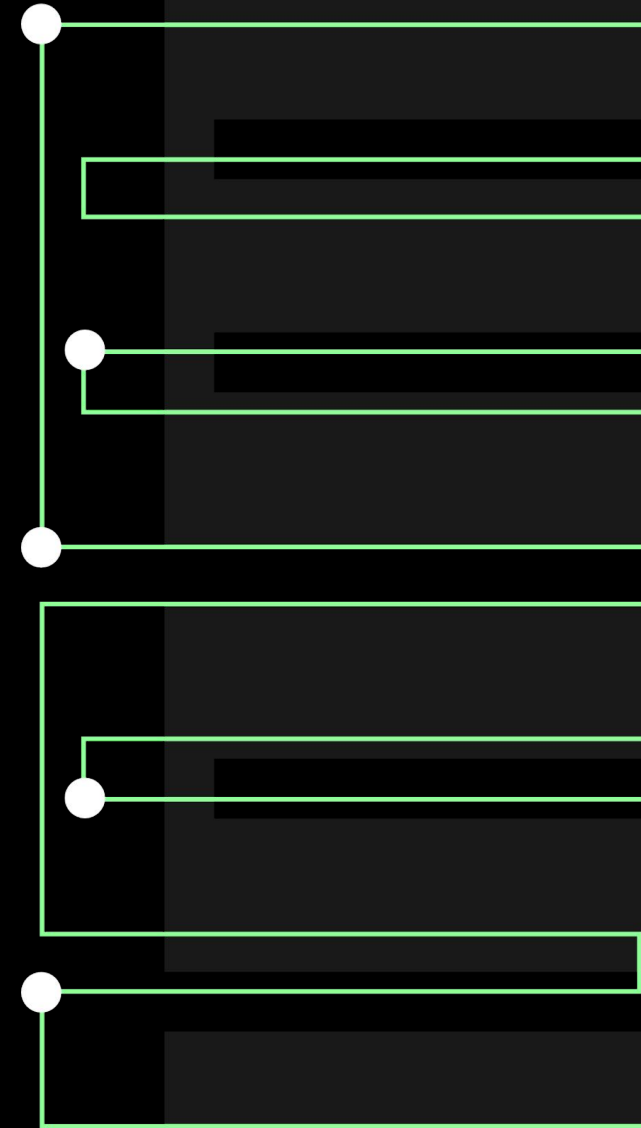
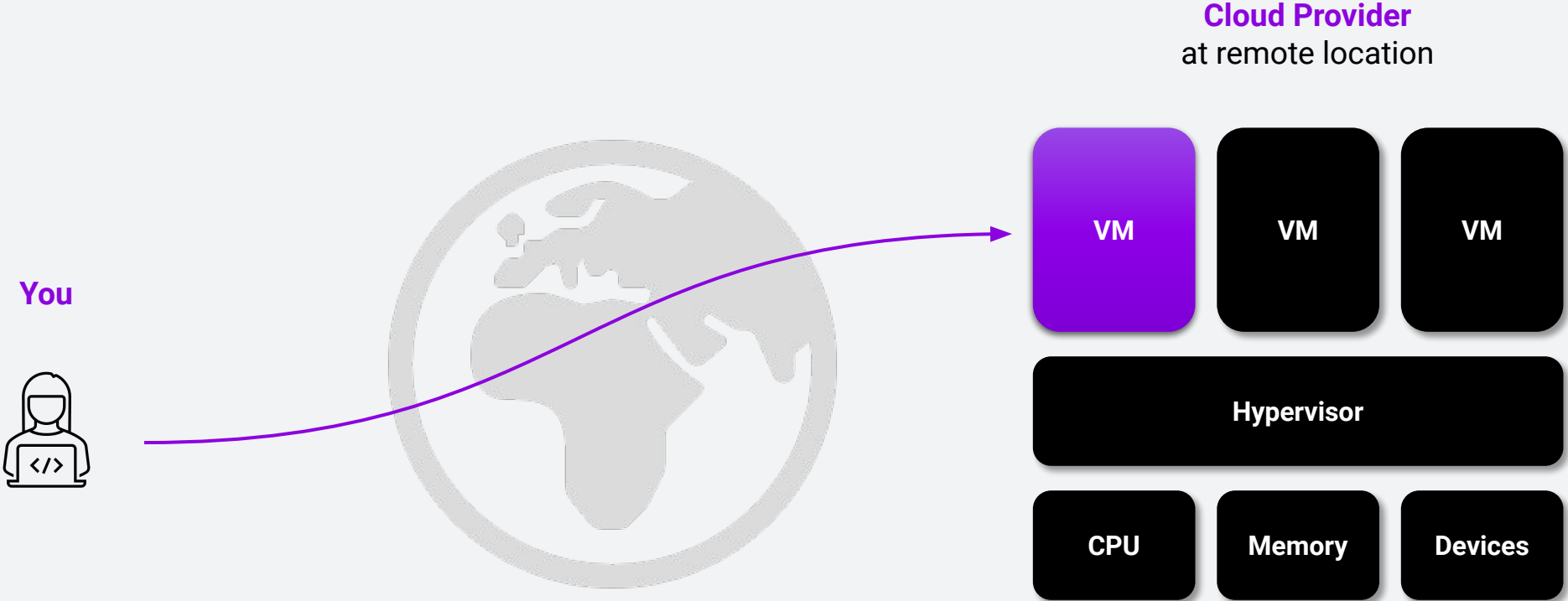


# Wrapping entire Kubernetes clusters into a confidential-computing envelope with Constellation

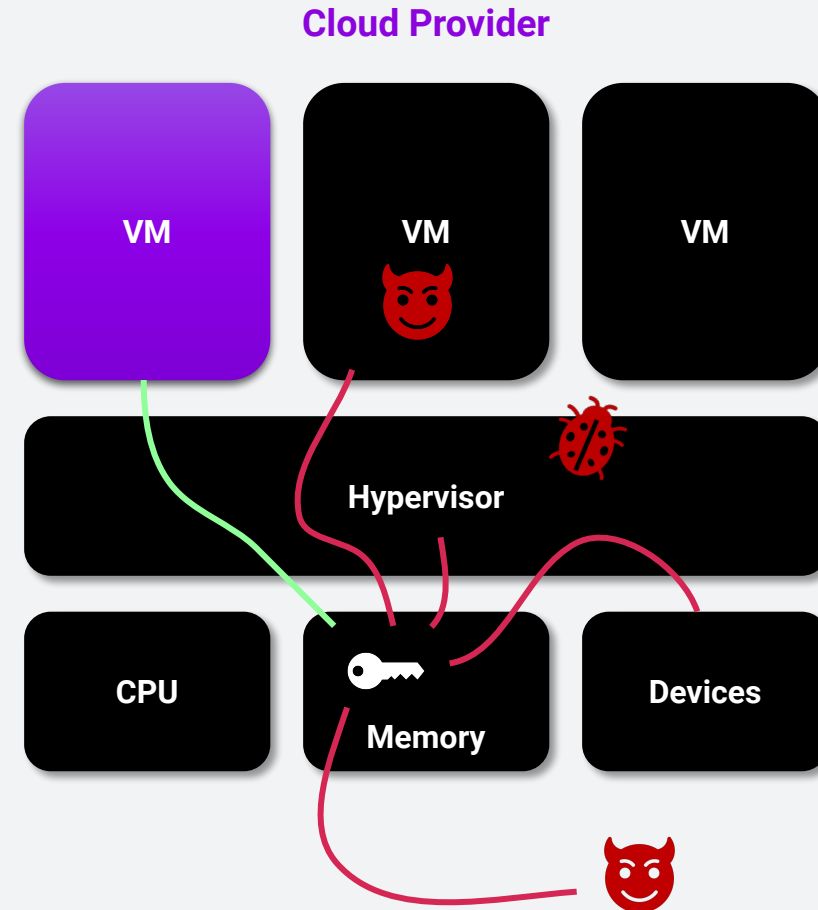


# What does cloud even mean?



# Threats

- Data in memory is plaintext
  - Physical access to memory
  - Insider attacks
  - Compromised cloud provider
  - Cross-tenants attacks

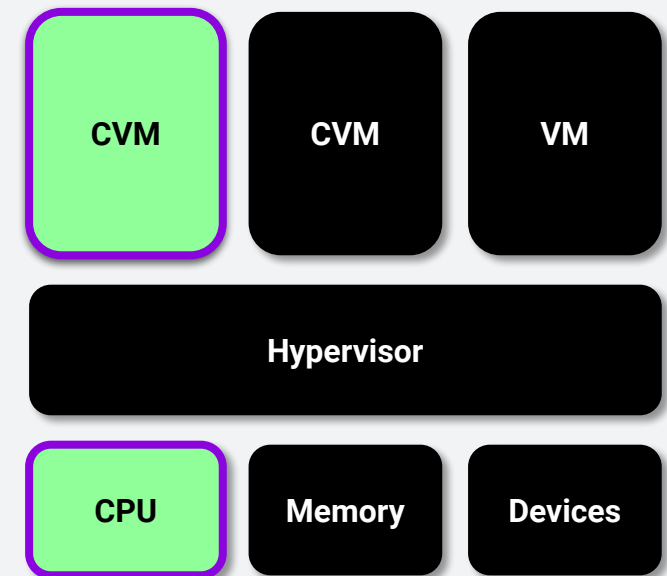


# Confidential Computing to the rescue!

- Hardware-based Trusted Execution Environment (TEE)
- Protects data confidentiality and integrity **in use**
- Protects code integrity **in use**
- Based on memory encryption

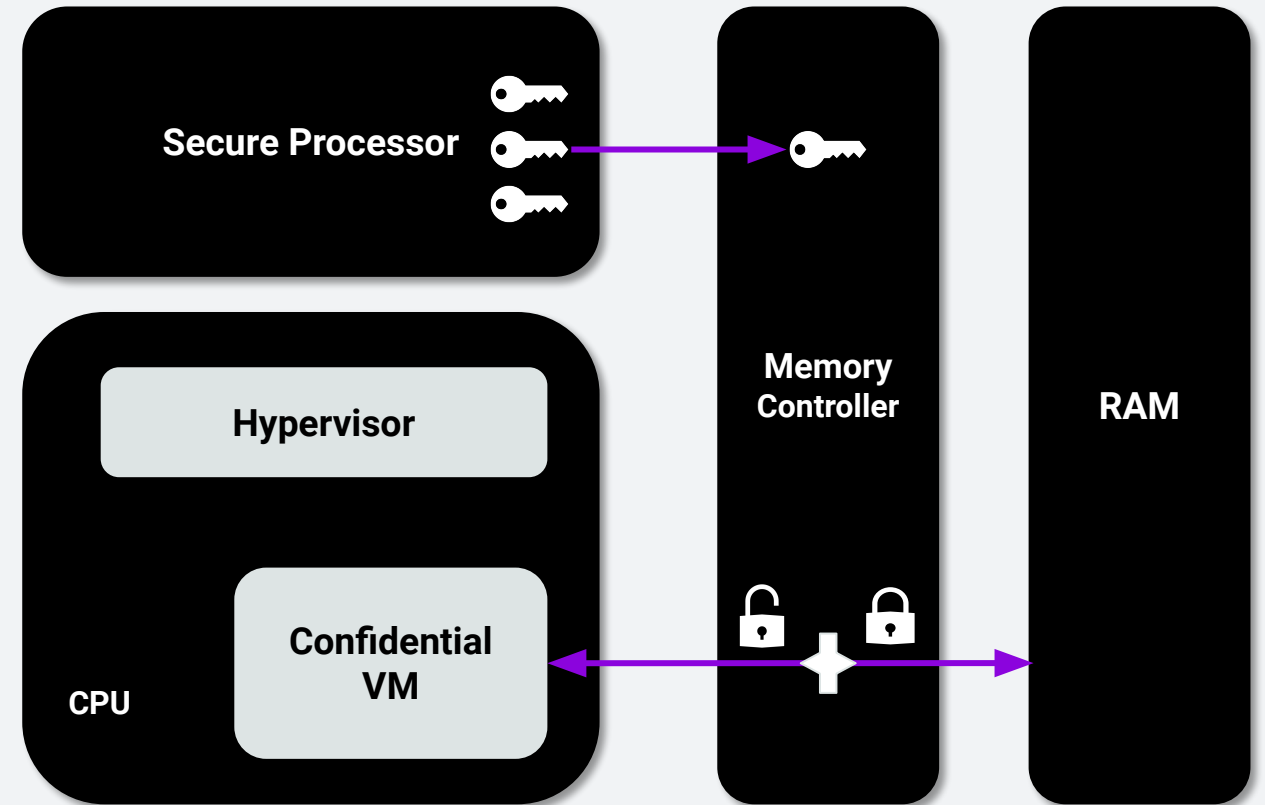
# AMD Secure Encrypted Virtualization (SEV)

