CONFIDENTIAL COMPUTING SUMMIT 2026

Hosted by THE LINUX FOUNDATION + OPAQUE

Realizing Confidential VMs Ensuring Privacy of AI Features at LY Corporation in a Real-World Cloud

Hiroki Narukawa, Akihiro Misawa

LY Corporation

Speakers

Hiroki Narukawa LY Corporation

Mainly working on software running inside hypervisors including low-layer.

Akihiro Misawa LY Corporation

Infrastructure engineer focused on server OS operations and automation tool development.

Agenda

- Our Goal: ensuring better privacy in LINE AI
- Security model realized in our Confidential VMs
- Implementation of Confidential VMs in our private cloud with OpenStack
- Application deployment: how we keep service application trusted

Agenda

- **Our Goal: ensuring better privacy in LINE AI**
- Security model realized in our Confidential VMs
- Implementation of Confidential VMs in our private cloud with OpenStack
- Application deployment: how we keep service application trusted

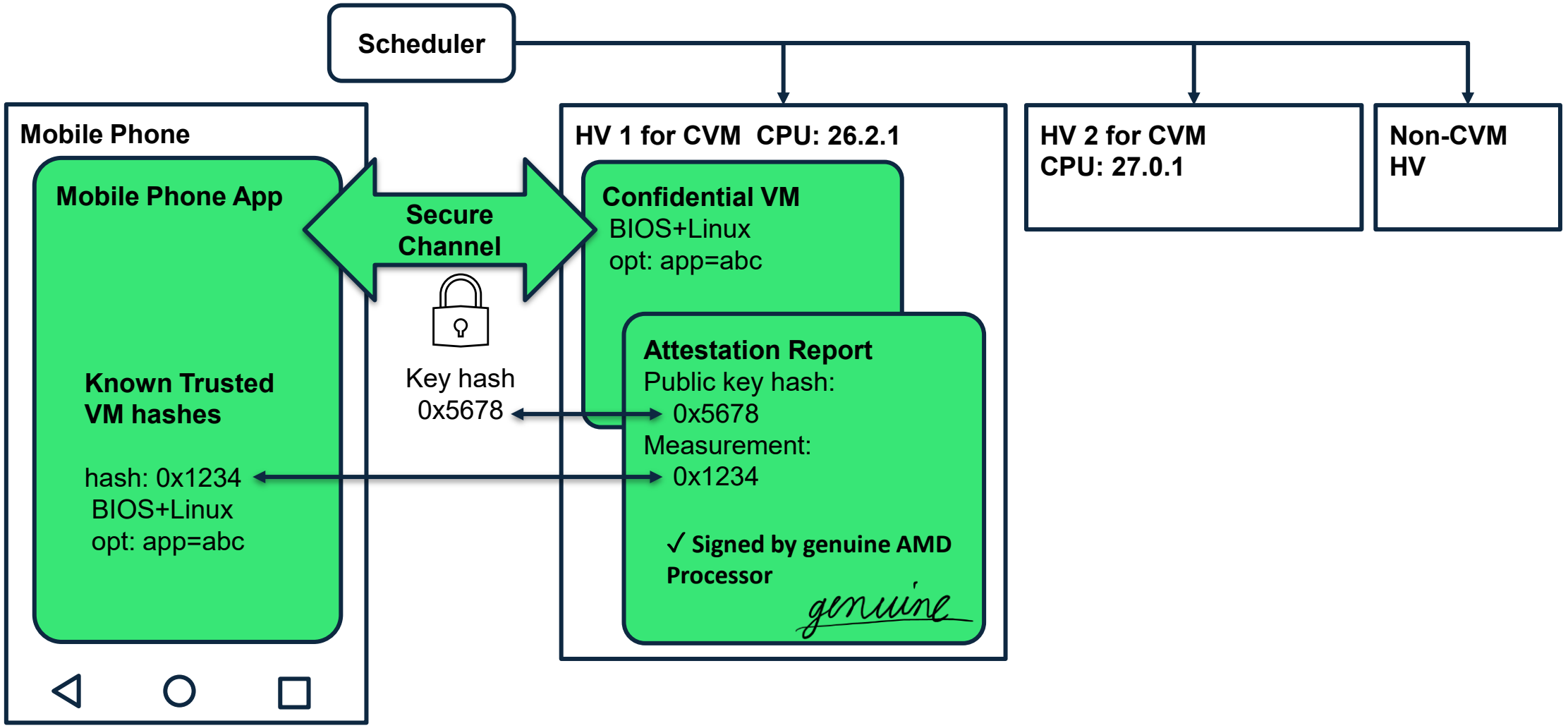
Our goal: Privacy in AI features

- LINE: messaging app service with 194 million active users
- LINE provides services that use AI, and some of these services handle private user information.
- Processing such data on a cloud platform requires a high level of security.
- We introduced Confidential VM feature to improve security.

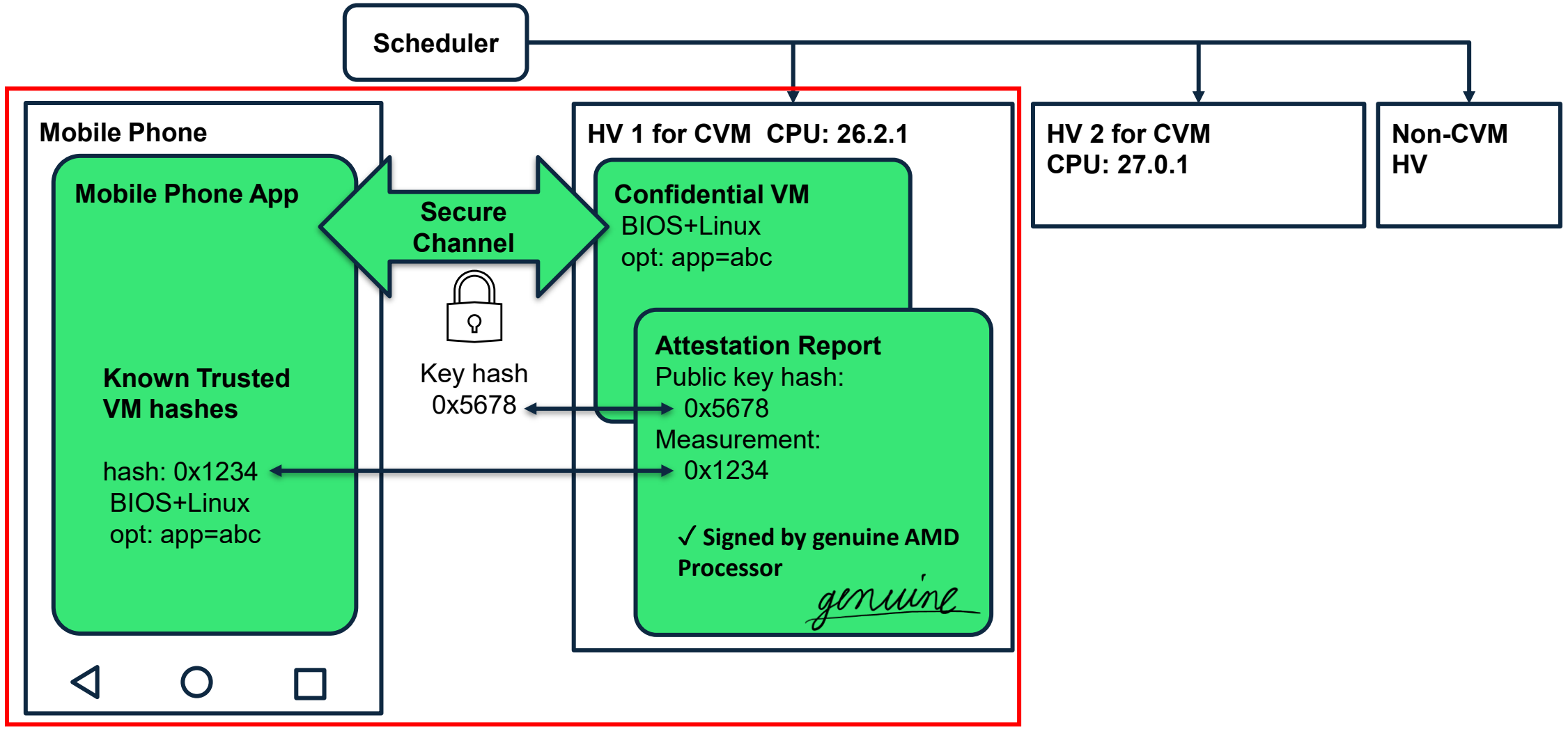
Agenda

- Our Goal: ensuring better privacy in LINE AI
- **Security model realized in our Confidential VMs**
- Implementation of Confidential VMs in our private cloud with OpenStack
- Application deployment: how we keep service application trusted

