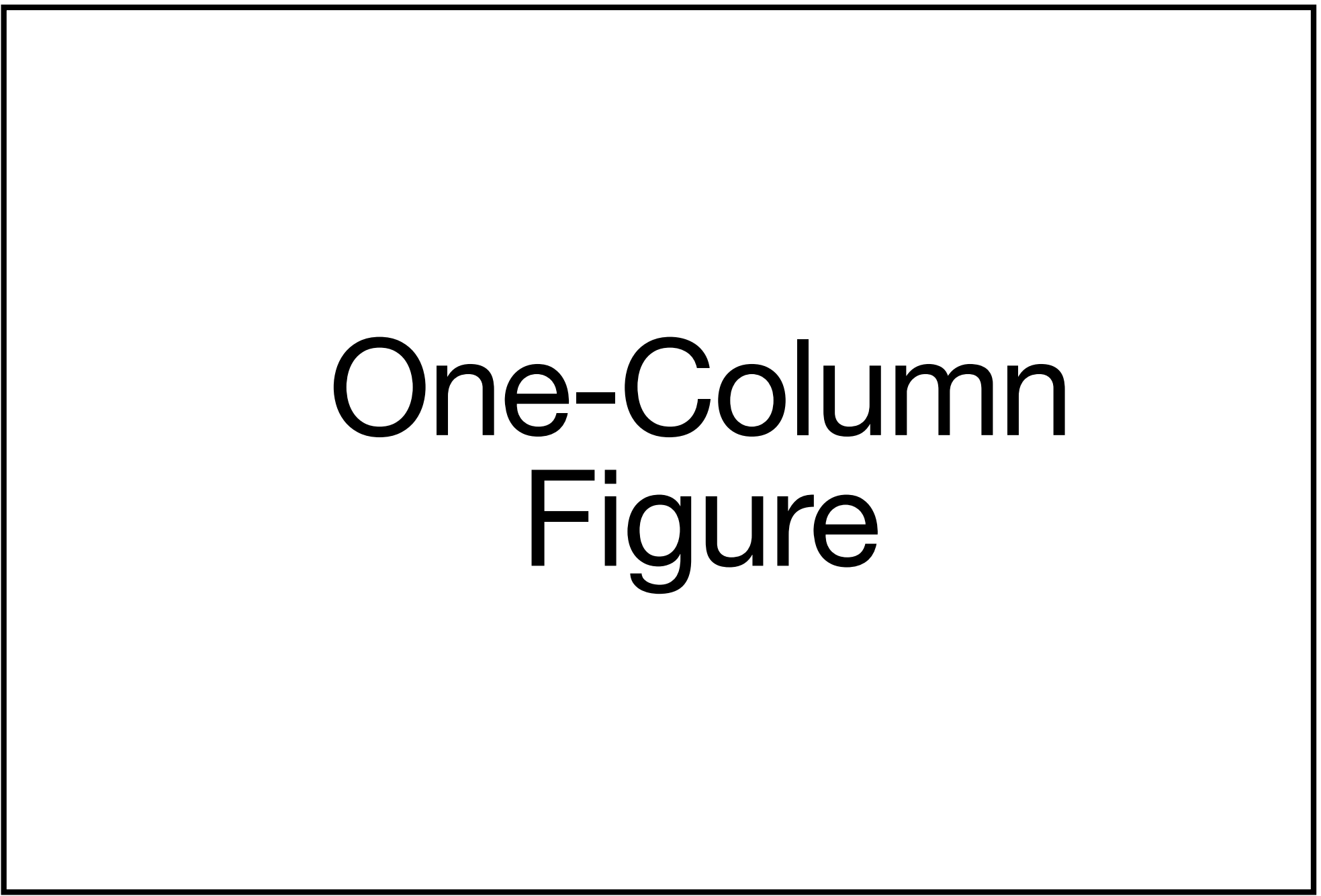
