X

D Fehler auf Layer 8 (falsche TPM-PIN eingegeben) ✓

E kann mit `tpm2_rc_decode` entschlüsselt werden ✓

TPM-Fehlercodes entschlüsseln

Fehlercodes 0x0000098e sind sehr verständlich für Menschen ;)

Übersetzung der TPM-Fehlercodes

```
# tpm2_rc_decode 0x0000098e
tpm:session(1):the authorization HMAC check failed and DA counter
  ↪  incremented
```

Dieser Fehlercode wird auch angezeigt, wenn die PIN falsch eingegeben wurde.

Welche Unterschiede bezüglich des TPMs gibt es bei Distributionen?

- es gibt unterschiedliche Tools zum Erstellen des initramfs
  - Dracut
  - Initramfstools
- es werden unterschiedliche Versionen von systemd eingesetzt
- es werden verschiedene Bootloader verwendet
- es werden unterschiedliche TPM-Bibliotheken eingesetzt

  `ibmtss2` IBM

  `tpm2-tss` Intel

Nachteile des TPM in Bezug auf `systemd-cryptenroll`

- LUKS-Header müssen zum Bearbeiten mit Passphrase entschlüsselt werden; zukünftig geht auch `systemd-cryptenroll --unlock-tpm2-device=auto ...`
- wenn eine Entschlüsselungs-Option nicht funktioniert, wird nicht automatisch auf die nächste gewechselt (bis systemd Version: 255)
- PCR Measurements sind zur Zeit noch nicht Update-sicher
- mehrere Versuche, die TPM-PIN einzugeben nur, wenn `tpm2-measure-pcr=yes` in `crypttab` gesetzt sind
- Debugging:
  - TPM-Fehlercodes müssen erst übersetzt werden
  - fehlerhafte PIN-Eingabe ist nicht erkennbar

Vielen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen wenden Sie sich bitte an info@b1-systems.de oder +49 (0)8457 - 931096