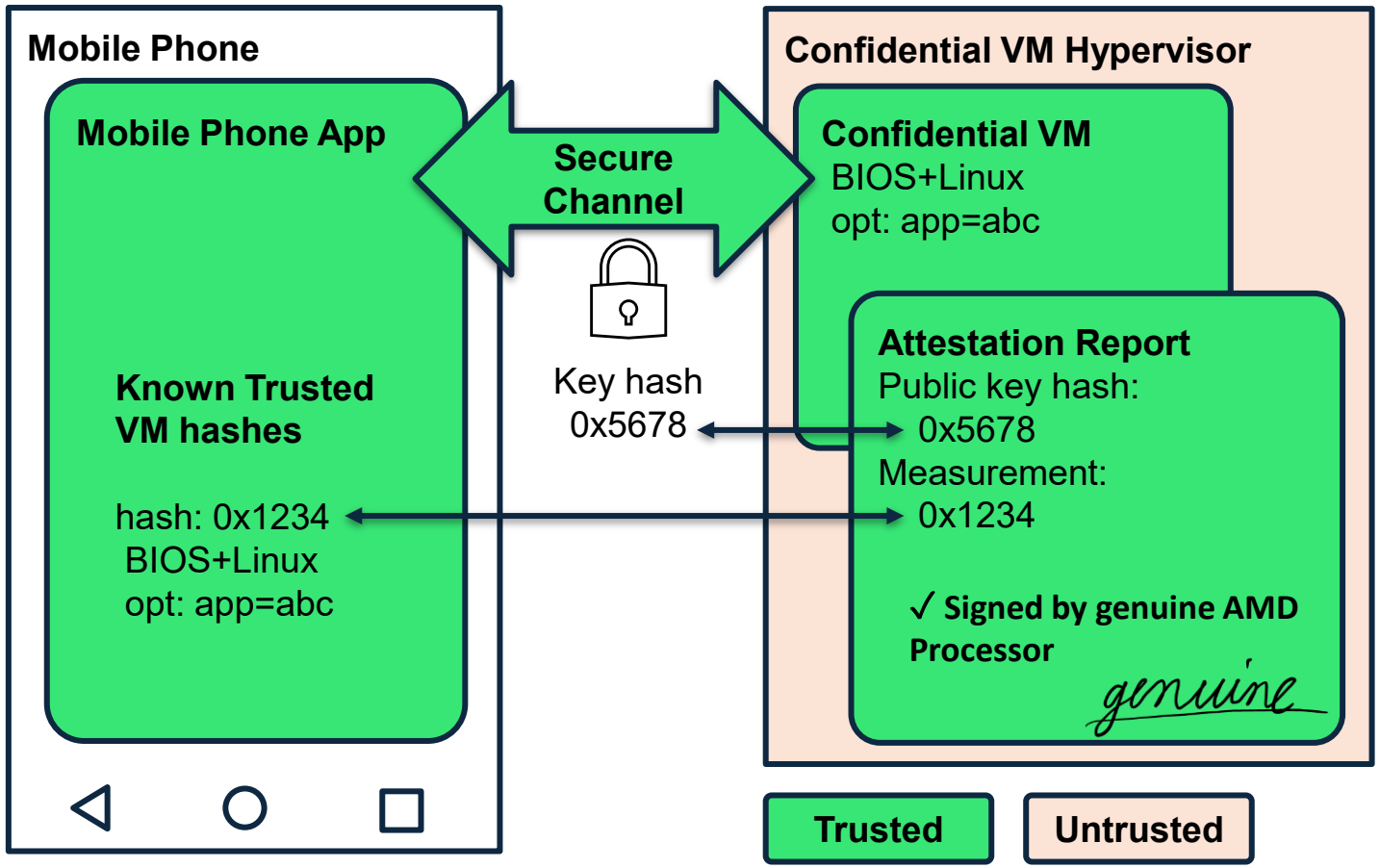
System Configuration



System Configuration

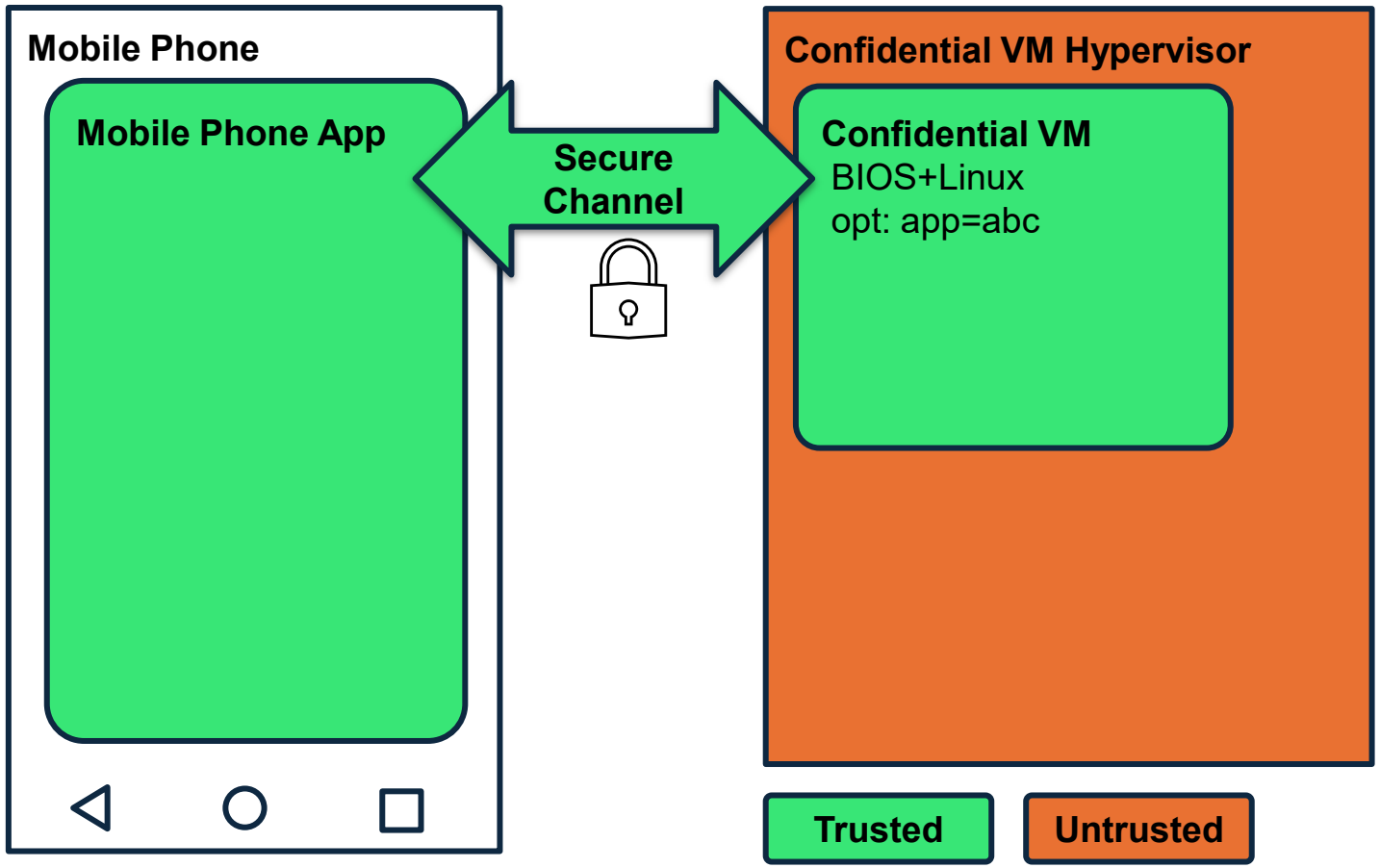


Securely sending information to CVM



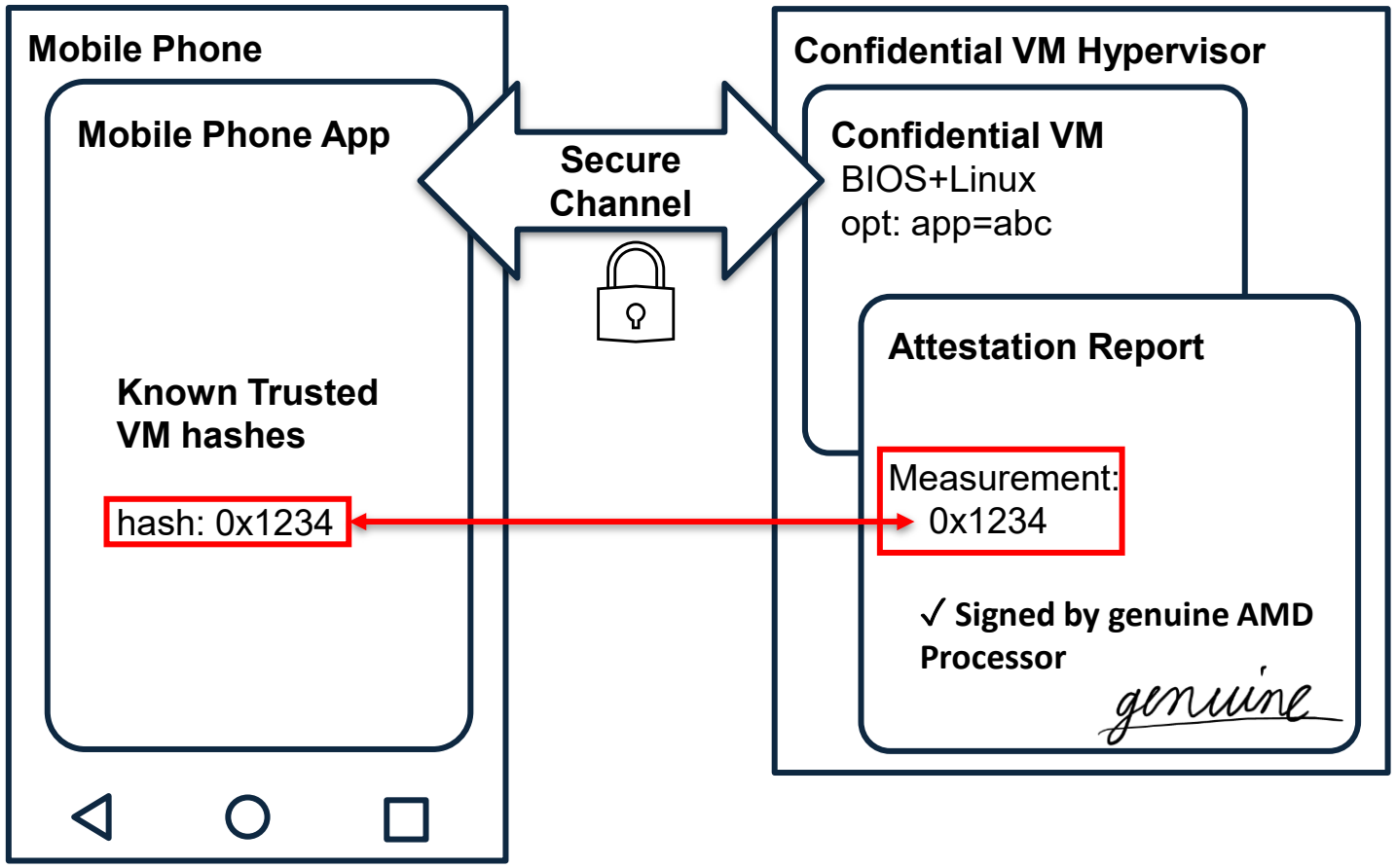
- Goal: client app can send private information to Confidential VM via secure channel

