



KubeCon



CloudNativeCon

Europe 2026

Enforce VIP access only through node attestation

Alice Frosi, Principal Software Engineer, Red Hat
Jakob Naucke, Software Engineer, Red Hat



Trusted Execution Cluster Club



KubeCon



CloudNativeCon

Europe 2026



Generated by Gemini

Confidential Computing



KubeCon



CloudNativeCon

Europe 2026

*“Confidential Computing protects **data in use** by performing computation in a hardware-based, attested **Trusted Execution Environment**. These secure and isolated environments **prevent unauthorized access or modification** of applications and data while in use, thereby increasing the security assurances for organizations that manage **sensitive and regulated data**.”*

Trusted execution clusters



KubeCon



CloudNativeCon

Europe 2026

- Confidential boundary is the entire cluster
 - each node in the cluster is confidential
 - Using technologies such as AMD SEV-SNP or Intel TDX
- The trust is in
 - the cluster administrator
 - but not in the cloud provider
- Use cases:
 - Migration to **public cloud** keeping the data confidential
 - On-premise, **data separation** among organizations
 - **Proof** that the nodes are **confidential**

Remote Attestation

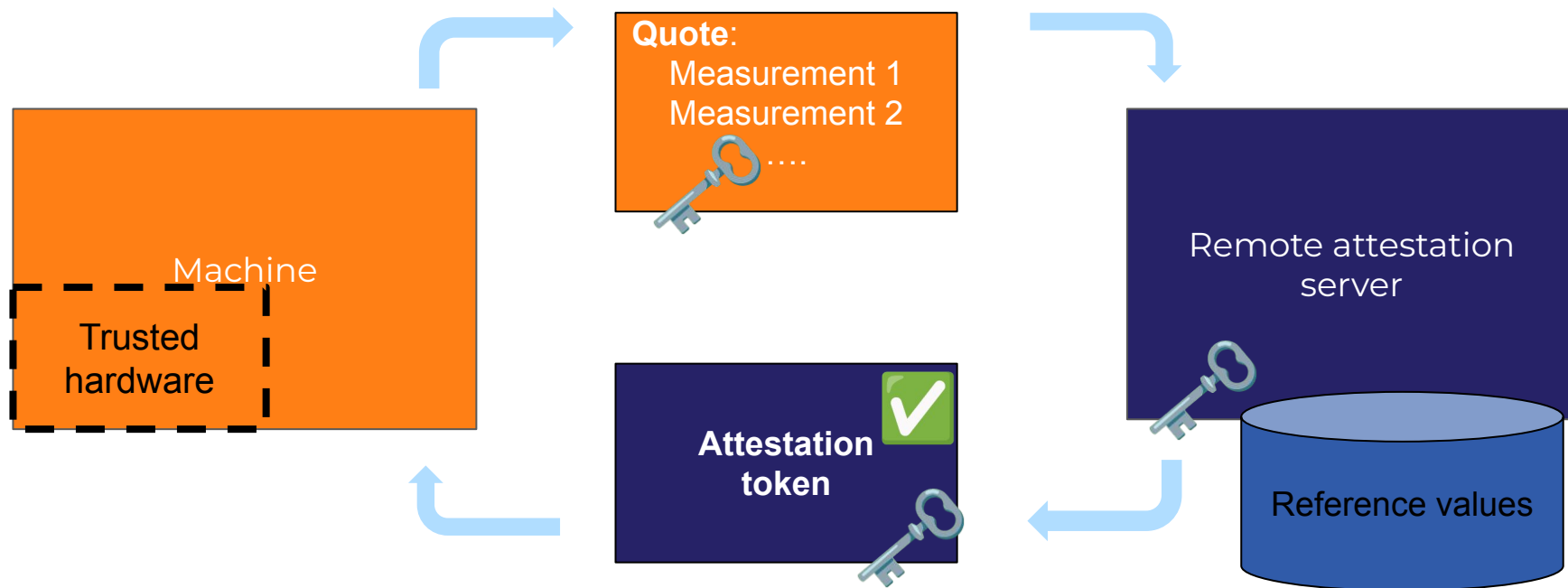


KubeCon



CloudNativeCon

Europe 2026



Attestation in practice



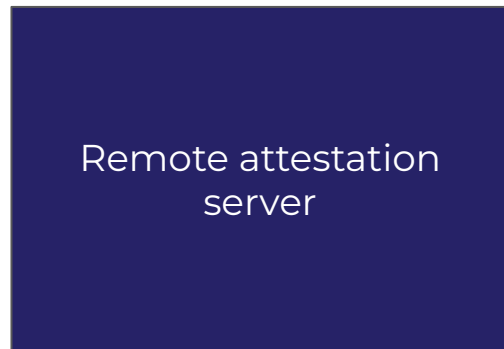
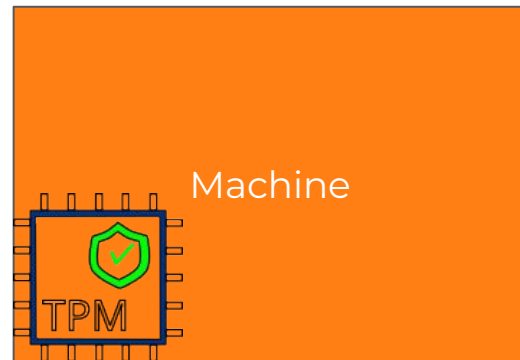
KubeCon