- Confidential Virtual Machine (CVM)
- CVM and CPU in Trusted Computing Base (TCB)
- Transparent encryption of memory per CVM



# AMD SEV: Memory encryption

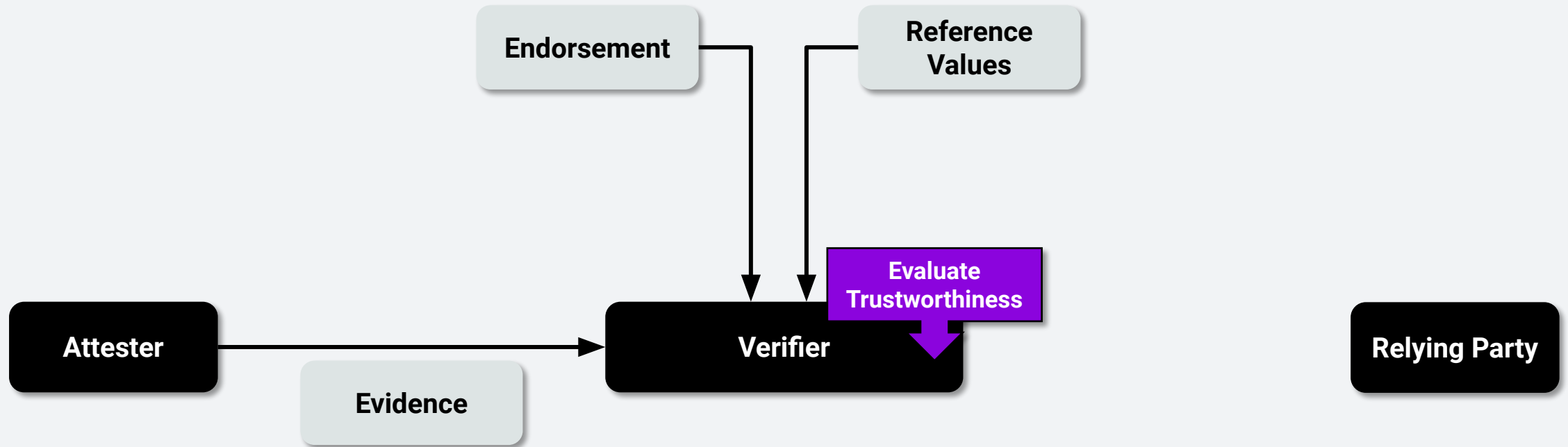
- Separate key per CVM
- Inaccessible by software
- Pages AES encrypted in RAM
- Tracking page ownership



# Problem solved?

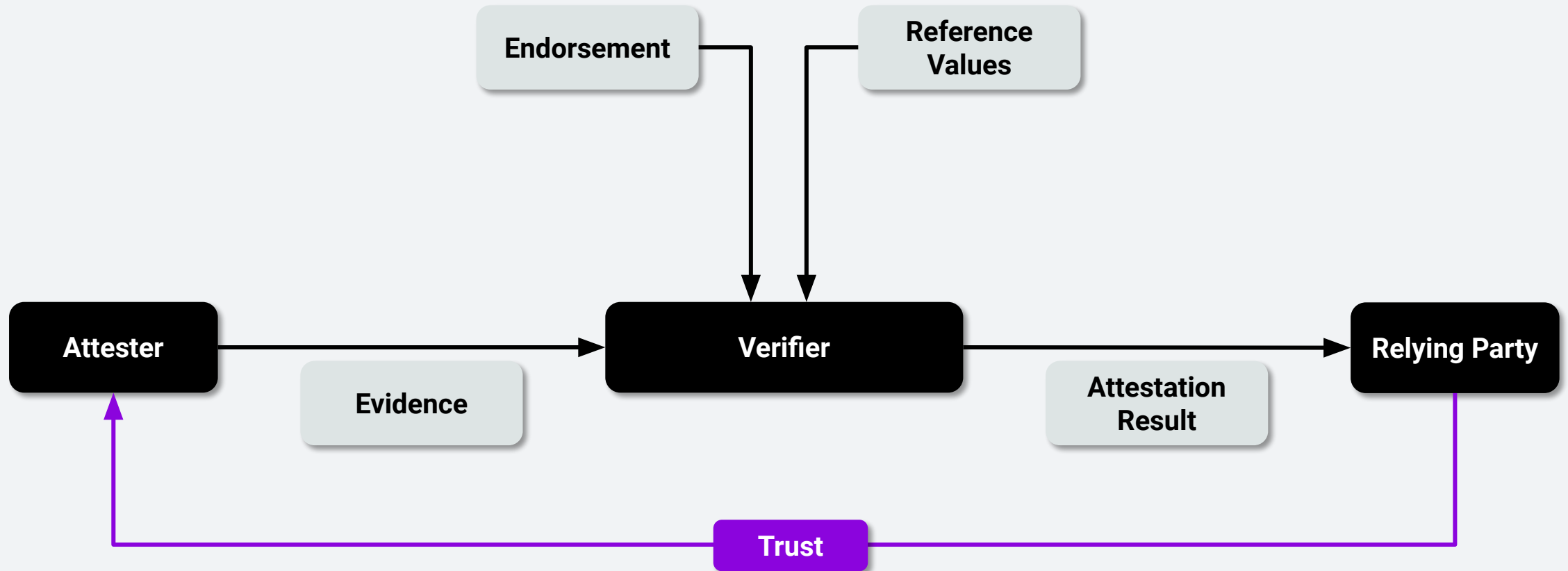
- Is TEE hardware used?
- Is the right code running?
- Is the firmware up to date?
- Remote attestation needed!

# Remote Attestation procedureS: RFC 9334 (RATS)





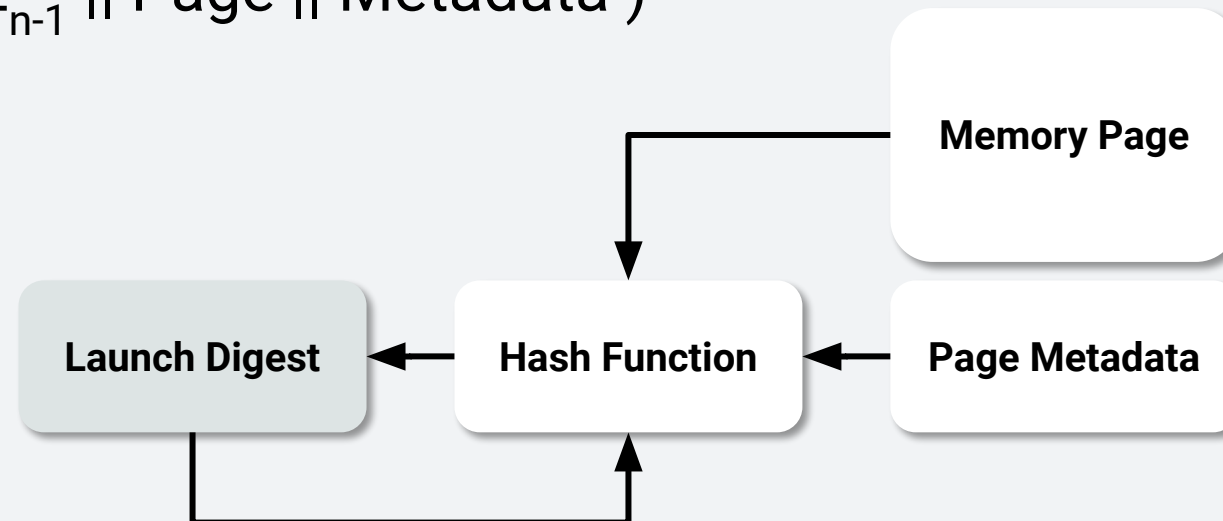
# Remote ATtestation procedureS: RFC 9334 (RATS)



# Measuring what's there

- **Launch measurement** during Confidential VM boot
- Measure guest Pages

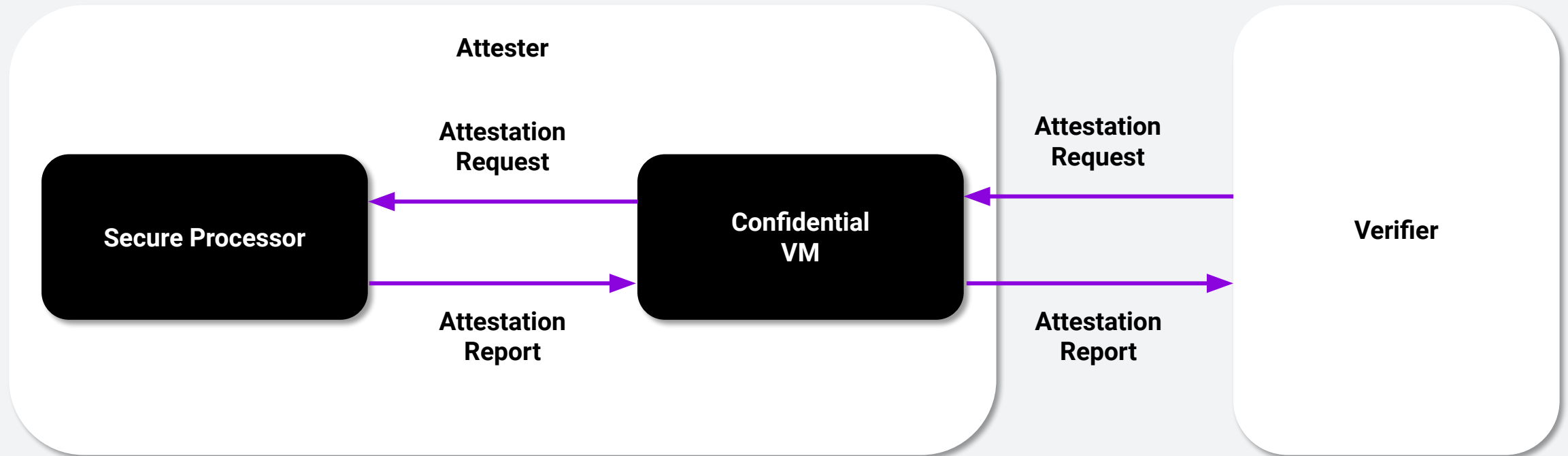
$$L_n = \text{Hash}( L_{n-1} \parallel \text{Page} \parallel \text{Metadata} )$$