Security model which does not trust HVs



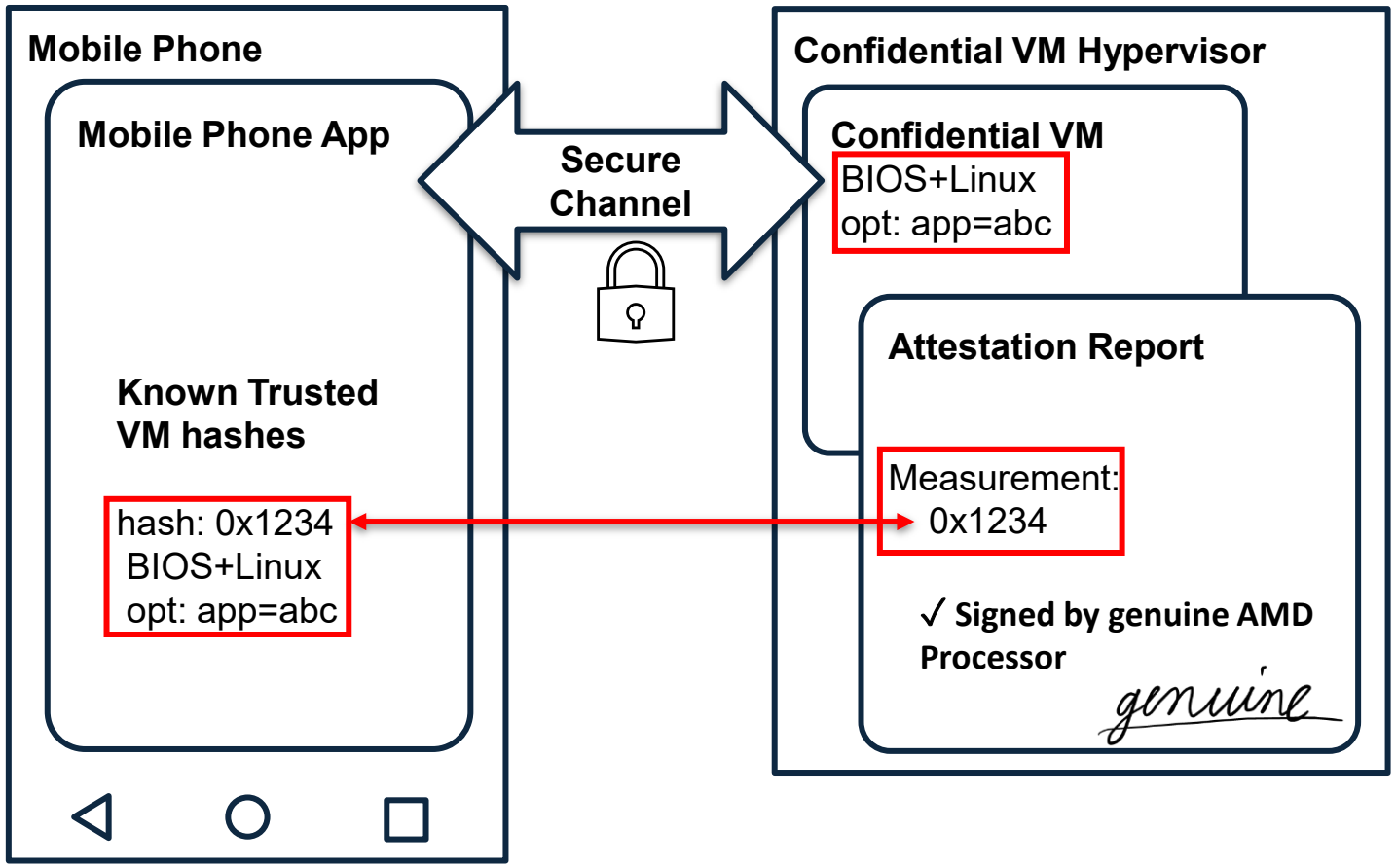
- Basic idea is that client app can establish secure channel to Confidential VM.
- Even employees of LY Corporation should not be able to read the private information

