

OpenCore Sammelthread (Hilfe und Diskussion)

Beitrag von „anonymous_writer“ vom 29. Februar 2020, 14:19

Du hast die Doku und die Sample.plist zu OC ignoriert.

6. Vault

Type: plist string

Failsafe: Secure

Description: Enables vaulting mechanism in OpenCore.

Valid values:

- **Optional** — require nothing, no vault is enforced, insecure.
- **Basic** — require `vault.plist` file present in OC directory. This provides basic filesystem integrity verification and may protect from unintentional filesystem corruption.
- **Secure** — require `vault.sig` signature file for `vault.plist` in OC directory. This includes **Basic** integrity checking but also attempts to build a trusted bootchain.

`vault.plist` file should contain SHA-256 hashes for all files used by OpenCore. Presence of this file is highly recommended to ensure that unintentional file modifications (including filesystem corruption) do not happen unnoticed. To create this file automatically use `create_vault.sh` script. Regardless of the underlying filesystem, path name and case must match between `config.plist` and `vault.plist`.

`vault.sig` file should contain a raw 256 byte RSA-2048 signature from SHA-256 hash of `vault.plist`. The signature is verified against the public key embedded into `OpenCore.efi`. To embed the public key you should do either of the following:

- Provide public key during the `OpenCore.efi` compilation in `OpenCoreVault.c` file.
- Binary patch `OpenCore.efi` replacing zeroes with the public key between `=BEGIN OC VAULT=` and `==END OC VAULT==` ASCII markers.

RSA public key 520 byte format description can be found in Chromium OS documentation. To convert public key from X.509 certificate or from PEM file use `RsaTool`.

The complete set of commands to:

- Create `vault.plist`.
- Create a new RSA key (always do this to avoid loading old configuration).
- Embed RSA key into `OpenCore.efi`.
- Create `vault.sig`.

Can look as follows:

Optional wäre hier richtig.