# Measuring what's there

- **Platform measurement** = Security Version Numbers (SVN)
  - Secure Processor Bootloader SVN
  - Secure Processor OS SVN
  - SNP firmware SVN
  - Processor microcode SVN

# Attestation flow



# Attestation report

Evidence

```
type snpAttestationReport struct {
```

```
    ReportedTCB          tcbVersion
```

```
    LaunchMeasurement [48]byte ← Identifies code running in CVM
```

```
    ReportData         [64]byte ← Data from attestation request
```

```
    IDKeyDigest        [48]byte
```

```
    ChipID             [64]byte
```

```
    ... more fields
```

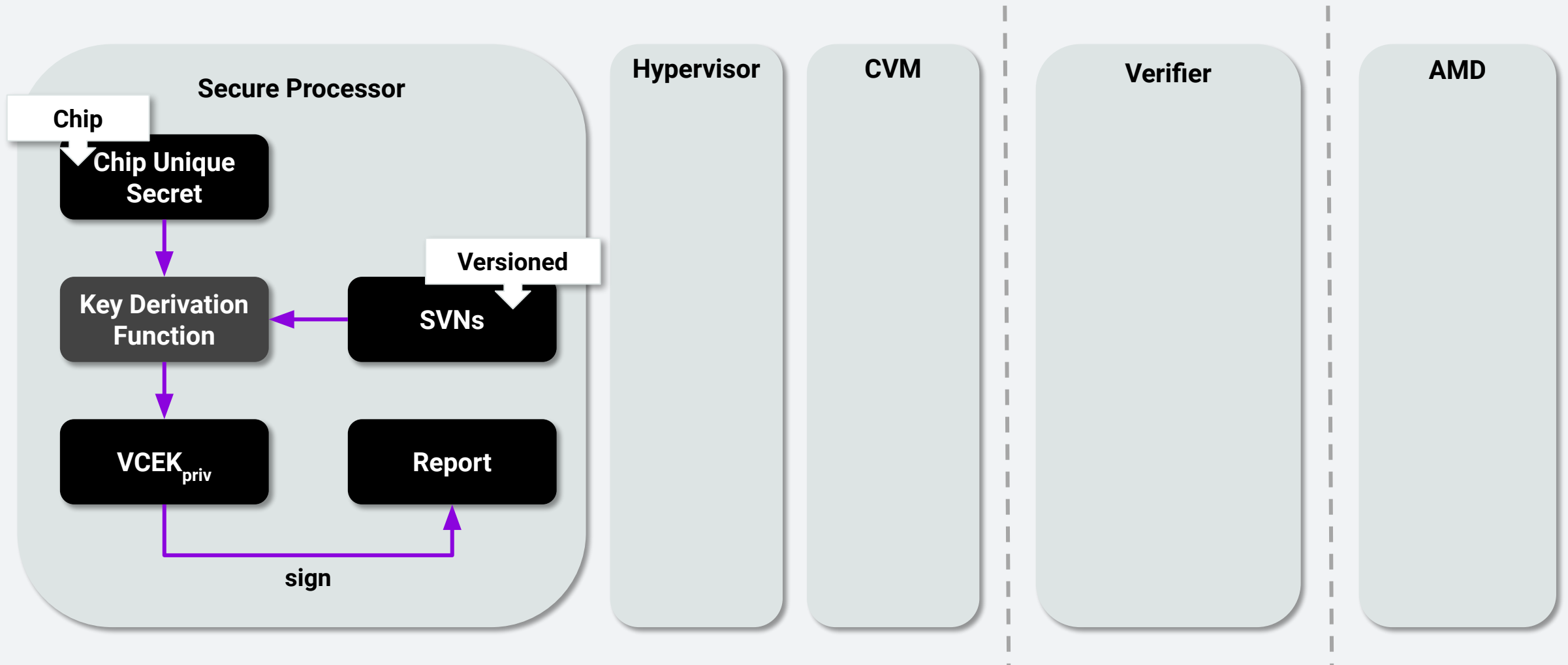
```
    Signature          [512]byte ← Signed by VCEK
```

```
}
```

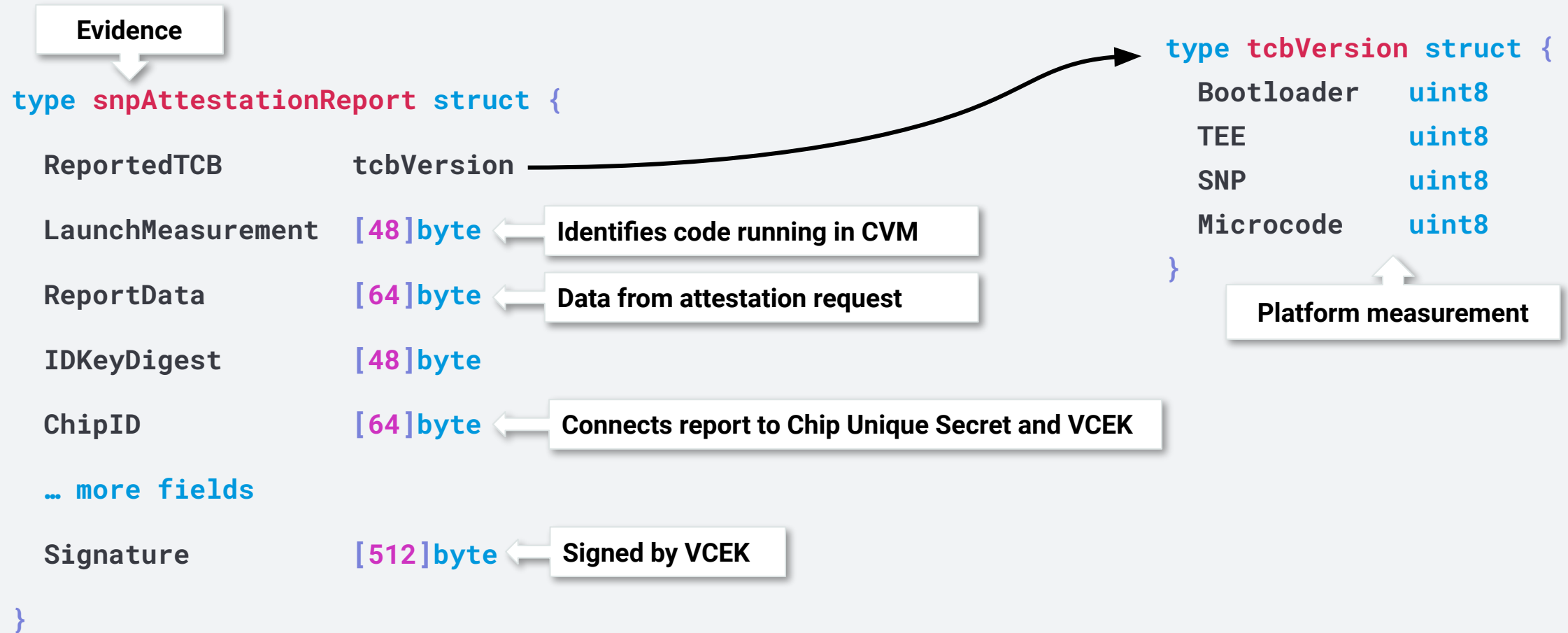
```
type tcbVersion struct {  
    Bootloader  uint8  
    TEE         uint8  
    SNP         uint8  
    Microcode   uint8  
}
```

Platform measurement

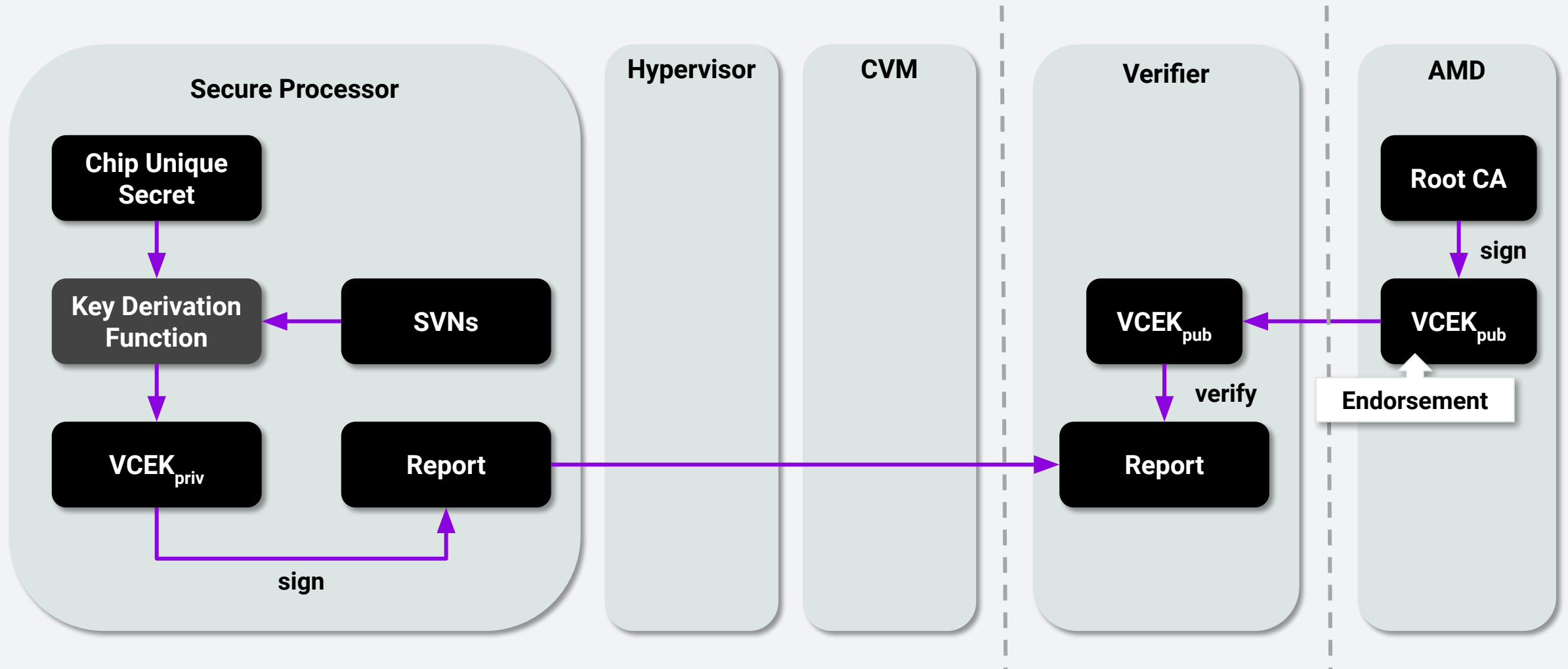
# Versioned Chip Endorsement Key (VCEK)