What Attestation Report shows



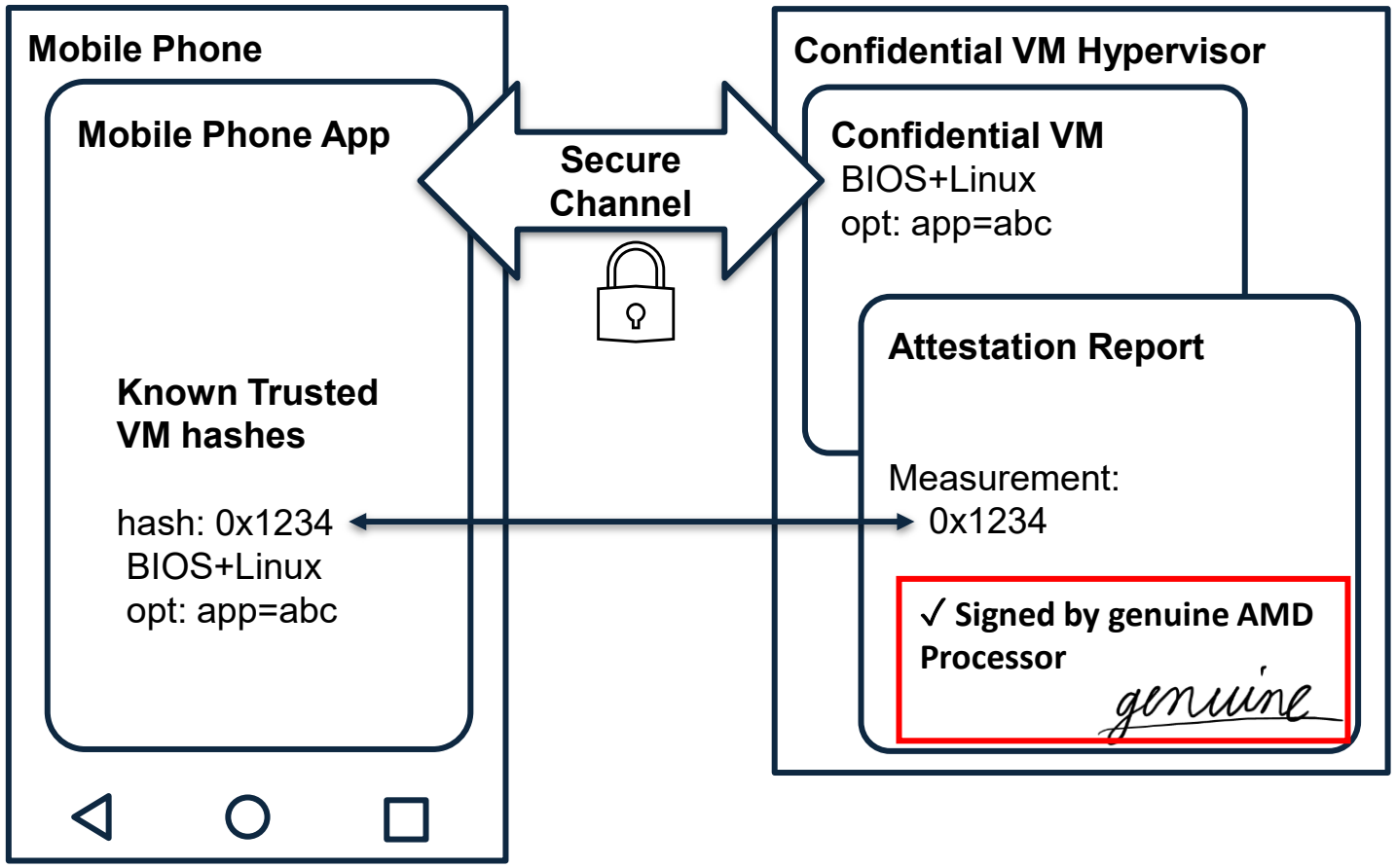
- Attestation Report includes:
  - Measurement: SHA384 hash value of memory loaded when VM is booted

What Attestation Report shows



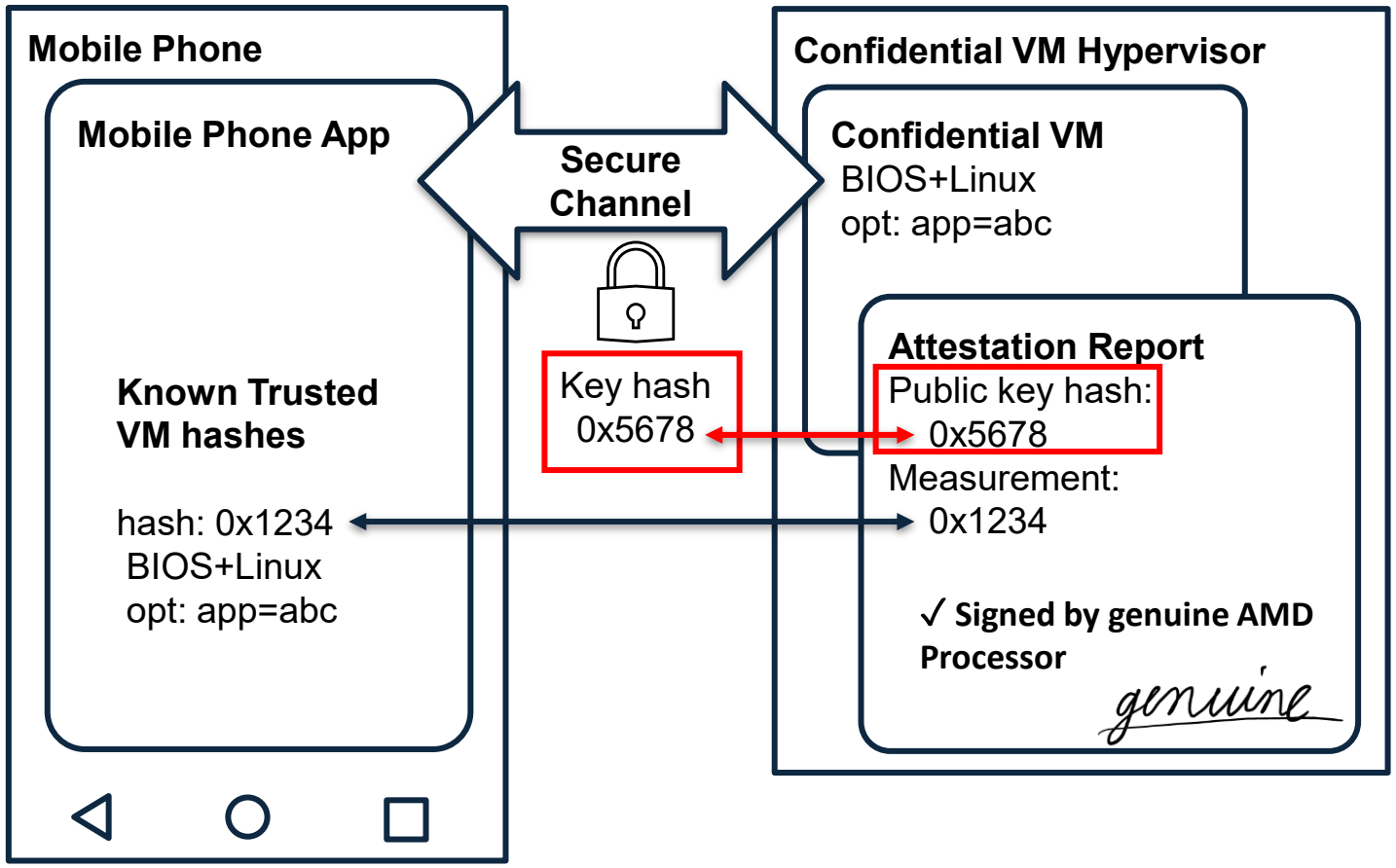
- Direct kernel boot: kernel and kernel options are expanded before starting VM.
- Following are attested by Attestation Report:
  - OVMF (VM BIOS)
  - Kernel, initrd
  - Kernel options

Why can client trust Attestation Report?