CloudNativeCon

Europe 2026

- **TPM** (Trusted Platform Modules) is the trusted hardware which creates and signs the quote
- The remote attestation server is implemented by [Trustee](#)
- **Security policies**
 - If the attestation is successful is defined by the **attestation policy**
 - A resource is unlocked by the **resource policy**



Attestation in practice

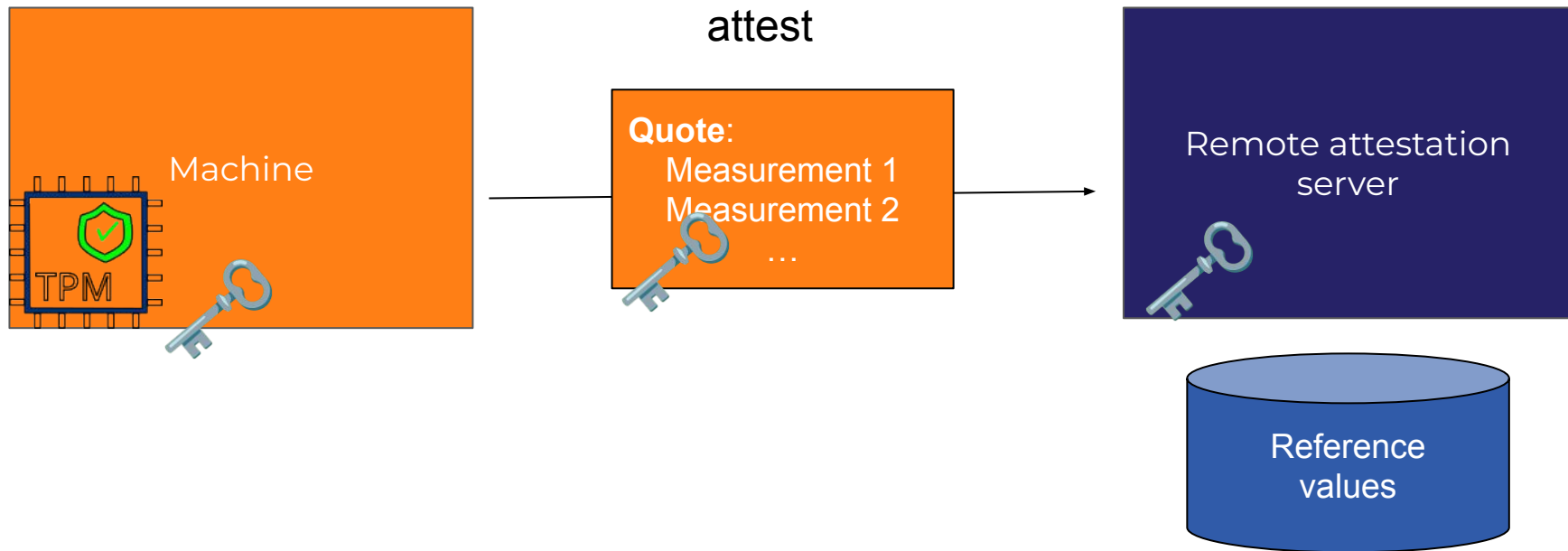


KubeCon



CloudNativeCon

Europe 2026



Attestation in practice

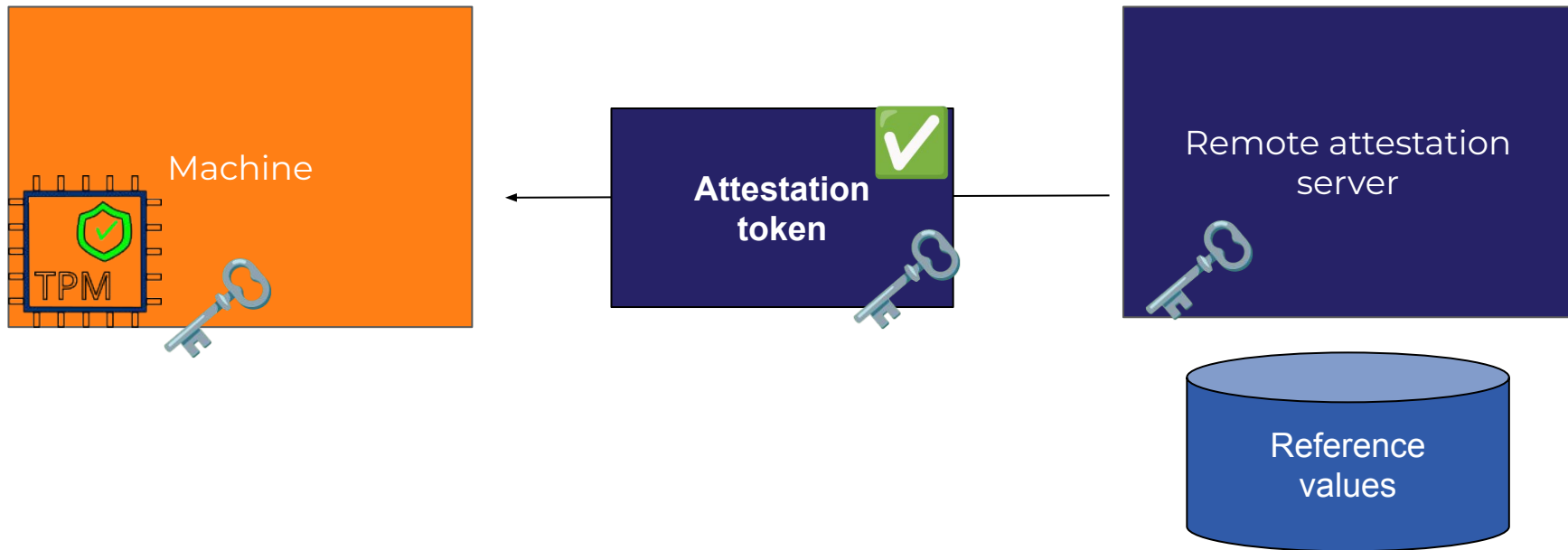


KubeCon



CloudNativeCon

Europe 2026



Attestation in practice

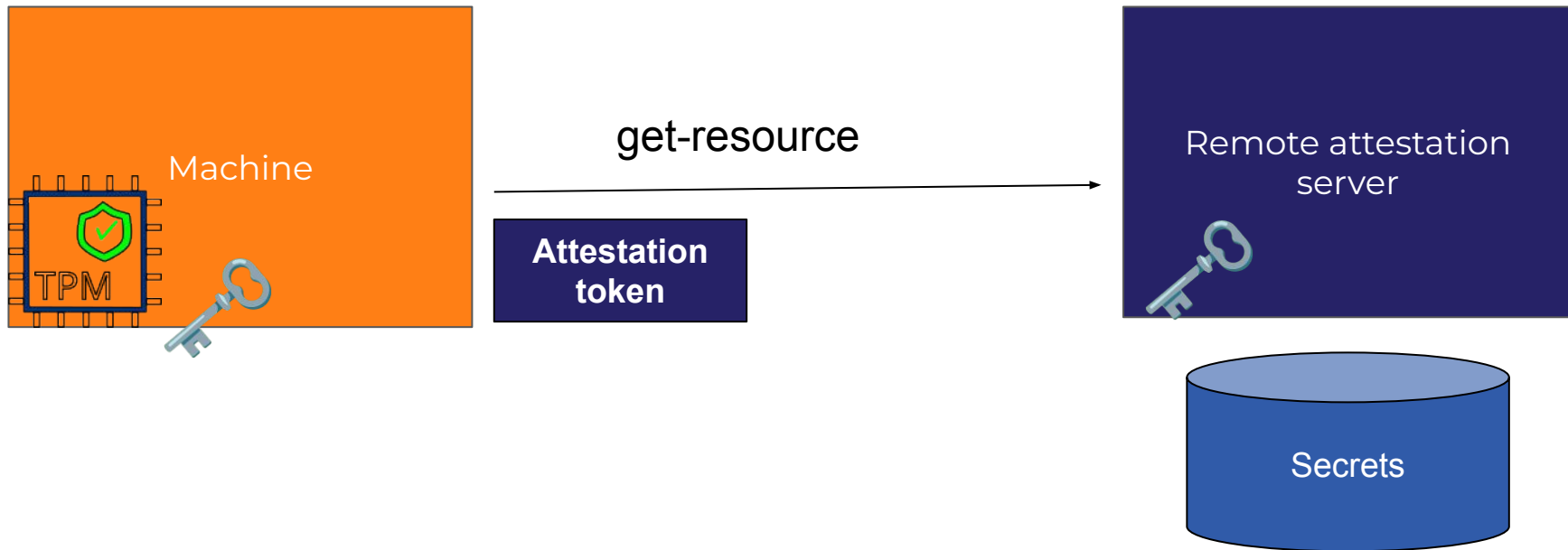


KubeCon



CloudNativeCon

Europe 2026



Attestation in practice

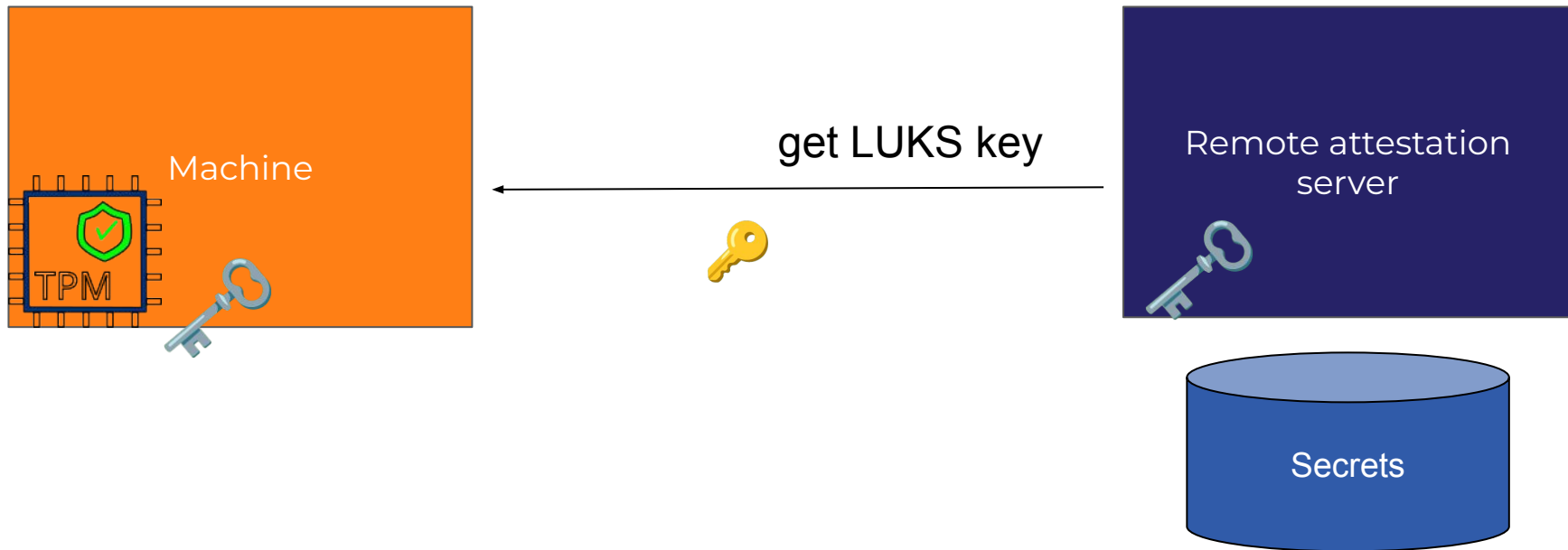


KubeCon



CloudNativeCon

Europe 2026



Challenges

- Automation of the complex process
- Coordination of the nodes in the cluster
- Reference values calculation and updates

Trusted Execution Cluster operator

+

machine components

Attester node requirements



KubeCon



CloudNativeCon

Europe 2026

- Ignition
- clevis-pin-trustee
