KUBECON + CLOUDNATIVECON NORTH AMERICA 2026

Legacy-Free, Zero-Maintenance Bare Metal Kubernetes Clusters

With RISC-V and Immutable Linux



Felicitas Pojtinger · LiveKit

PROBLEM

Every layer has a vendor

ISA	Firmware	Image	Cluster	Identity	Repair

RISC-V

ISA

Open

Small base, optional extensions

PROFILE

RVA23

Required extensions for application processors

LICENCE

Royalty-free

No licence fee

OVERVIEW

Six layers

01

Silicon

One image on K3 and QEMU

02

Enablement

Blank board to desktop

03

Firmware

Signed payload, one boot

04

Image

UKI, A/B, rollback

05

Cluster

Forgejo on two nodes

06

Trust

Mutual attestation

SpacemiT K3

RVA23 certified

8
X100 RISC-V cores

8
A100 AI cores

60
TOPS

130
KDMIPS

18–35
W

LPDDR5
6400, UFS, NVMe



One image on K3 and QEMU

Signed UKI, measured from SPL

HARDWARE

SpacemiT K3

k3s agent

DEVELOPMENT

QEMU

`rva23s64` CPU model

k3s server

Pushrod

AGENT INTERFACE

MCP server

RELAY

dcttech, 4 channels

UART

CH343

KVM

NanoKVM-USB

FLASHER

BROM, fastboot

JTAG

In progress

TBD

Bring-up from a blank board

BROM FDL → FSBL → U-Boot → EDK2 → OS

RELAY

Reset, FDL

```
target.reset
target.enterFDL
```

FLASHER

Write image

```
flash.stage
flash.continue
```

UART

First boot

```
serial.readFrom
```

DEMO 1

DEMO

Blank board to desktop

01

Enter FDL

02

Flash

03

First boot

DEMO 2

DEMO

Agent uses the desktop

01

Add top bar item

02

Restart Weston

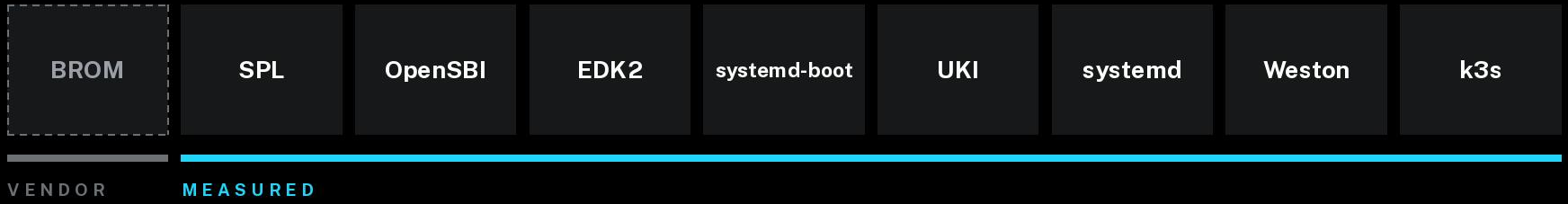
03

Click item

04

Read PCRs

Boot chain


BROM
SPL
OpenSBI
EDK2
systemd-boot
UKI
systemd
Weston
k3s
VENDOR
MEASURED

DEMO 3

DEMO

Signed payload, one boot

01

Patch

02

Sign

03

Boot once

04

Back to UKI

OS image

7.3.1
Linux

262.1
systemd

EROFS
/usr

BUILD

Buildroot

UKI

Signed

Kernel, initramfs, command line, OS metadata

A/B

systemd-sysupdate

dm-verity on /usr, rollback after 3 failed boots

EXTENSIONS

sysext

Signed, k3s included

Two-node k3s

k3s as a signed sysext

K3S SERVER

QEMU

K3S AGENT

SpacemiT K3

`forgejo` Deployment, Service

DEMO 4

DEMO

Forgejo on two nodes

01
Nodes

02
Deploy

03
Pod on K3

04
Request

Reports

PCR 11



UKI

PCR 13



Sysexts

SYSTEMD-REPORT



JSON-SEQ

With TPM quote

NONCE



Fresh per quote

Receiver checks signature

Reports: evidence for the admin

Wallet consent: evidence for the client

DEMO 5

DEMO

Admin report

01

Upload

02

Inspect

Consent tiers

The client always verifies the full K3 server chain

TIER 0 · SMALL-PAYMENT

200 CAD

250 CAD per day

TPM AK

TIER 1 · DEVELOPMENT-PAYMENT

300 CAD

1,000 CAD per day

Smart card or FIDO2

Full client report

TIER 2 · MORTGAGE

No payment

Host OS report

or smart card

Example limits

DEMO 6

DEMO

Mutual attestation

01

Verify server

02

Tier 0

03

Tier 1

04

Tier 2

05

Replay



Mutual attestation

DIRECTION · CONTRACT	PROOF
Client to server `all`	Full K3 host OS chain
Server to client `small-payment`	TPM AK
Server to client `development-payment`	TPM AK, smart card or FIDO2, client report
Server to client `mortgage, host`	TPM AK, client report
Server to client `mortgage, card`	TPM AK, smart card or FIDO2

Tier 2 without OS report

SMART CARD OR FIDO2

User presence

TPM AK

Key residency

SERVER

Accepts consent proof

In place of the OS report

TEE

TBD

Medium assurance without user presence

DEMO 7 · STRETCH

DEMO

CRIU migration, QEMU to K3

01

Checkpoint

02

Copy

03

Restore

04

Switch

SUMMARY

Results

01	**Silicon**	One image on K3 and QEMU
02	**Enablement**	Blank board to desktop
03	**Firmware**	Signed payload, one boot
04	**Image**	UKI, A/B, rollback
05	**Cluster**	Forgejo on two nodes
06	**Trust**	Mutual attestation

LIMITS

Open gaps

BROM



Vendor code

Unmeasured

K3 PORT



Downstream patches

Small, shrinking

TEE



TBD

Thank you



Felicitas Pojtinger

LiveKit

WEB	felicitas.pojtinger.com
MASTODON	@pojntfx@mastodon.social
BLUESKY	@felicitas.pojtinger.com
LINKEDIN	linkedin.com/in/pojntfx
CODEBERG	codeberg.org/pojntfx
GITHUB	github.com/pojntfx

TBD

CODE

Pushrod

codeberg.org/pojntfx/pushrod

LIVEKIT BOOTH 254

Careers

livekit.com/careers

SESSIONIZE

Feedback

TBD