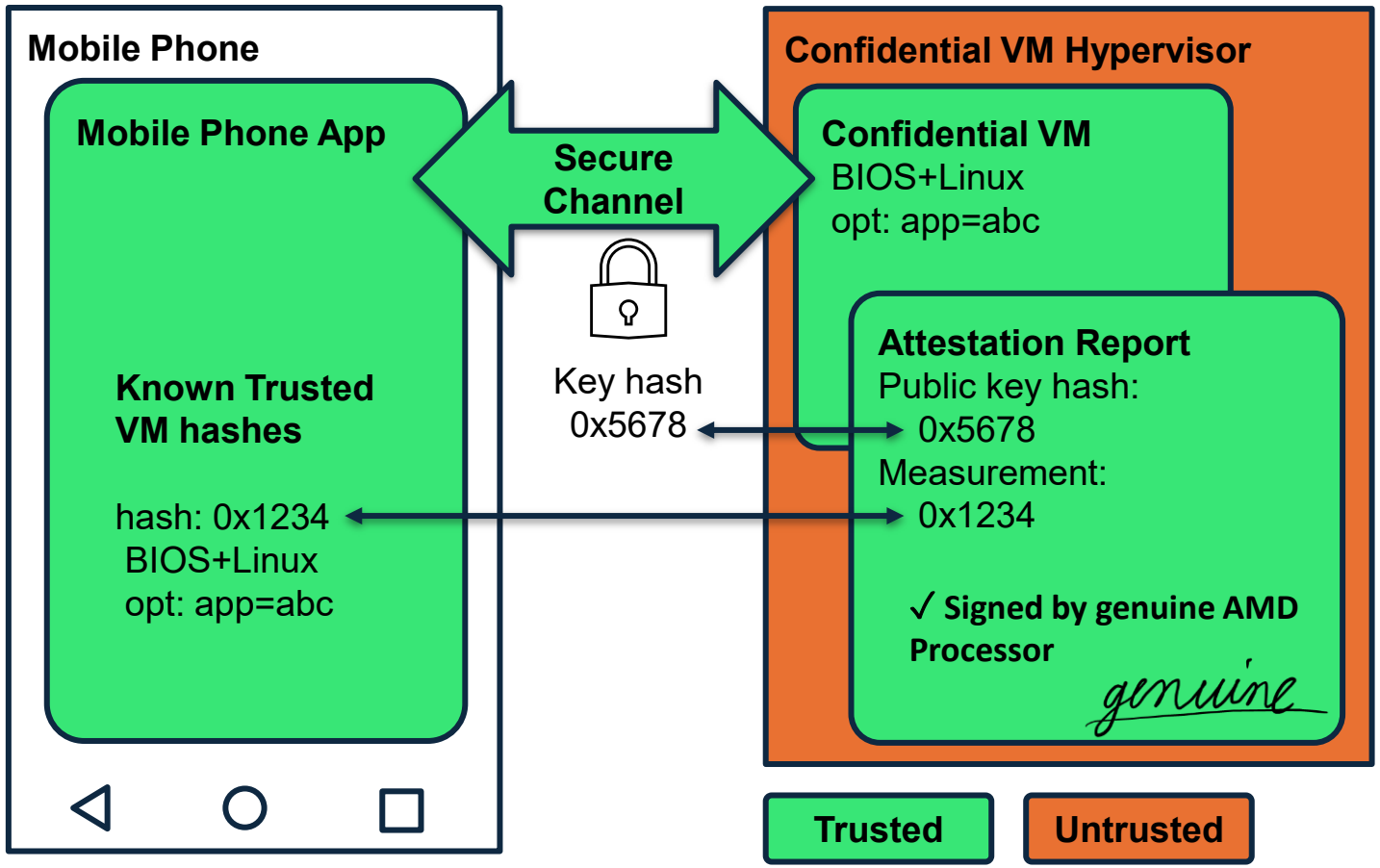
- Attestation Report is signed by genuine AMD Secure Processor and can be verified using AMD certificate chain.

Why can mobile app trust the server?



- Attestation Report includes:
  - A hash of public key for VM application
    - Report data: arbitrary 64-byte data requested by VM, with typical usage of public key hash

Client can establish secure channel with trust



- By this configuration, client can establish secure channel to Confidential VM with:
  - Genuine AMD CPU
  - Known BIOS
  - Known kernel
  - Known kernel options

Agenda

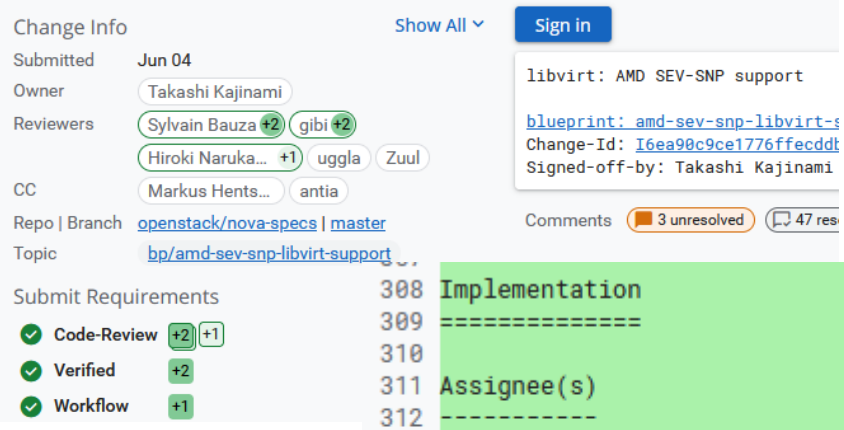
- Our Goal: ensuring better privacy in LINE AI
- Security model realized in our Confidential VMs
- **Implementation of Confidential VMs in our private cloud with OpenStack**
- Application deployment: how we keep service application trusted

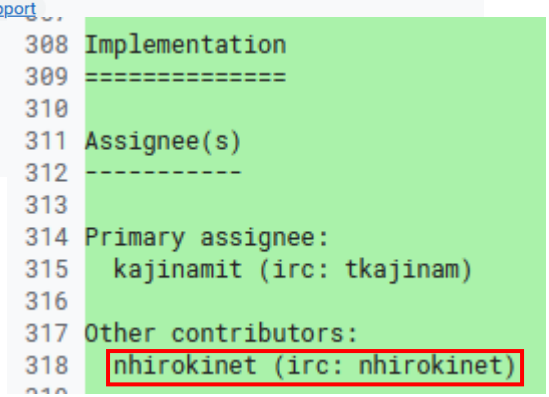
Implementation into our OpenStack cluster

1. SEV-SNP support
2. Kernel options in Direct Kernel Boot
3. VM scheduling to guarantee verification

1. SEV-SNP support

- We implemented SEV-SNP support in our private cloud.
- We are also contributing to OpenStack Nova.
  - LY Corporation member has been assigned as contributor and pushed PoC.