- trustee-attester

<https://github.com/coreos/ignition>

<https://github.com/latchset/clevis-pin-trustee>

<https://github.com/confidential-containers/guest-components>

Node requirements: Ignition



KubeCon



CloudNativeCon

Europe 2026

- Ignition
- clevis-pin-trustee
- trustee-attester

```
{
  "storage": {
    "luks": [
      {
        "clevis": {
          "custom": {
            "config": "{ \"servers\": {...} ",
            "needsNetwork": true,
            "pin": "trustee"
          },
          "tpm2": null
        },
        "device": "/dev/disk/by-partlabel/root"
      }
    ]
  }
},
  "ignition": {
    "config": {
      "merge": [
        {
          "source": "https://register-server:8000/ignition-clevis-pin-trustee"
        }
      ]
    },
    "security": {
      "tls": {
        "certificate_authorities": [
          {
            "source": "data: ,-----%20BEGIN%20CERTIFICATE%20-----..."
          }
        ]
      }
    },
    "version": "3.6.0-experimental"
  }
}
```

Node requirements: clevis-pin-trustee



KubeCon



CloudNativeCon

Europe 2026

- Ignition
- clevis-pin-trustee
- trustee-attester

```
clevis luks bind -f \  
  -k /tmp/$existing_key \  
  -d /dev/mapper/root \  
  trustee $json
```

```
{  
  "servers": [  
    {  
      "url": "https://kbs-service:8080",  
      "cert": "----- BEGIN CERTIFICATE ----- \n ..."  
    }  
  ],  
  "path": "default/225777d3-297c-4529-bf0c-30fc13803710/root",  
  "initdata": "{\"uuid\": \"225777d3-297c-4529-bf0c-30fc13803710\"}",  
  "attestation_key": {  
    "registration": {  
      "url": "https://attestation-key-register:8001/register-ak",  
      "cert": "----- BEGIN CERTIFICATE ----- \n ...",  
      "uuid": "225777d3-297c-4529-bf0c-30fc13803710"  
    }  
  }  
}
```

Node requirements: trustee-attester



KubeCon



CloudNativeCon

Europe 2026

- Ignition
- clevis-pin-trustee
- trustee-attester

```
trustee-attester \  
  --url https://kbs-service:8080 \  
  --cert ...  
get-resource \  
  --path default/225777d3-297c-4529-bf0c-30fc13803710/root \  
  --initdata '{"uuid": "225777d3-297c-4529-bf0c-30fc13803710"}'
```