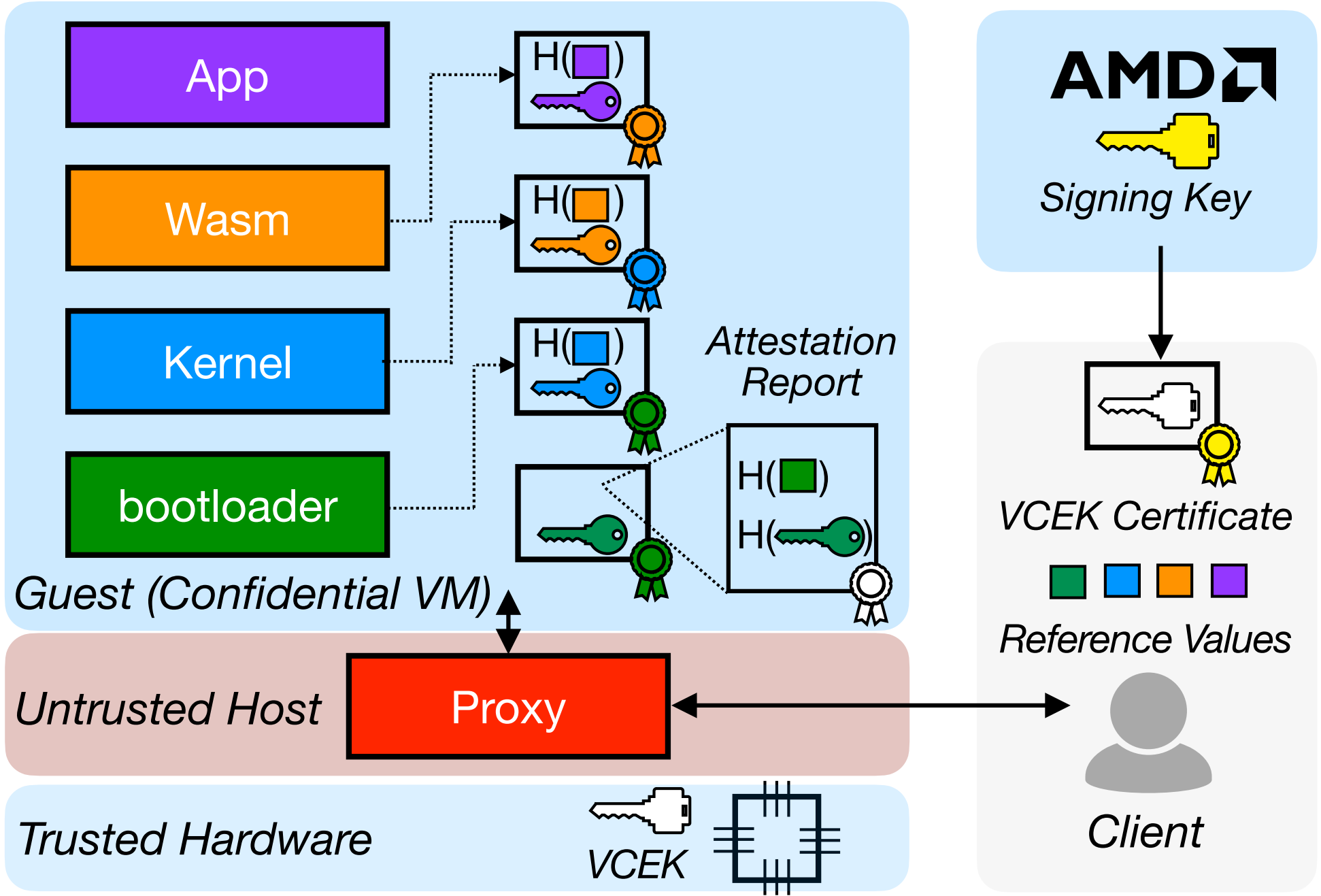
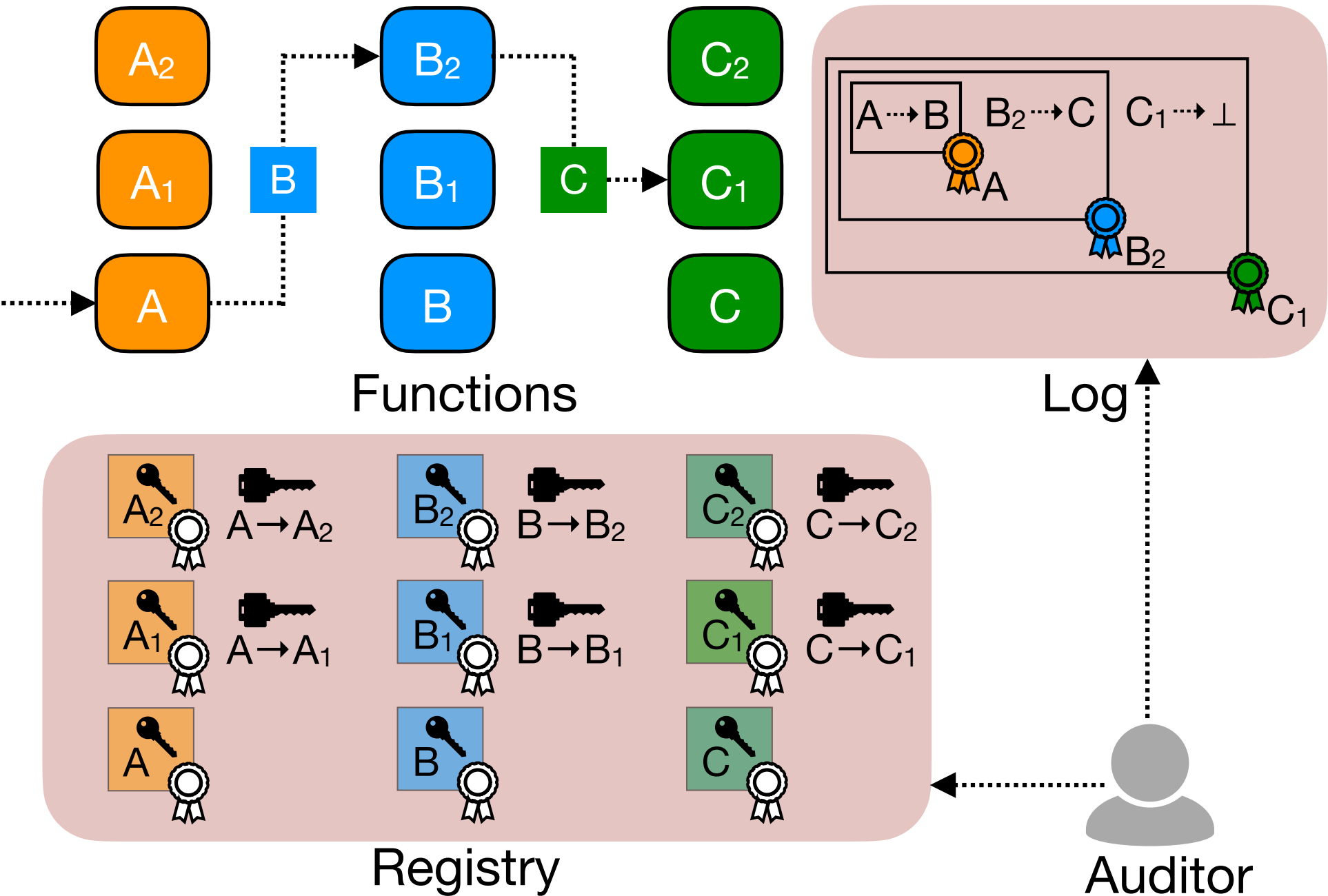