Subject	Owner
SEV-SNP PoC: os_loader_type 'rom' instead of 'pflash' if SEV-SNP	Hiroki Naruka...
SEV-SNP PoC: add SEV-SNP launch_security to libvirt driver	Hiroki Naruka...
SEV-SNP PoC: split libvirt config SEV-ES as another class	Hiroki Naruka...
SEV-SNP PoC: Add SEV_SNP to MemEncryptionModel object	Hiroki Naruka...
SEV-SNP PoC: scheduler translates SEV-SNP request	Hiroki Naruka...
SEV-SNP PoC: libvirt driver to report SEV-SNP trait in sev_es RP	Hiroki Naruka...
SEV-SNP PoC: libvirt host to check SEV-SNP availability	Hiroki Naruka...

2. Kernel options in Direct Kernel Boot

Direct Kernel Boot was supported by OpenStack, but…

- Kernel options are bound property of each VM image
  - Our Confidential VM: VM users can add application-related options
  - Combines options from IaaS operator and options from VM users.
- OpenStack kernel options have 255 characters limit
  - Extended to support more than 256 characters, and we plan to upstream it to OpenStack Nova.

```
OS Image:
 os_command_line='roothash=12ab'
```

```
VM:
  cmdline='container=34cd'
```

```
cmdline: roothash=12ab container=34cd  (can be >255 chars)
```

3. VM scheduling to guarantee verification

- Certificate chain for each CPU generation (like Turin)
  - AMD certificate chain is provided per generation, so verification fails if changed unexpectedly.
- Measurement is affected by vCPU model (CPUID like family=26, model=2, stepping=1)
  - In “passthrough” mode, the model of vCPU is the same as the host CPU

Flavor includes CPU ID to guarantee Measurement.

```
Flavor 8vCPU_16GiB_10GiB.CVM_CPU_AMD_26_2_1

  trait:HV_AMD_CPU_ID_26_2_1='required'
```

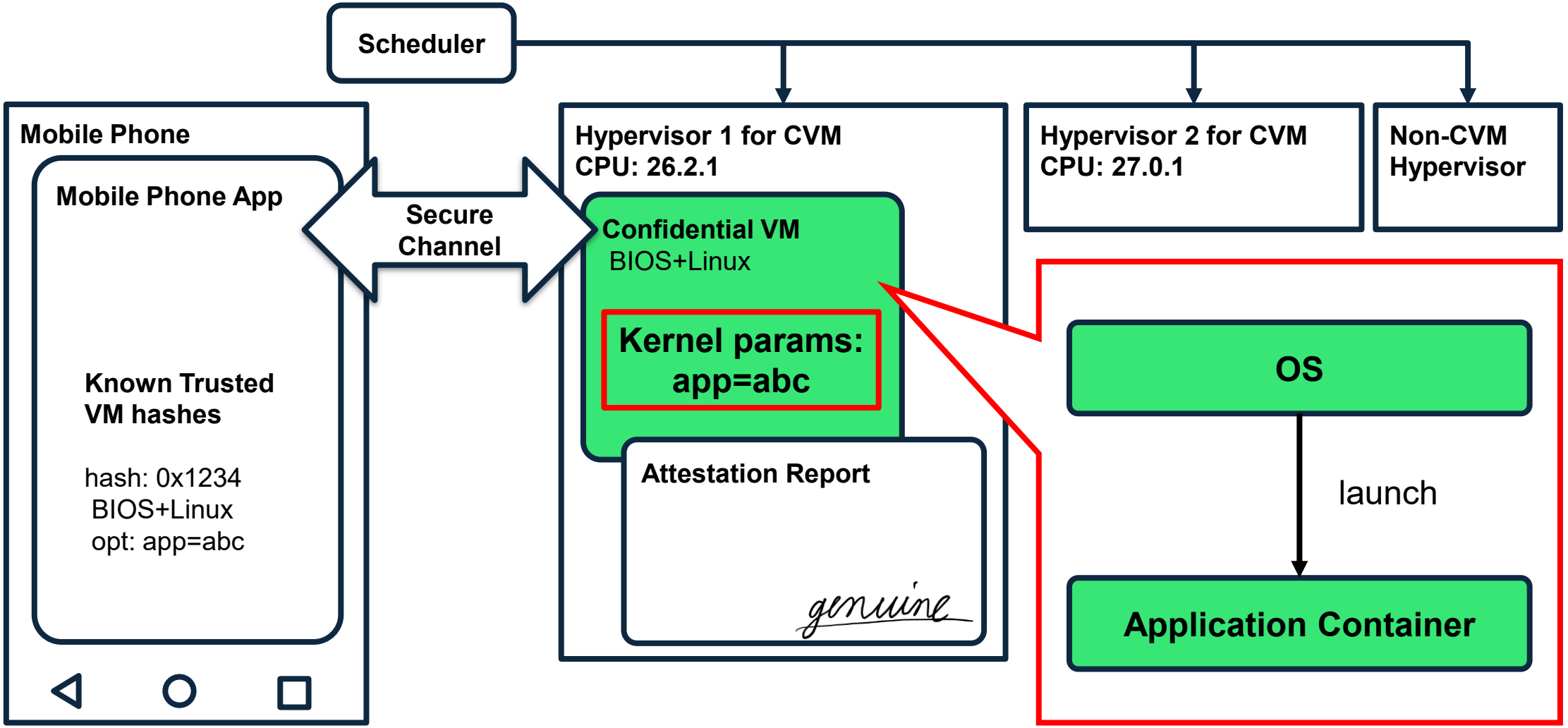
Our Confidential VMs in OpenStack

- SEV-SNP supported (planned to be upstreamed to OpenStack)
- Kernel options in direct kernel boot
  - Combines options from IaaS operators and options from VM users
  - Supports kernel options longer than 255 characters (planned to be upstreamed to OpenStack)
- VM users can control when the Measurement changes, while IaaS operators can deploy new hypervisors at any time
  - VM users can pin CPU generation and CPUID just by choosing flavor