Key brokering & attestation: Trustee

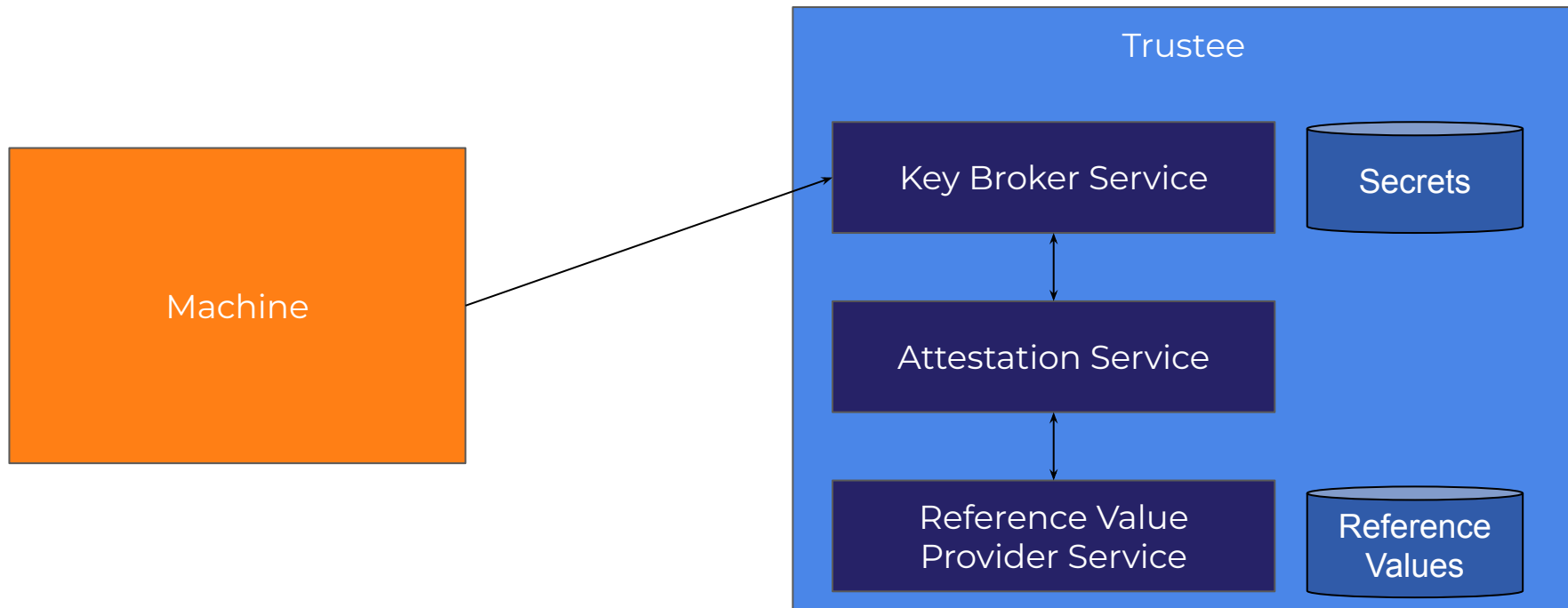


KubeCon



CloudNativeCon

Europe 2026



Attestation policy & reference values



KubeCon

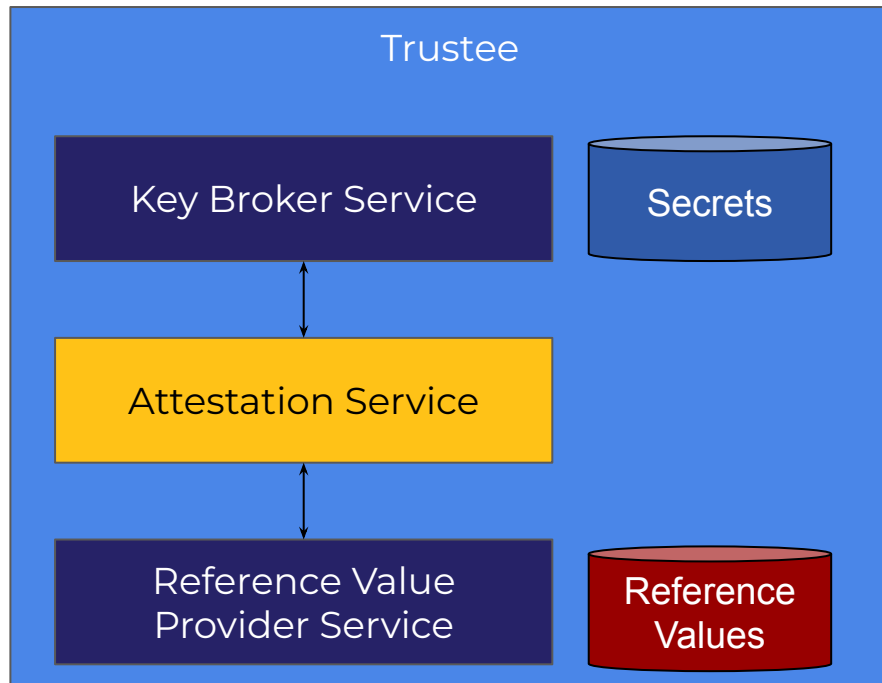


CloudNativeCon

Europe 2026

```
default executables := 33
executables := 3 if {
  input.tpm.pcr04 in
    query_reference_value(
      "tpm_pcr4"
    )
}
```

