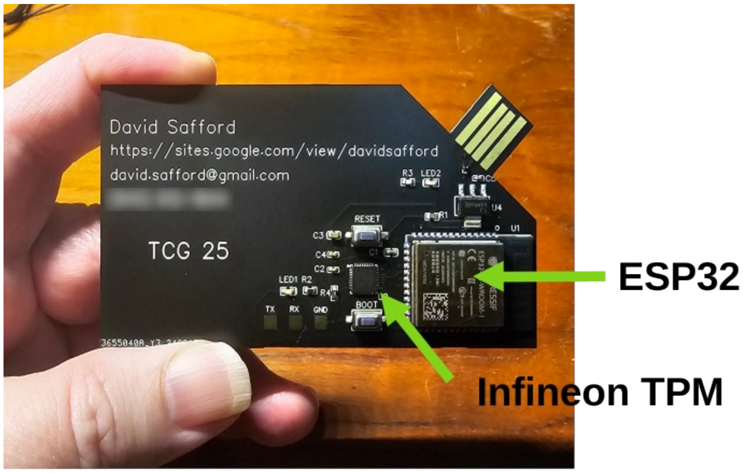
DEMONSTRATION
OVERVIEW

TRUSTED® COMPUTING GROUP

A Trusted Business Card:
Demonstrating Supply Chain Defenses

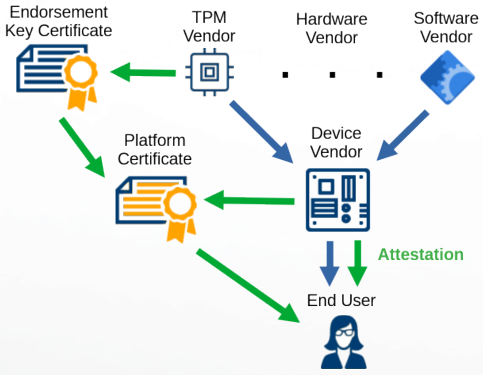


How do you know if your device is authentic and untampered?

This is a fun and fast demonstration of how TCG standards can be used for supply chain defense.

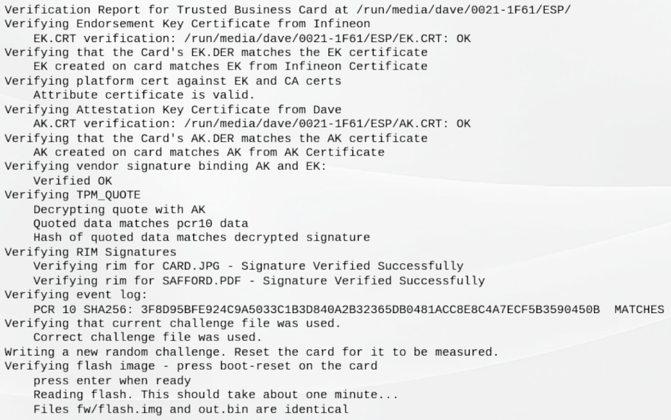
Cards will be given away to the first twenty attendees who ask.

Supply Chain Defense with TPM



The end user can verify:
Authenticity of TPM
Authenticity of device
Authenticity of firmware

Demonstration



```
Verification Report for Trusted Business Card at /run/media/dave/0021-1F61/ESP/
Verifying Endorsement Key Certificate from Infineon
    EK.CRT verification: /run/media/dave/0021-1F61/ESP/EK.CRT: OK
Verifying that the Card's EK.DER matches the EK certificate
    EK created on card matches EK from Infineon Certificate
Verifying platform cert against EK and CA certs
    Attribute certificate is valid.
Verifying Attestation Key Certificate from Dave
    AK.CRT verification: /run/media/dave/0021-1F61/ESP/AK.CRT: OK
Verifying that the Card's AK.DER matches the AK certificate
    AK created on card matches AK from AK Certificate
Verifying vendor signature binding AK and EK:
    Verified OK
Verifying TPM_QUOTE
    Decrypting quote with AK
    Quoted data matches pcr10 data
    Hash of quoted data matches decrypted signature
Verifying RIM Signatures
    Verifying rim for CARD.JPG - Signature Verified Successfully
    Verifying rim for SAFFORD.PDF - Signature Verified Successfully
Verifying event log:
    PCR 10 SHA256: 3F8D95BFE924C9A5033C1B3D840A2B32365DB0481ACC8E8C4A7ECF5B3590450B  MATCHES
Verifying that current challenge file was used.
    Correct challenge file was used.
Writing a new random challenge. Reset the card for it to be measured.
Verifying flash image - press boot-reset on the card
    press enter when ready
    Reading flash. This should take about one minute...
    Files fw/flash.img and out.bin are identical
```

This is an open source, open hardware project, with all details at: github.com/safforddr/tbc