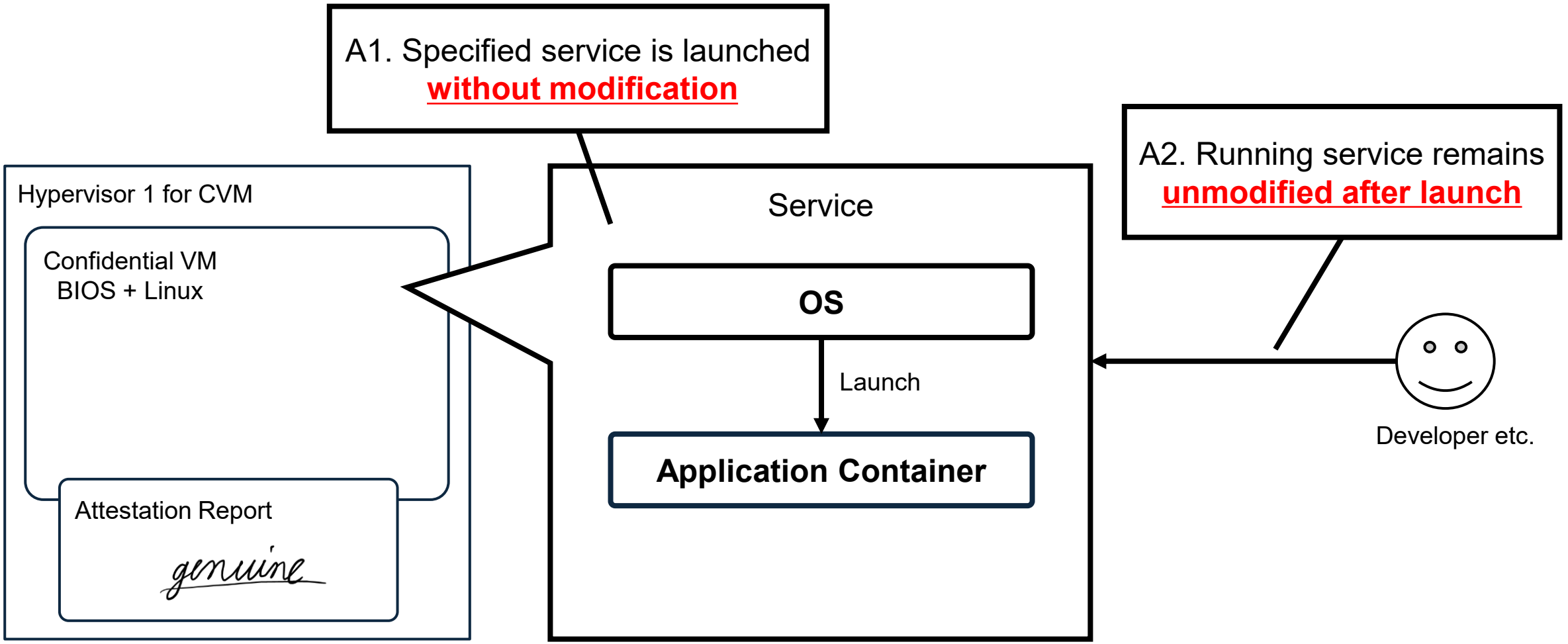
Agenda

- Our Goal: ensuring better privacy in LINE AI
- Security model realized in our Confidential VMs
- Implementation of Confidential VMs in our private cloud with OpenStack
- **Application deployment: how we keep service application trusted**

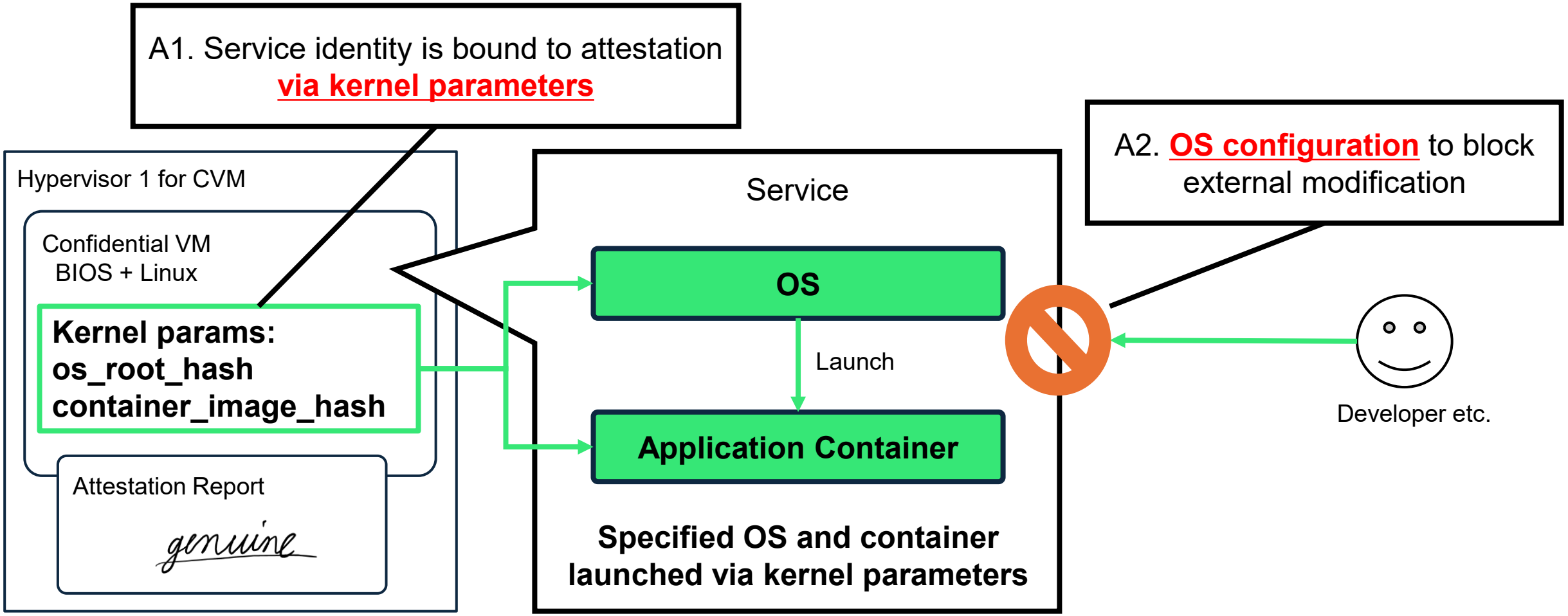
System Configuration



What is a trusted service state?

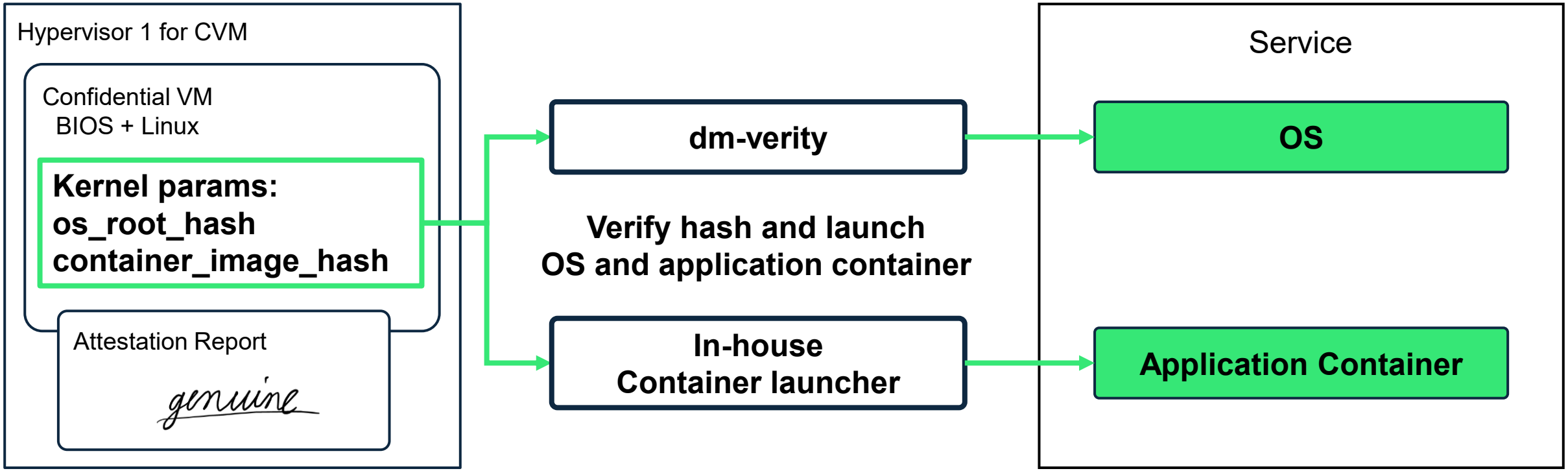


How can we trust a service running in a CVM?