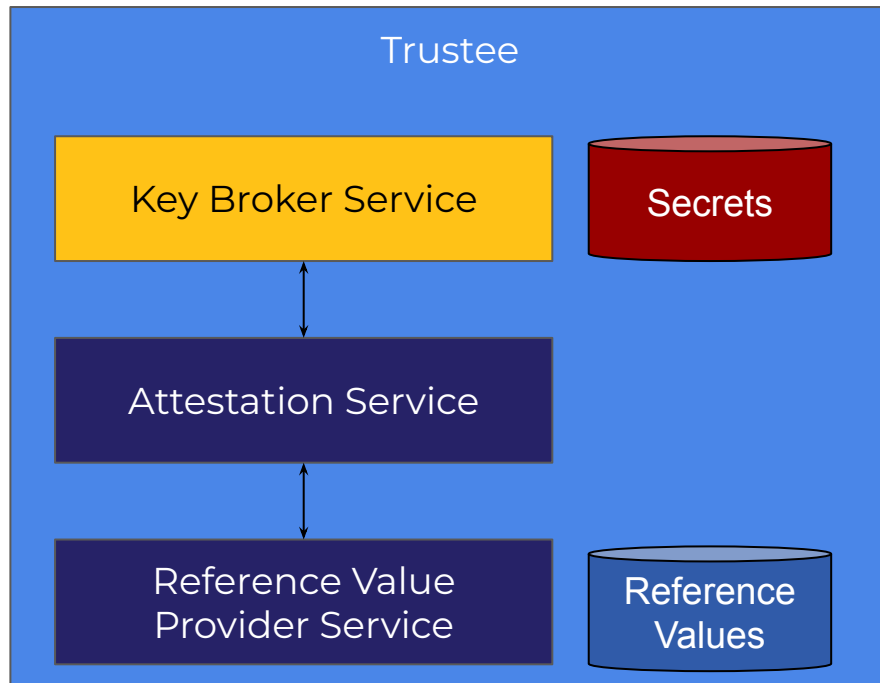
Each update to kernel and bootloader changes the reference values, on next boot and once more on boot thereafter



Initdata & resource policy

```
default allow := false
allow if {
  input.submods.cpu0
    ["status"] == "affirming"
  input.submods.cpu0
    ["annotated-evidence"]
      .init_data_claims.uuid ==
        data["resource-path"]
}
```