# Attestation report



# Versioned Chip Endorsement Key (VCEK)

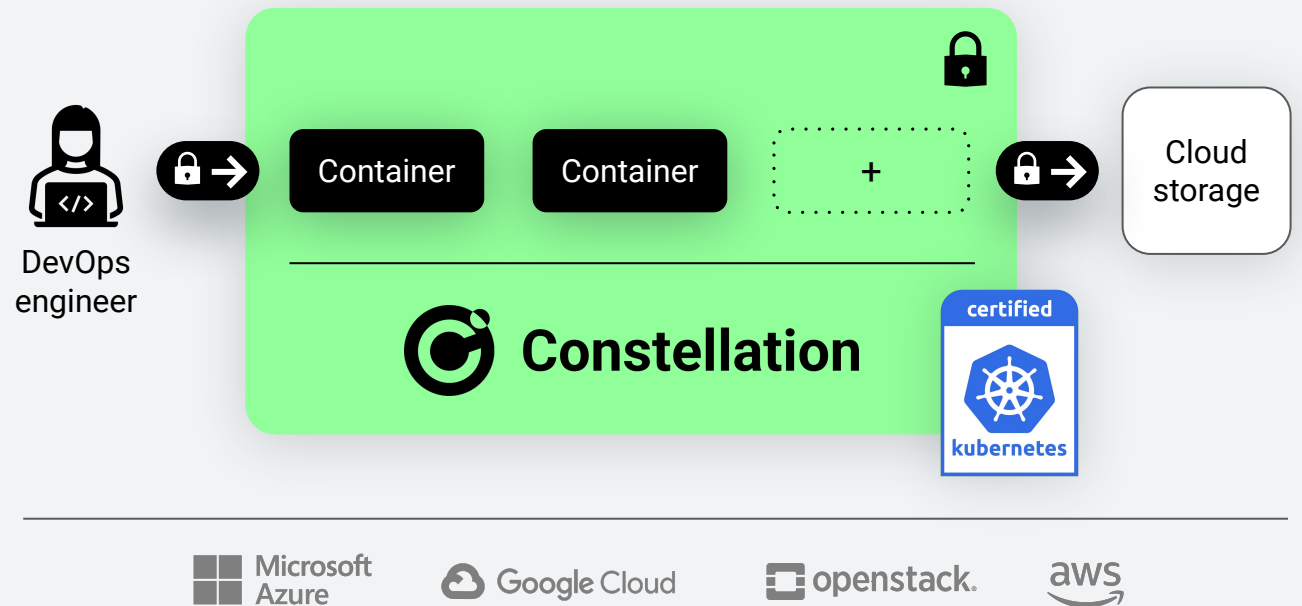




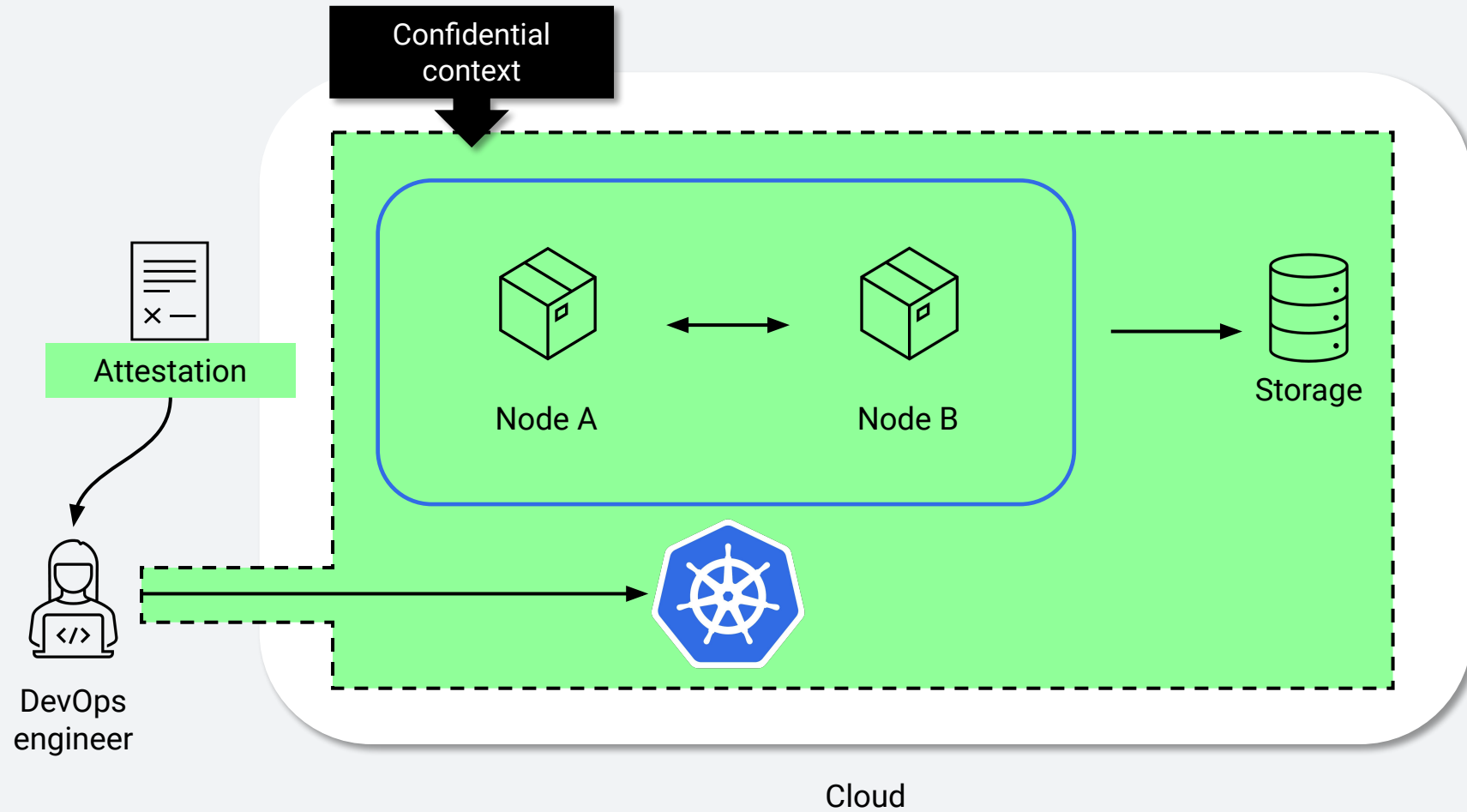
# Constellation

```
constellation config generate <cloud>
constellation create
constellation init

kubectl [scale anything!]
```