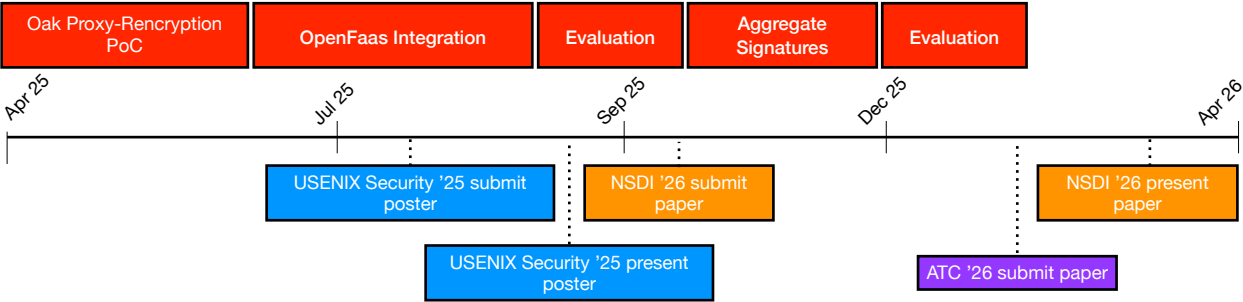
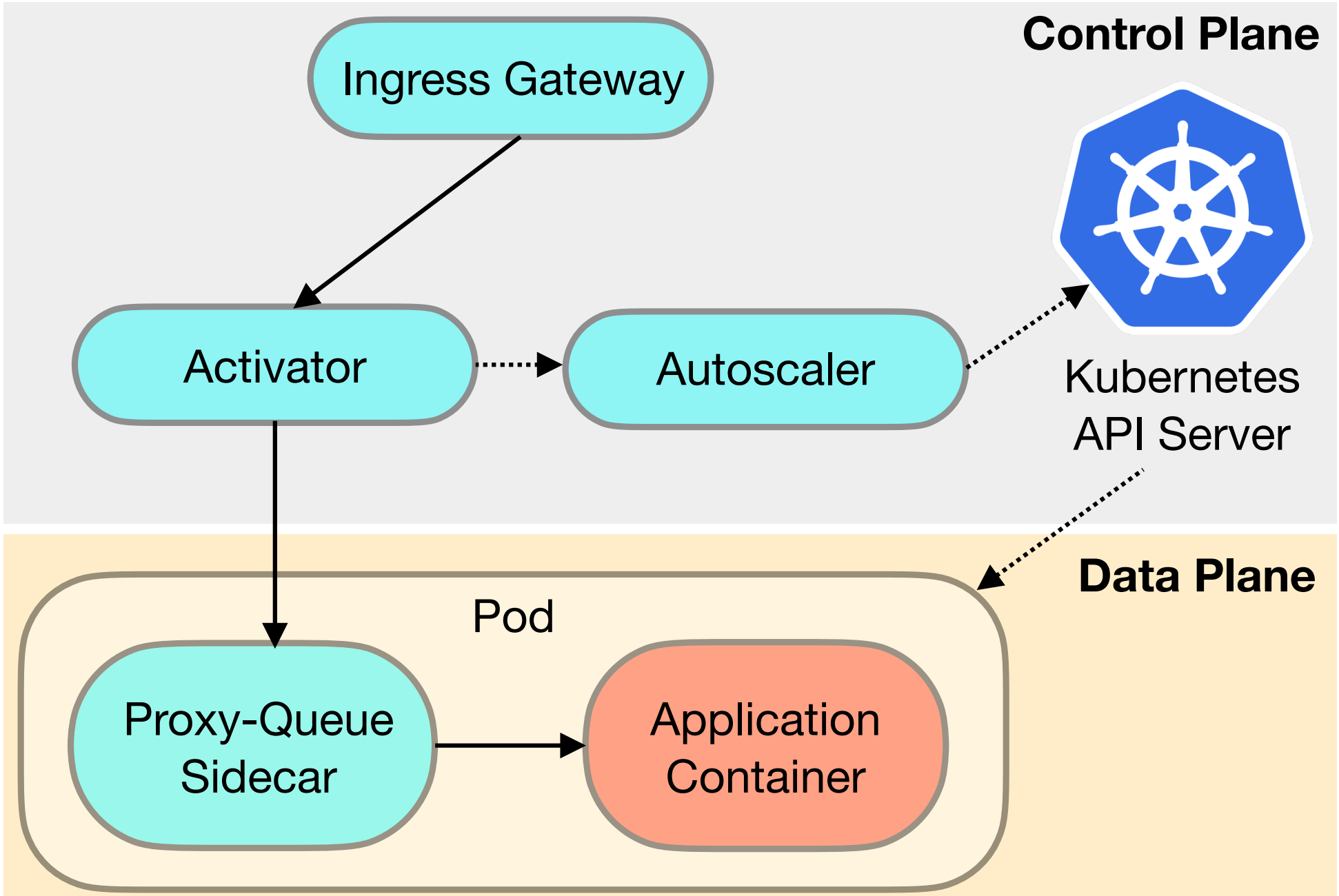