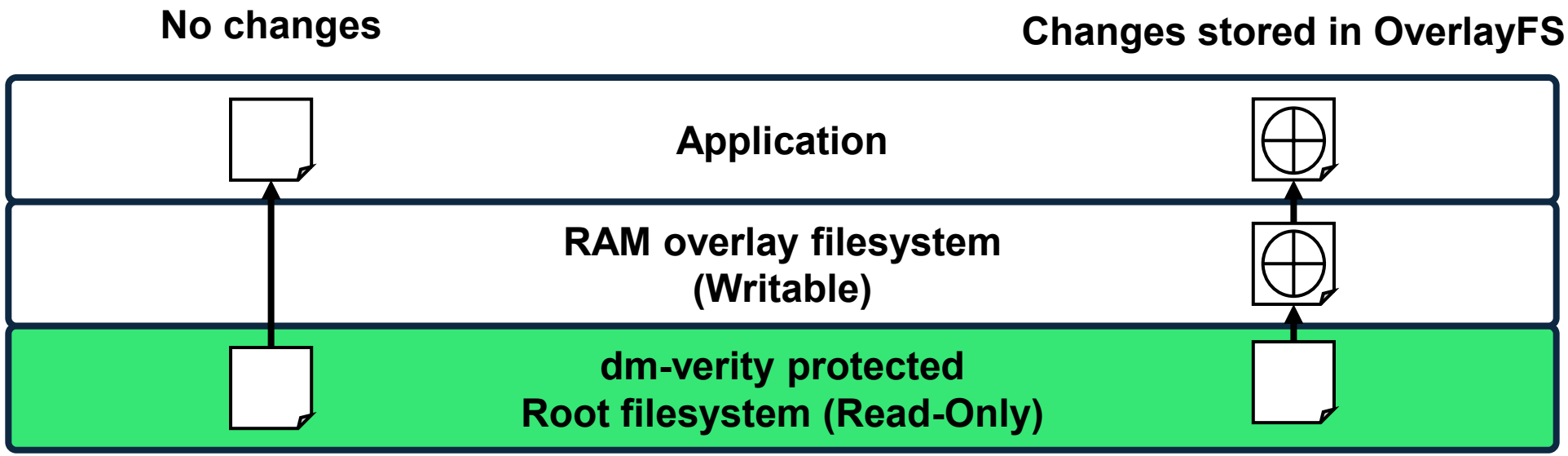
Specifying and launching the OS and service app

- Kernel params contain hashes identifying the OS and service app.
  - OS state hash: dm-verity
  - Service app container image hash: in-house container launcher



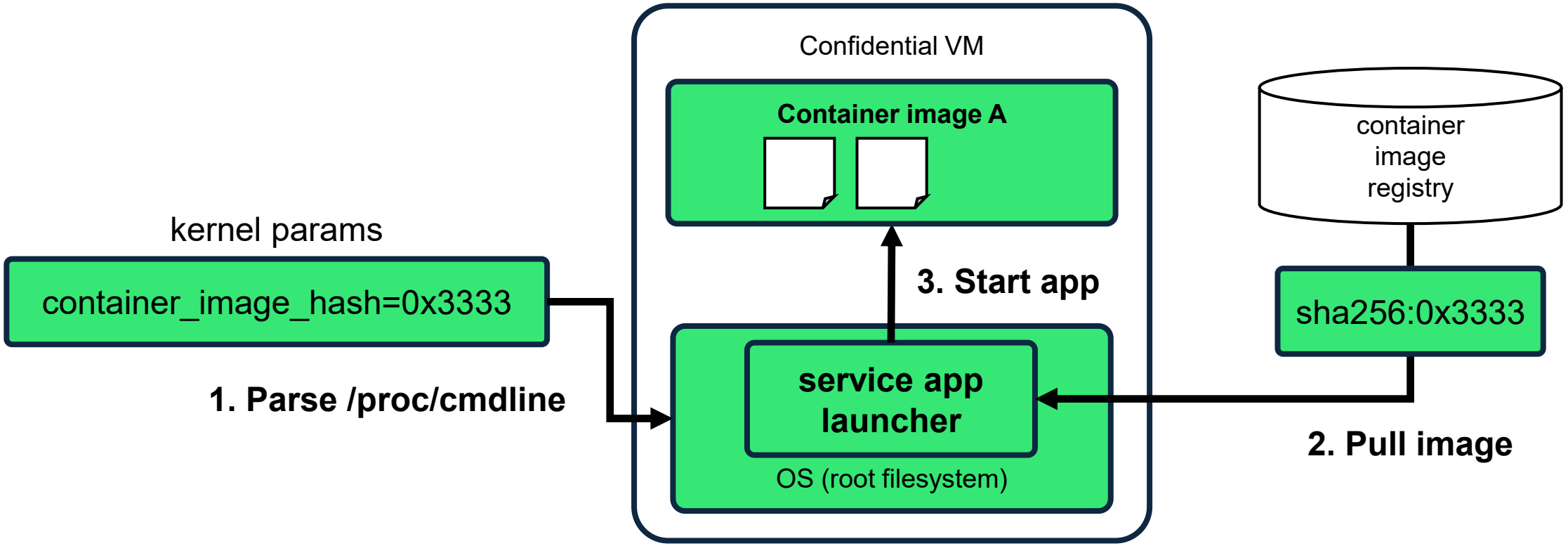
Immutable root filesystem, writable runtime state

- The root filesystem is verified by dm-verity and mounted read-only.
- Runtime writes are redirected to a RAM-backed OverlayFS layer.



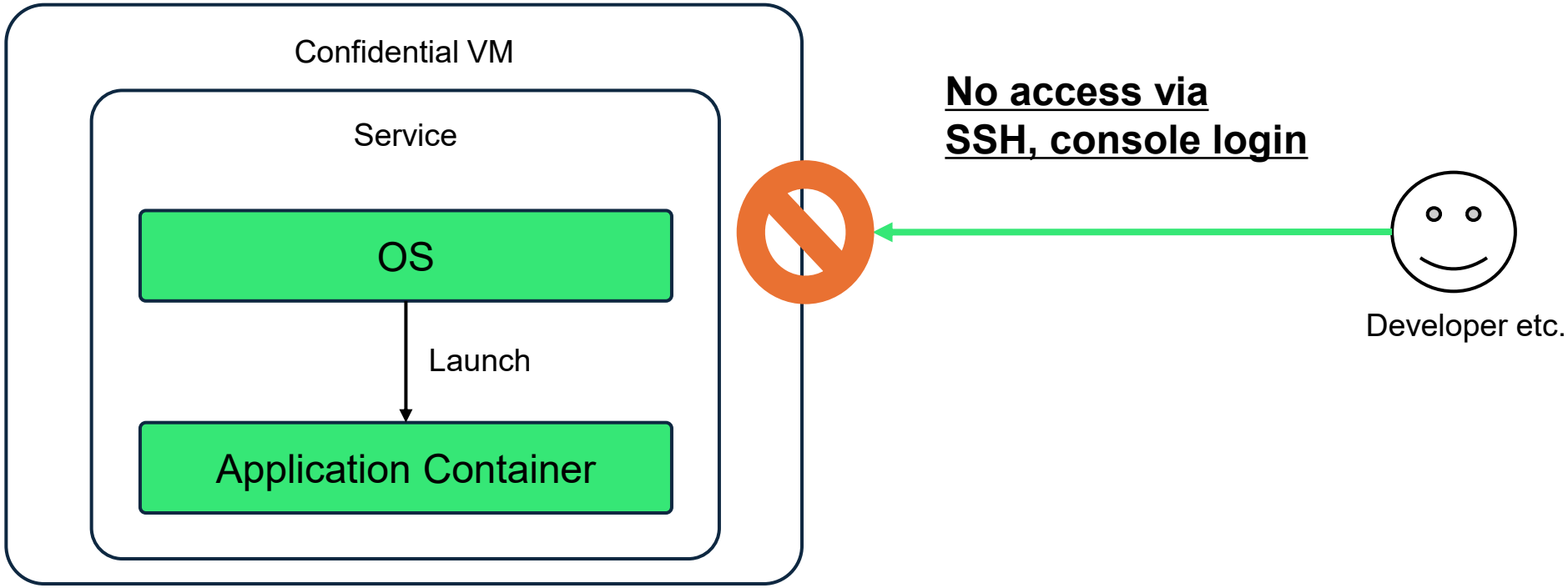
In-house container launcher

- The in-house launcher retrieves and launches the container specified in kernel parameters



Preserving OS and service app integrity

- Prevent modification of the OS and service app after startup.
  - SSH login disabled
  - Console login disabled



Summary

- SEV-SNP Attestation Reports enable secure communication with Confidential VMs
- Implemented SEV-SNP Confidential VM support for OpenStack and contributed it upstream
- Extend attestation-based trust from the Confidential VM to the application container
- Cloud users can deploy containers with minimal configuration, while still benefiting from Confidential VM attestation.