# How do we get there?

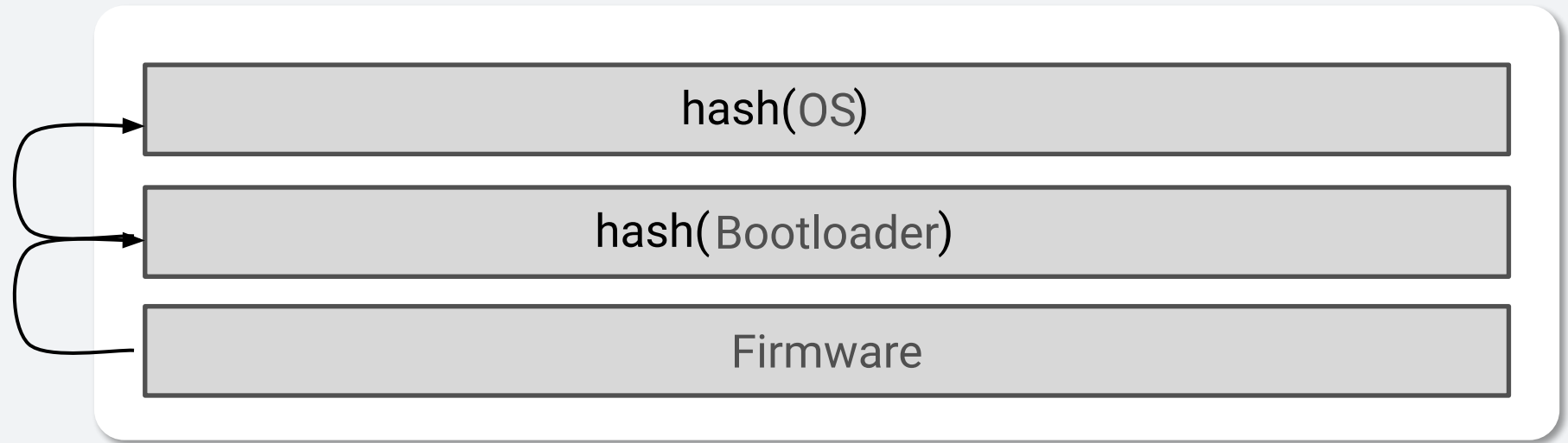




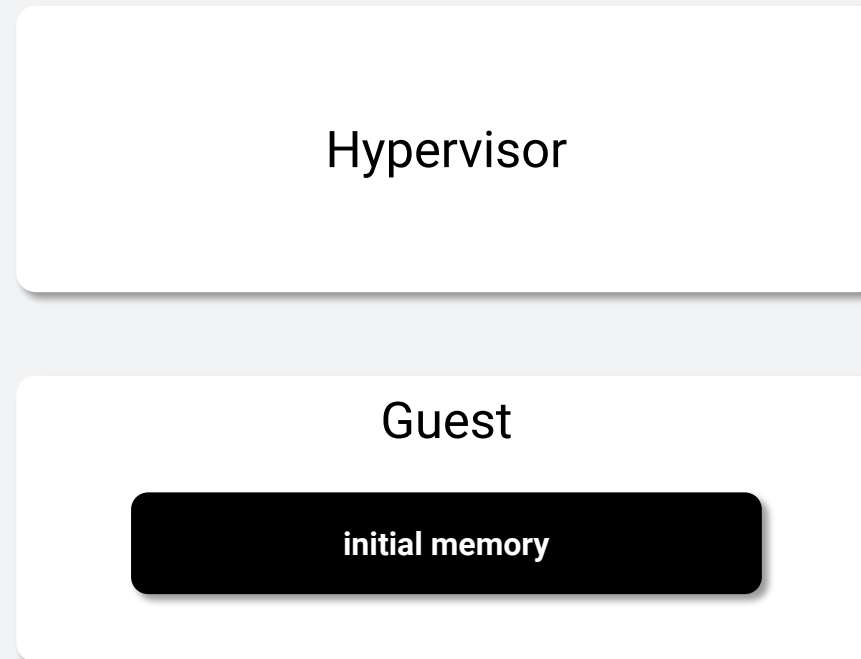
## Measured Boot 101 – Extend PCR

$$\text{PCR}[i]' = \textit{hash}(\text{PCR}[i] \parallel \text{data})$$

# Measured Boot Chain



# Confidential VM Boot



# Launching a Guest

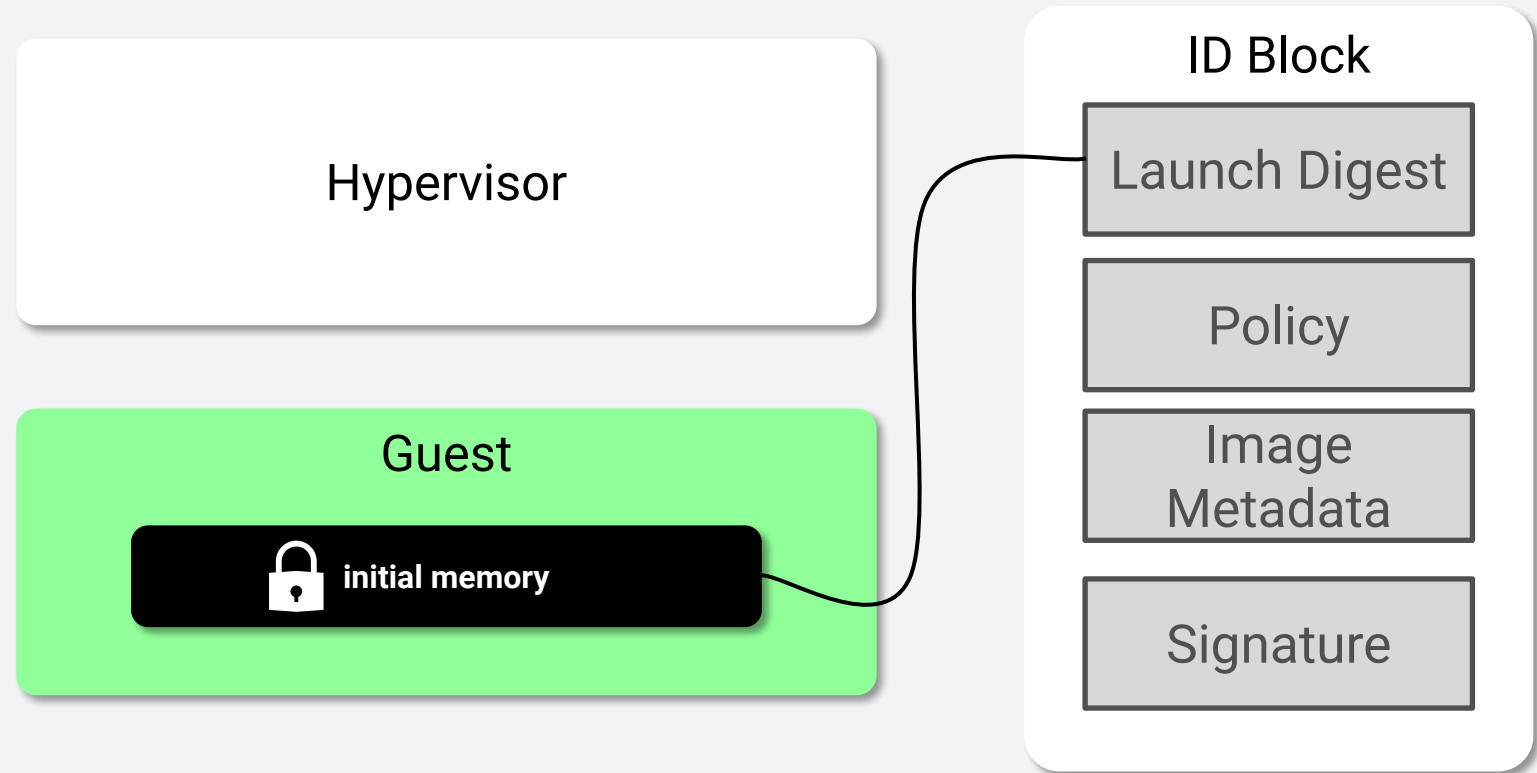
Hypervisor

Guest