One-Column
Figure

Two-Column Figure

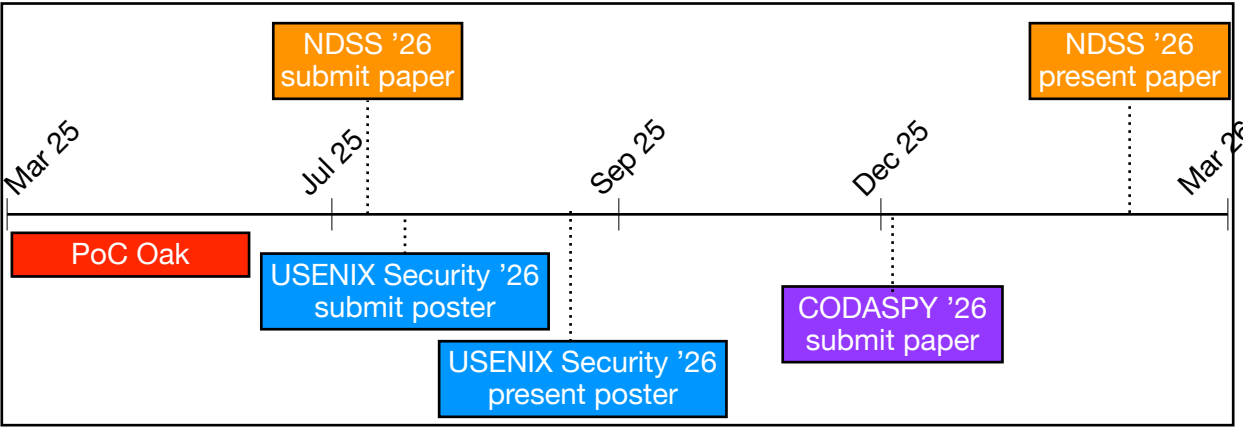

App
Wasm
Kernel
bootloader
H(■)
H(■)
H(■)
H(■)
H(■)
Attestation Report
Guest (Confidential VM)
Untrusted Host
Proxy
Trusted Hardware
VCEK
AMD
Signing Key
VCEK Certificate
Reference Values
Client


A2
A1
A
B
B2
B1
B
C2
C1
C
Functions
A→B
B2→C
C1→⊥
A
B2
C1
Log
A→A2
B→B2
C→C2
A→A1
B→B1
C→C1
Registry
Auditor


Oak Proxy-Rencryption PoC
OpenFaas Integration
Evaluation
Aggregate Signatures
Evaluation
Apr 25
Jul 25
Sep 25
Dec 25
Apr 26
USENIX Security '25 submit poster
NSDI '26 submit paper
NSDI '26 present paper
USENIX Security '25 present poster
ATC '26 submit paper


Control Plane
Ingress Gateway
Activator
Autoscaler
Kubernetes
API Server
Data Plane
Pod
Proxy-Queue
Sidecar
Application
Container

Scratch Slides


NDSS '26
submit paper
NDSS '26
present paper
Mar 25
Jul 25
Sep 25
Dec 25
Mar 26
PoC Oak
USENIX Security '26
submit poster
USENIX Security '26
present poster
CODASPY '26
submit paper