Store UUID in PCR8,
irreversibly mutating it



Operator: Registration flow

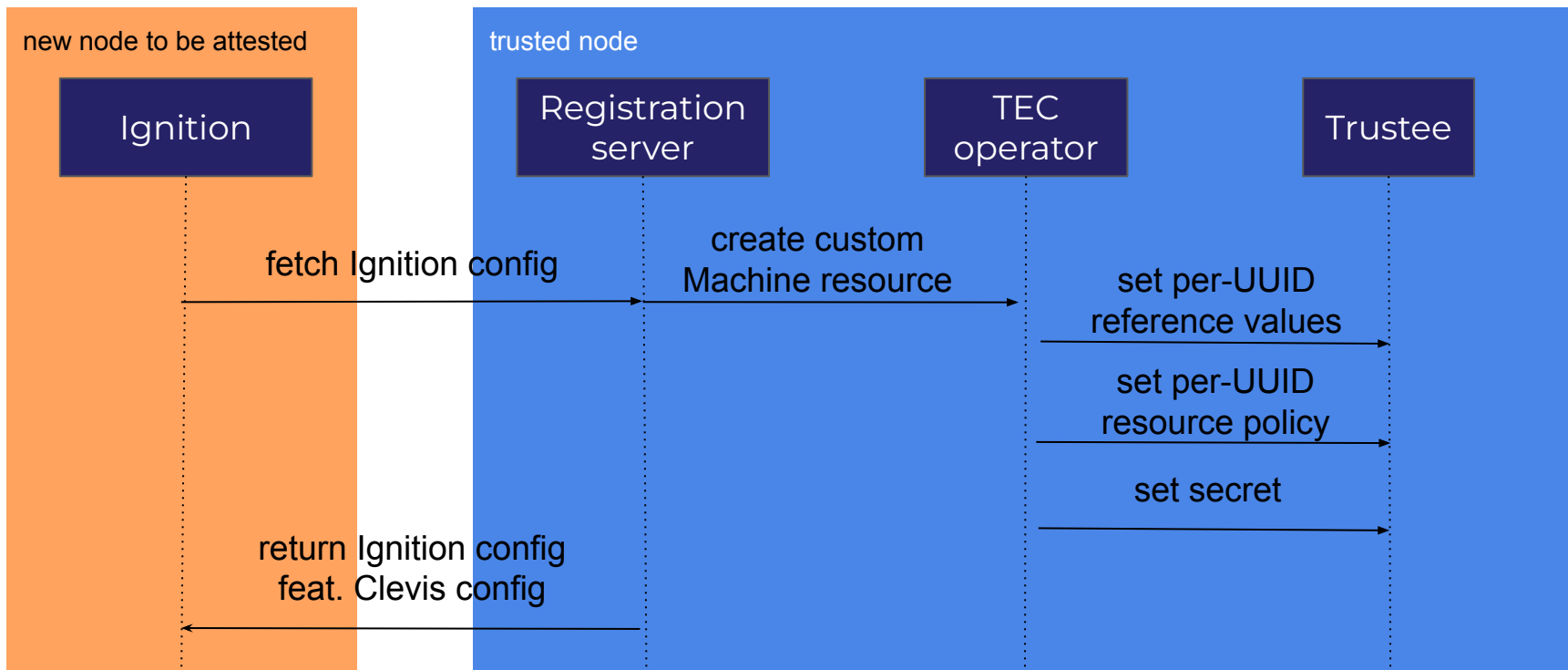


KubeCon



CloudNativeCon

Europe 2026



Operator: Attestation flow

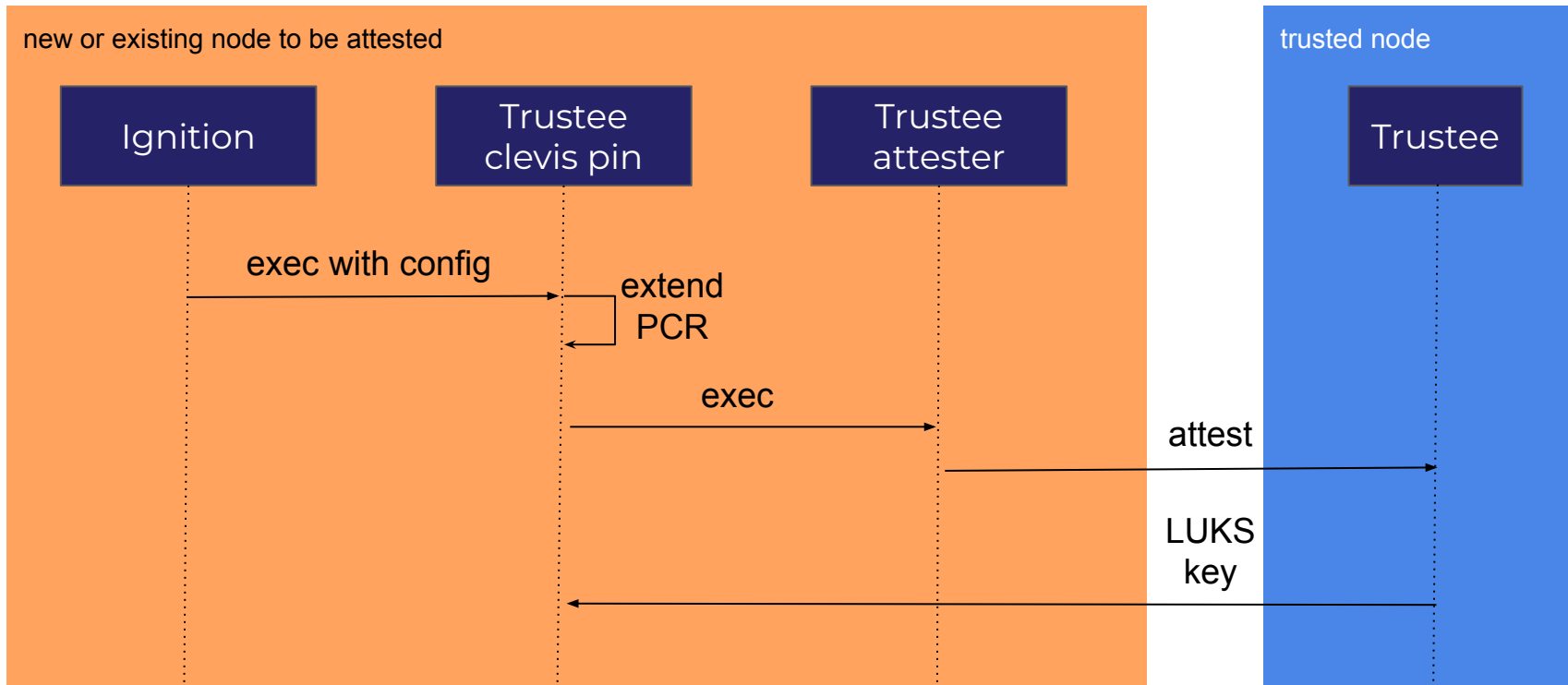


KubeCon



CloudNativeCon

Europe 2026



Operator: Approval flow



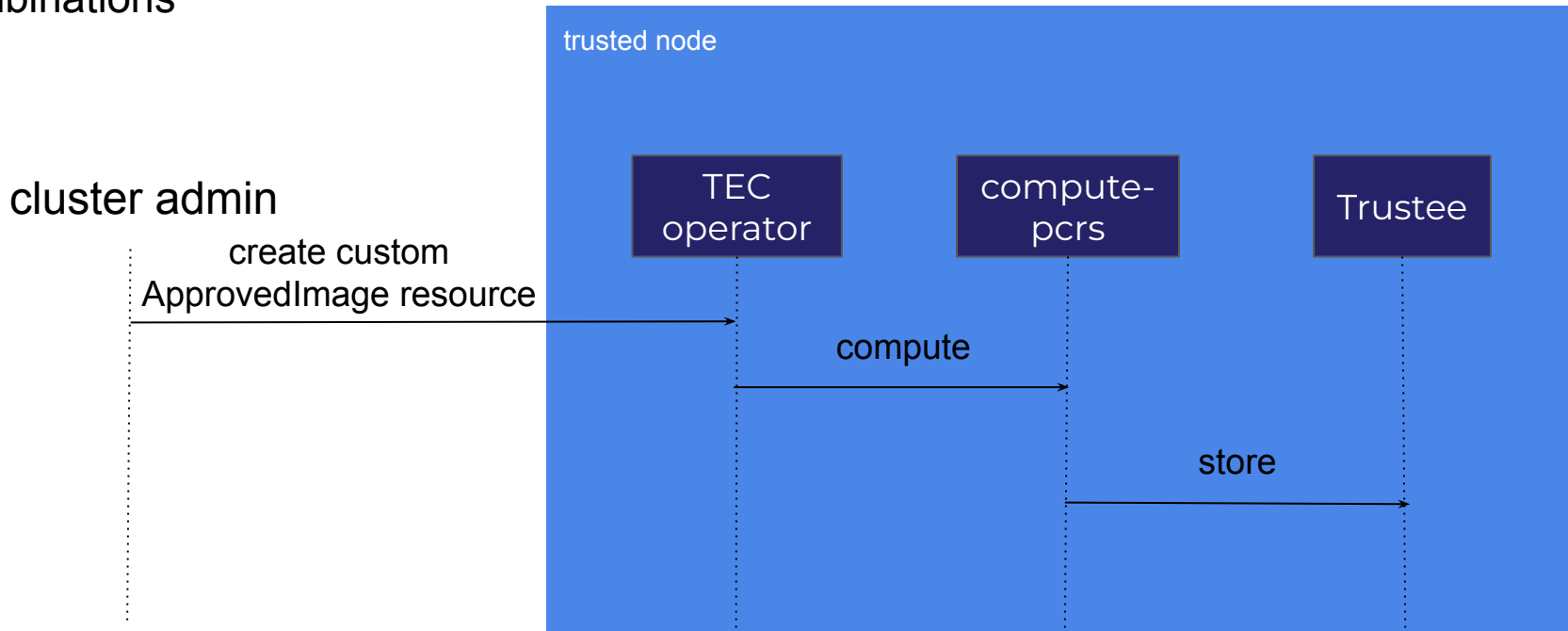
KubeCon



CloudNativeCon

Europe 2026

Reference values also depend on guest OS! must be computed for all bootloader/kernel combinations



<https://github.com/trusted-execution-clusters/compute-pcrs>

bootc: Wait, what *did* we approve?



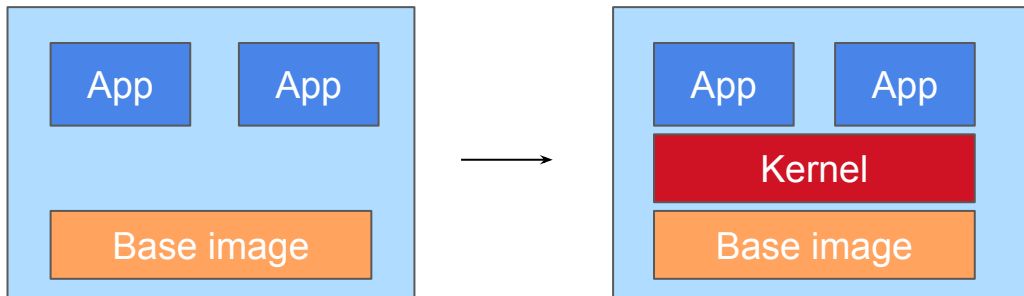
KubeCon



CloudNativeCon

Europe 2026

- bootable container images, with a kernel & init system
- Trusted Execution Clusters relies on nodes booted with a bootable container image



What's next



KubeCon



CloudNativeCon

Europe 2026

- Currently focusing on Azure
- Support of various cloud providers,
 - GCP and AWS
- Support for virtualization platform for bare metal deployments
 - KubeVirt
- Support generic TPM attester with the attestation key (AK) and verification of the AK is signed by the TPM endorsement key
- Move to UKI (Unified Kernel Image) for the guest

What's next



KubeCon



CloudNativeCon

Europe 2026

- Protection of the ignition and kubeconfig configuration with a double attestation
- Integrate attestation with the node approval
 - Protecting the CSR with attestation
- Bootstrapping the cluster, attestation of the first node
- Move the operator in-cluster once first control plane is ready

Conclusions

- How to automate the process with the Trusted Execution cluster operator
- The Trusted Execution Cluster operator
 - Ensures that the nodes are confidential
 - Coordinates the machines joining the clusters
 - Calculates the reference values
 - Deploys and maintains the Trustee, the security policies and the secrets

References

- [Trusted Execution Cluster organization](#)
- [Blog post about Trusted Execution Clusters](#)
- [UKI, composefs and remote attestation for Bootable Containers](#)
- [Bootable containers](#)
- [Confidential containers](#)
- [Linux TPM PCR Registry](#)
- [Demo setup](#)



KubeCon



CloudNativeCon

Europe 2026





KubeCon



CloudNativeCon

Europe 2026

Questions?