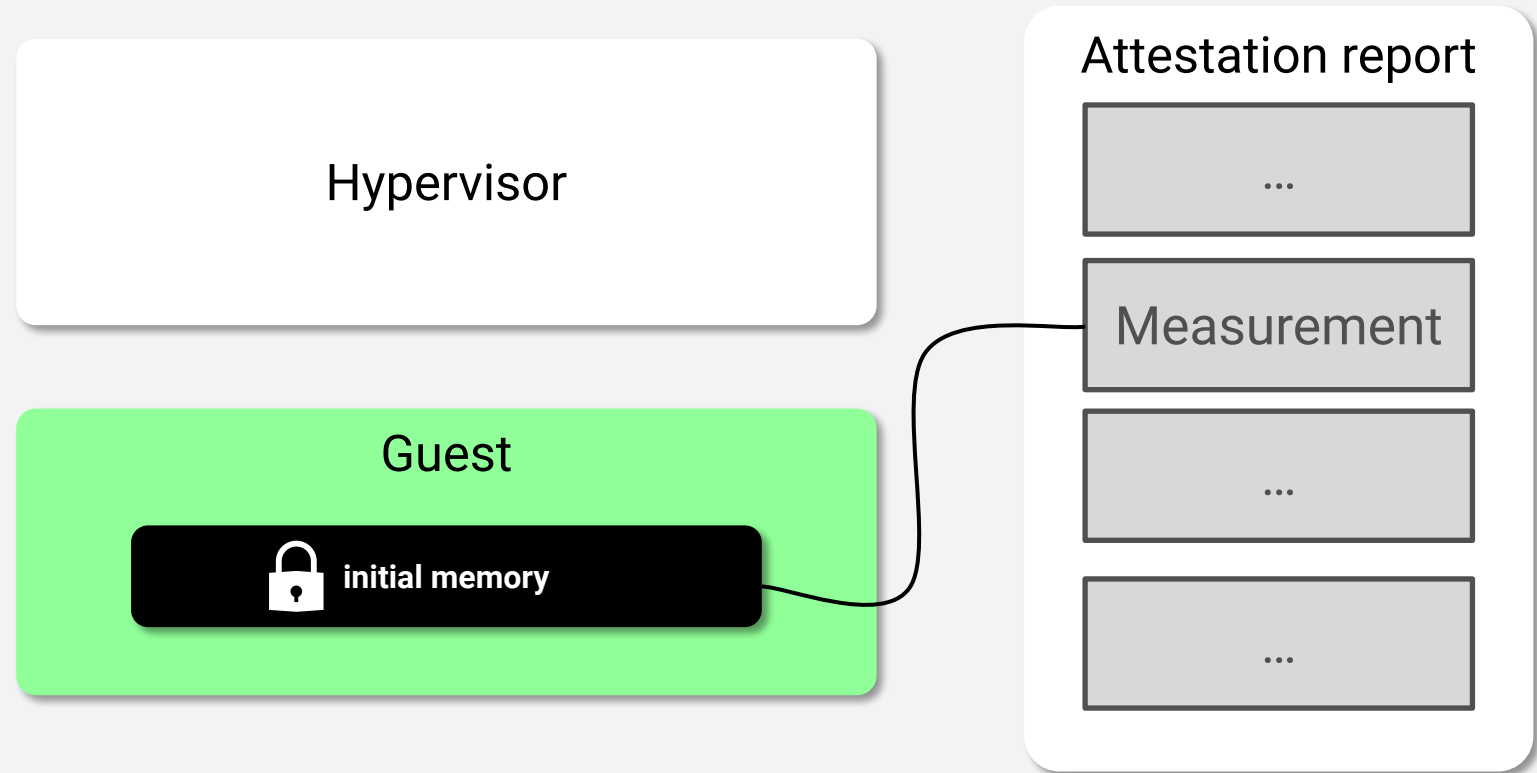
initial memory

# Launch measurement





# Launch measurement



# Protection rings

ring 1

Userspace

ring 0

Kernel

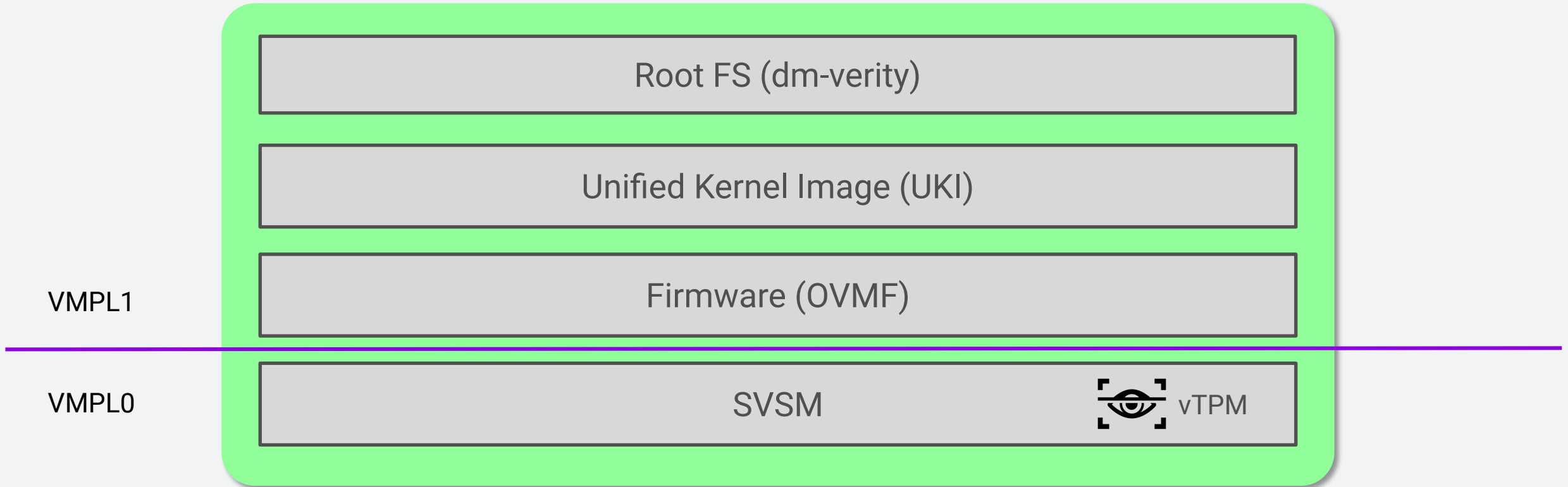
ring -1

Hypervisor

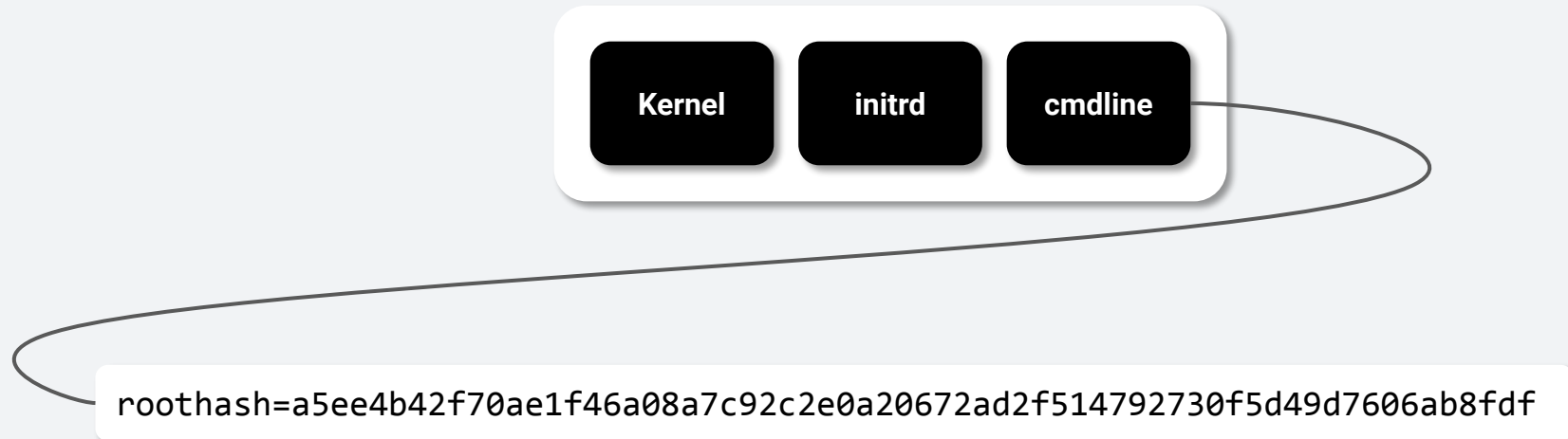
# Measured boot chain – SVSM



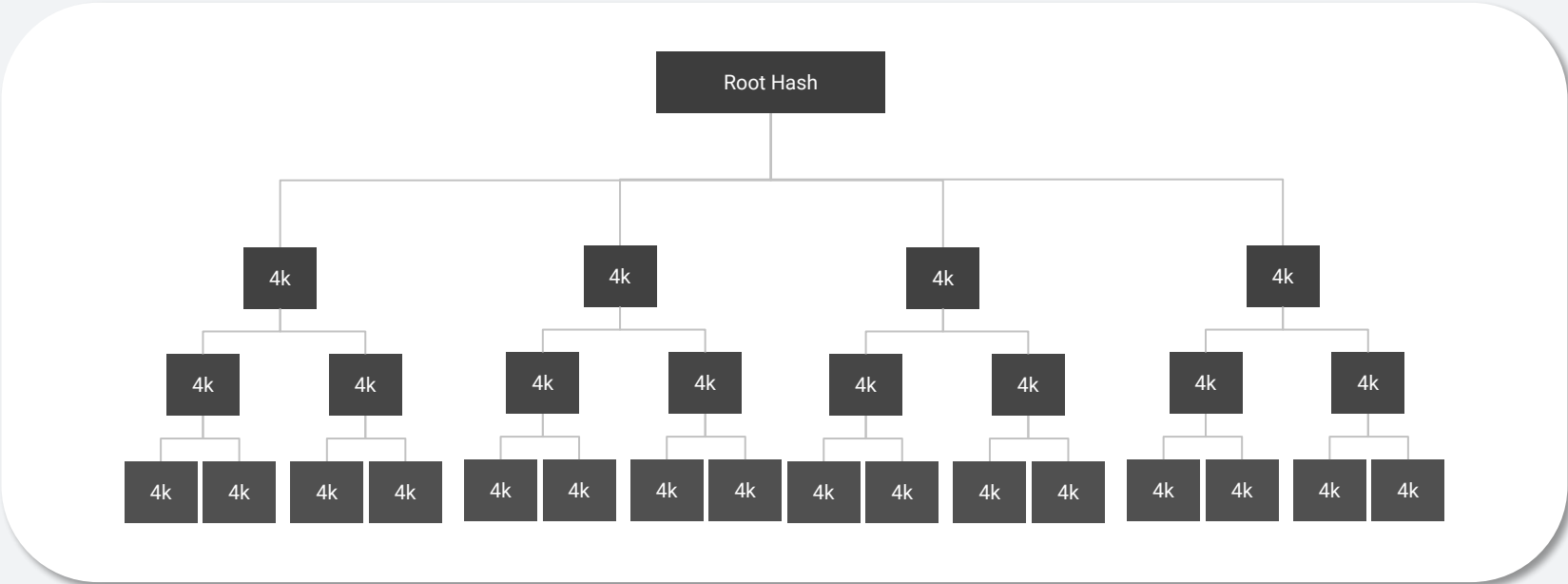
