Benutzer: mustermann

Passwort: ●●●●●●●●●●

Schlüssel: ●●●●●●●●●●●●●●●

Anmelden   Zurücksetzen

Bitte geben Sie Benutzername und Passwort ein.

Tastendruck erzeugt
einmaligen Schlüssel

Picosafe ®
SmartKey

Zähler Datenblock Echtzeit Uhr

counter datablock timestamp

AES Decyrption

AES Verschlüsselung

Start

loads bootloader

Crypted
Bootloader
from sd card

decrypt bootloader

AES key
from otp
storage
(locked
by fused)

Secure AES ROM

decryption
successful

no → hang

yes

run bootloader

Load kernel
from sd card
and decrypt

crypt
Rootfs
from sd
card

boot kernel

Mount root filesystem

System start

key or file

LUKS rootFS
Container

Encrypted or Signed
Kernel + Initrd

AES Encrypted
Secure APEX Bootloader

Boot
from
sd card

ARM9
with
Decryption Engine

Secure ROM for AES Key

Load kernel and signature
and verify signature

SSH

https://

File Storage	SSH-Server	Picosafe Console Web Application
		Webserver
Debian 6.0		
GNU/Linux Kernel		
APEX Bootloader		
ARM9 with Decryption Engine		