# Measured boot chain



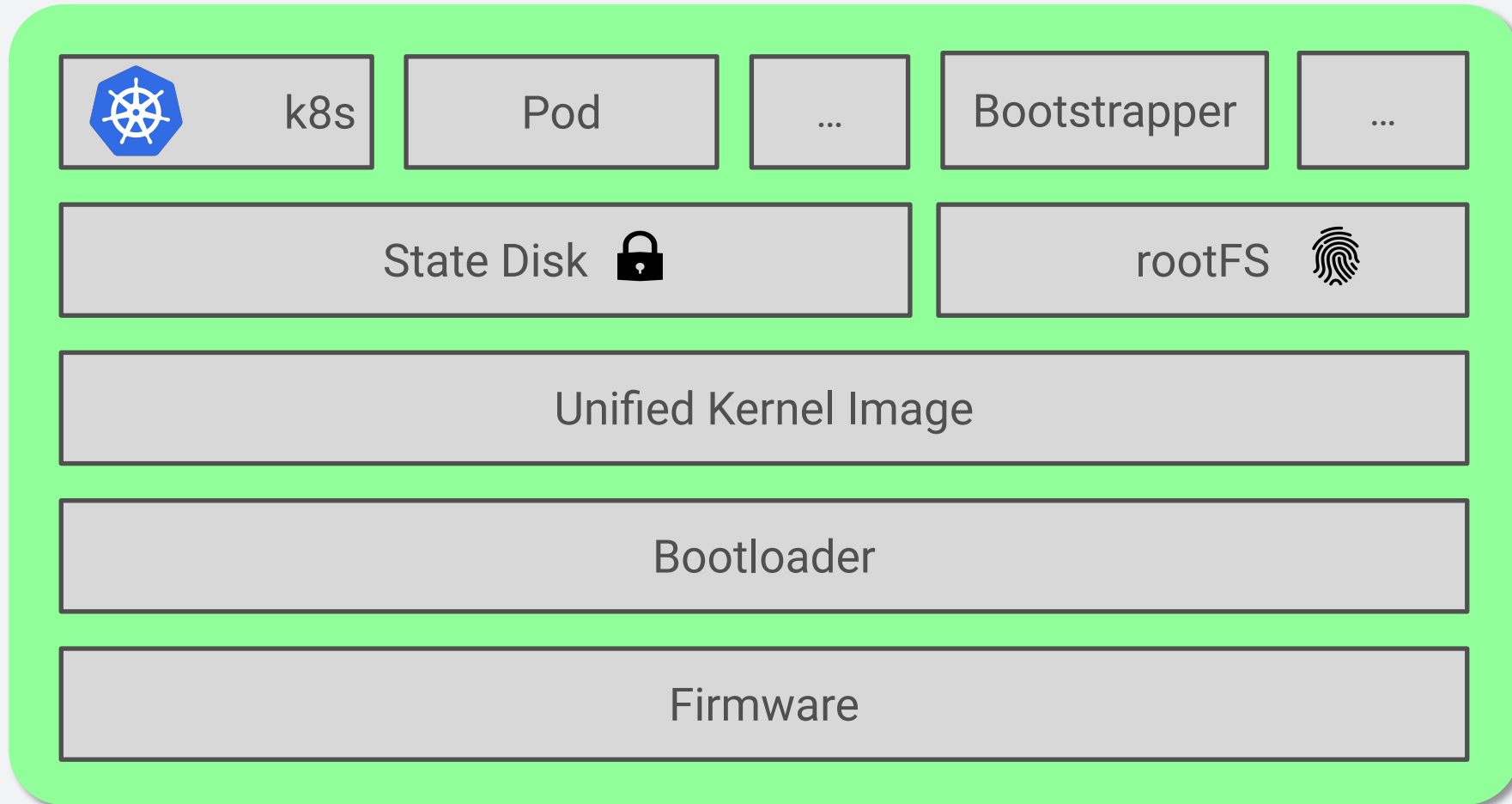
# Unified Kernel Image



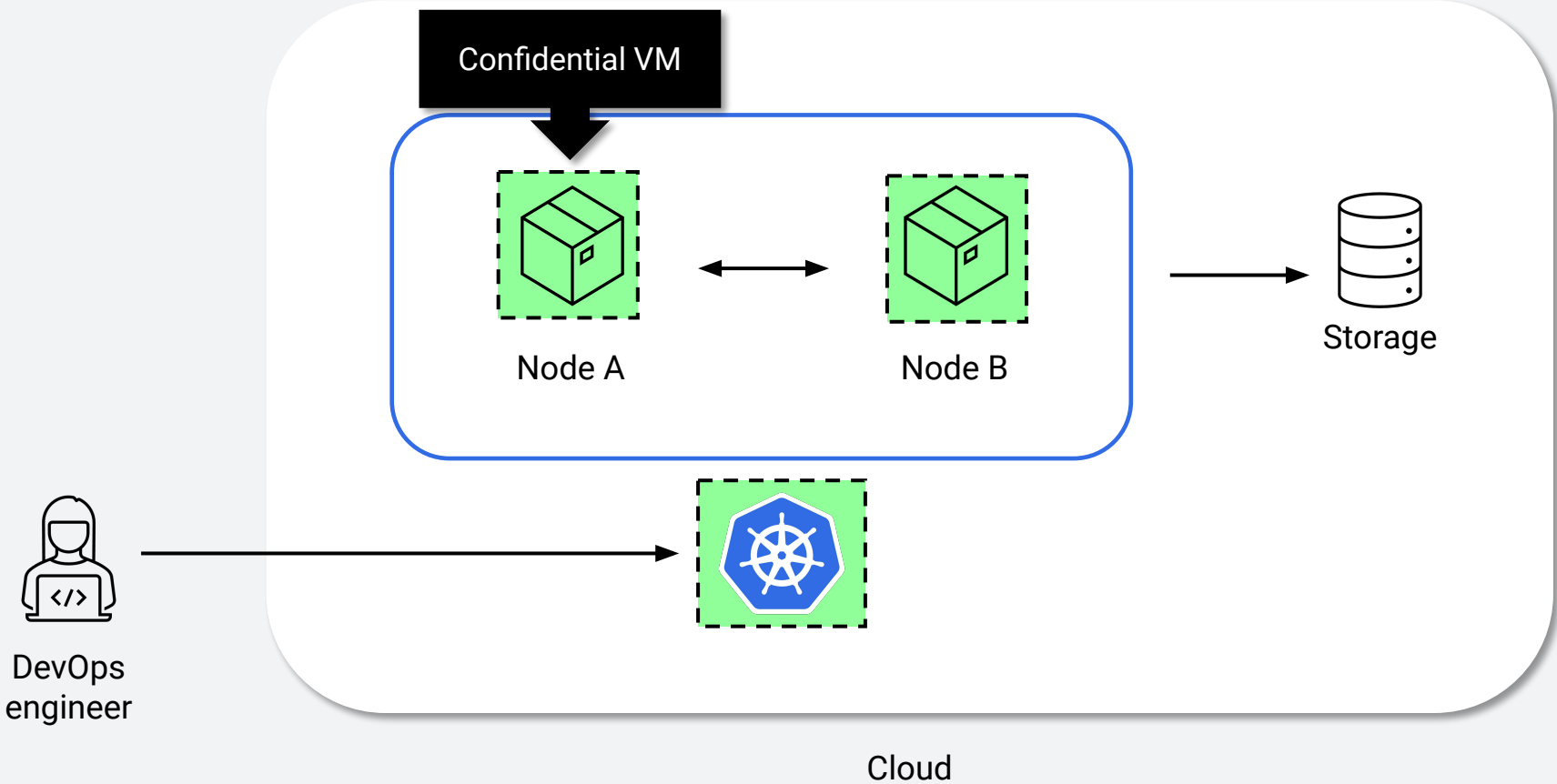
# dm-verity



# Constellation Nodes

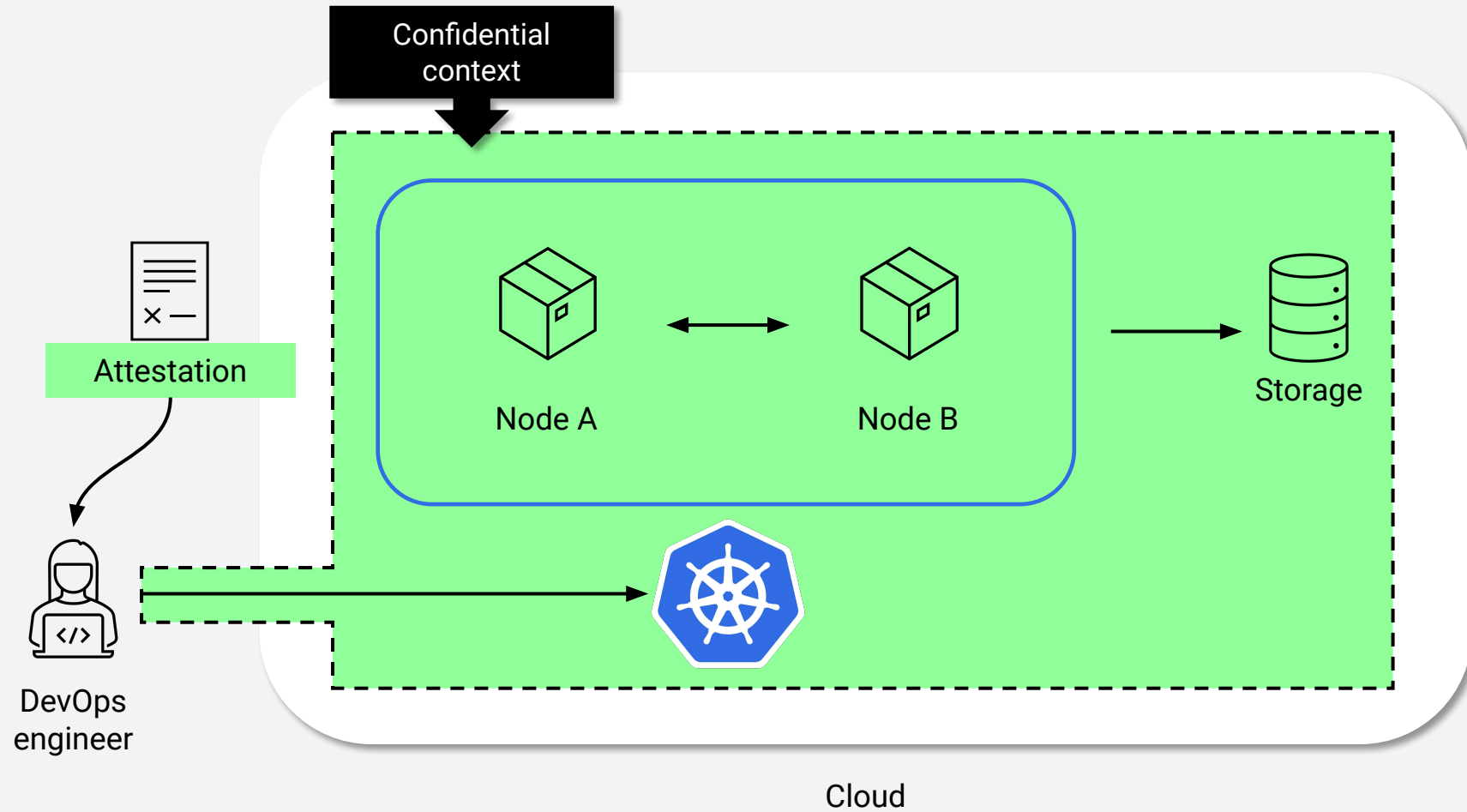


# How to get from here...

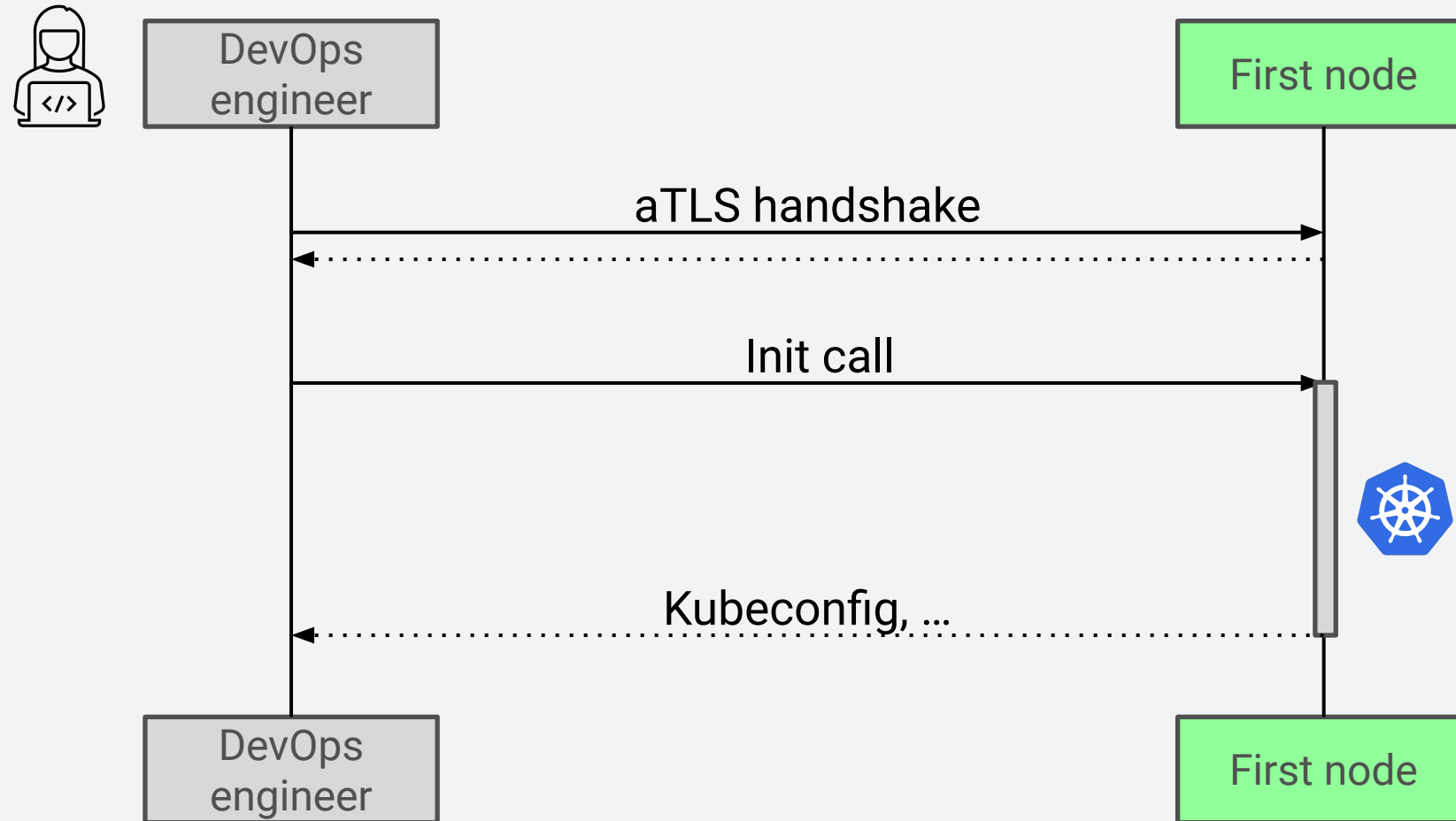




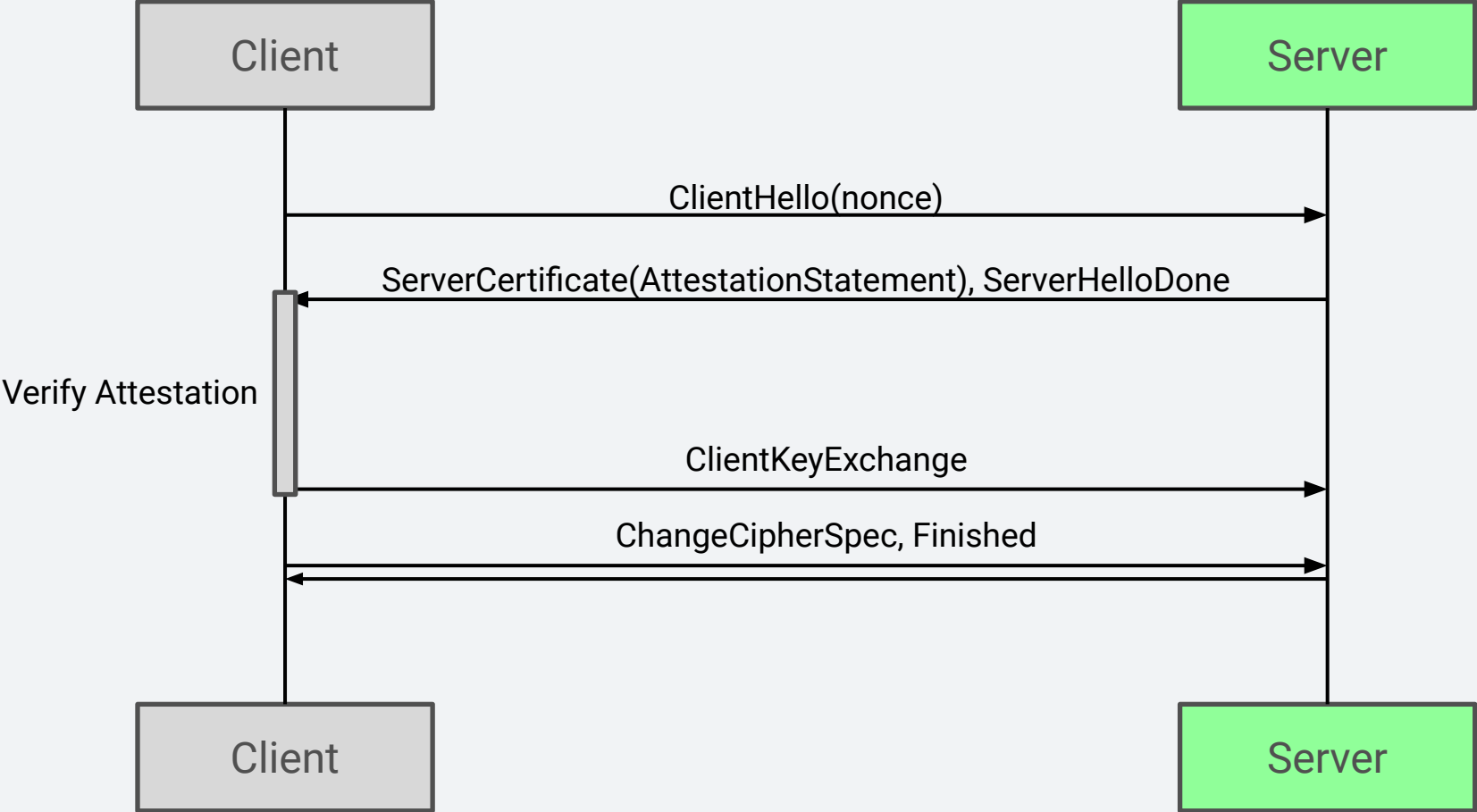
# ... to a Confidential Cluster?



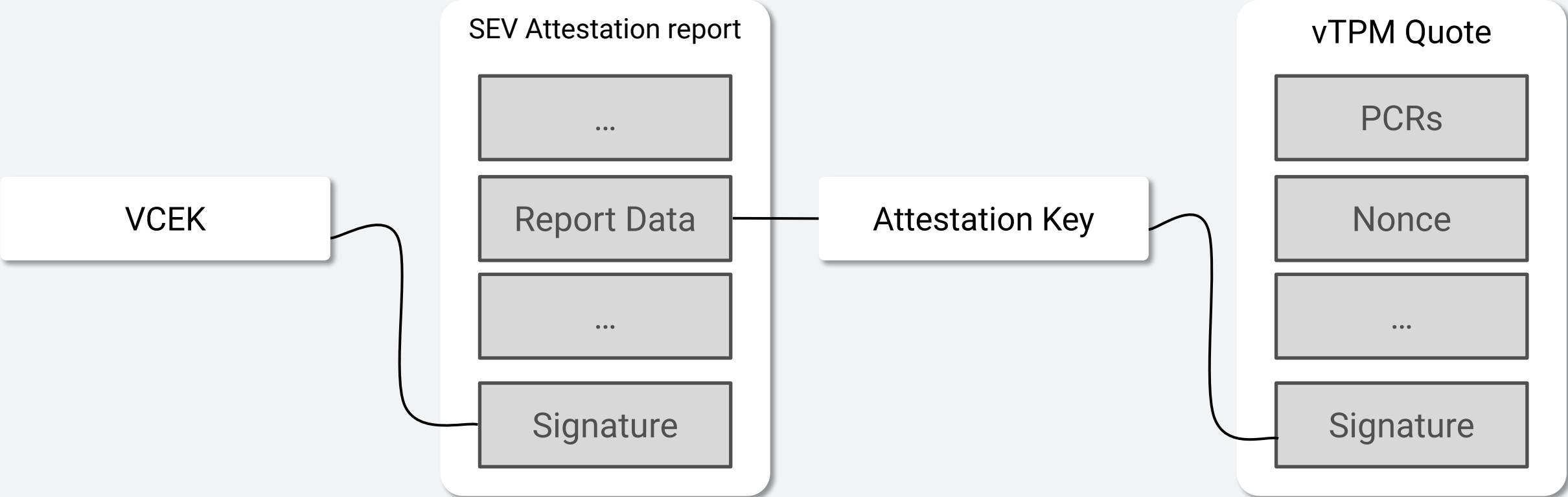
# Cluster initialization



# aTLS handshake



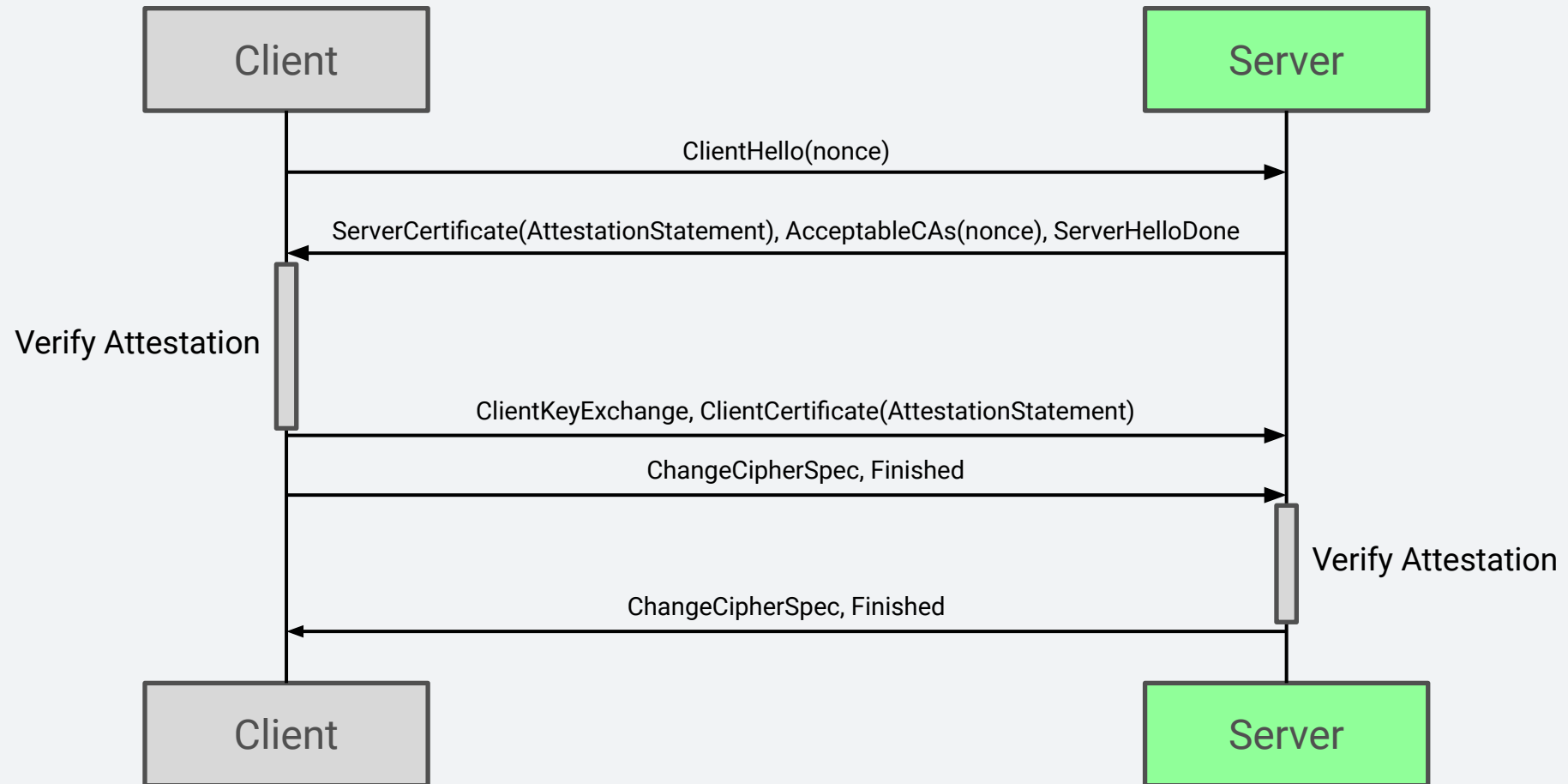
# aTLS handshake - Attestation



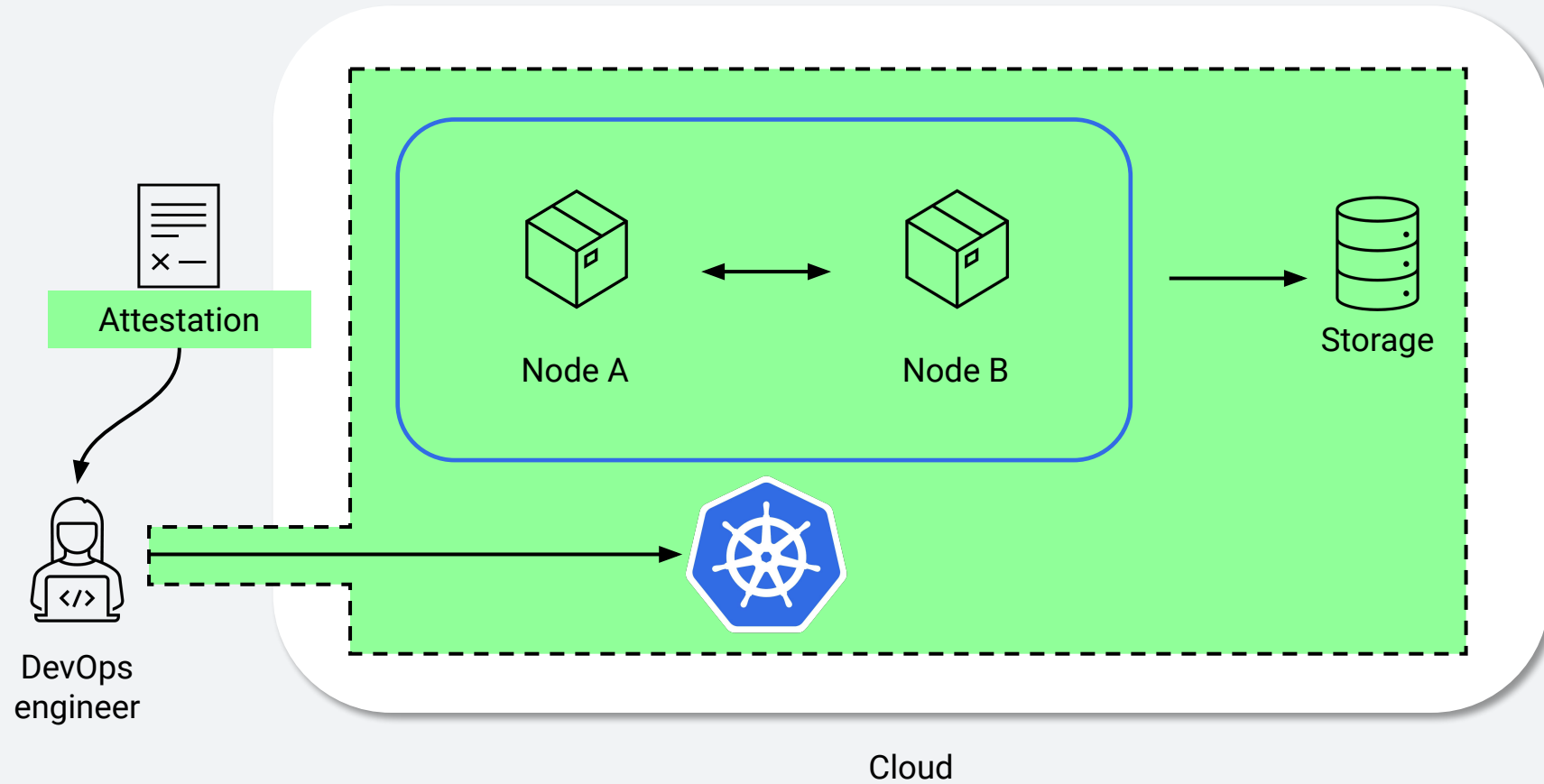
# Autonomous Join



# mutual aTLS handshake



# ... bringing it all together



# What are you waiting for?

```
constellation config generate <cloud>  
constellation create  
constellation init  
  
kubect1 [scale anything!]
```



# Thanks!

- Check it out on GitHub: [github.com/edgelessys/constellation](https://github.com/edgelessys/constellation)
- Ask us for a demo!



Malte Poll

[@malte@chaos.social](mailto:@malte@chaos.social)

[@malt3](https://twitter.com/malt3)

[github.com/malt3](https://github.com/malt3)



Paul Meyer

[@katexochen@infosec.exchange](mailto:@katexochen@infosec.exchange)

[@katexochen](https://twitter.com/katexochen)

[github.com/katexochen](https://github.com/katexochen)

# Learn more

- [Constellation documentation](#)
- [Confidential Computing whitepaper](#)
- [Constellation cluster attestation](#)
- [Edgeless Systems blog](#)

## App demos on Constellation

