Secure Over-the-Air Updates Designed for the Automotive Industry.

01 June 2017.

Advanced Telematic SYSTEMS

I

Introduction
ATS Advanced Telematic Systems.

Moving toward Open Mobility.

German automotive-focused software company specializing in open source and open standards based software solutions for the mobility industry.

Highly specialised on server side technologies, but delivered also embedded software projects with in-house resources and external partners.

Developed OTA Plus, the only open source client/server solution for over-the-air software updates for OEMs and Tier1s.

First cloud-only service provider to be accepted into the German Association of the Automotive Industry (VDA), and leads the OTA activities inside GENIVI and Automotive Grade Linux.

Headquartered in Berlin, ATS operates a regional hub in Tokyo.

II

Introduction OTA.

Background
OTA Plus.

In 2015, ATS was contracted by JLR to develop core components of an OTA solution. Later on that year, these OTA core components were contributed as open source to the automotive alliance GENIVI.

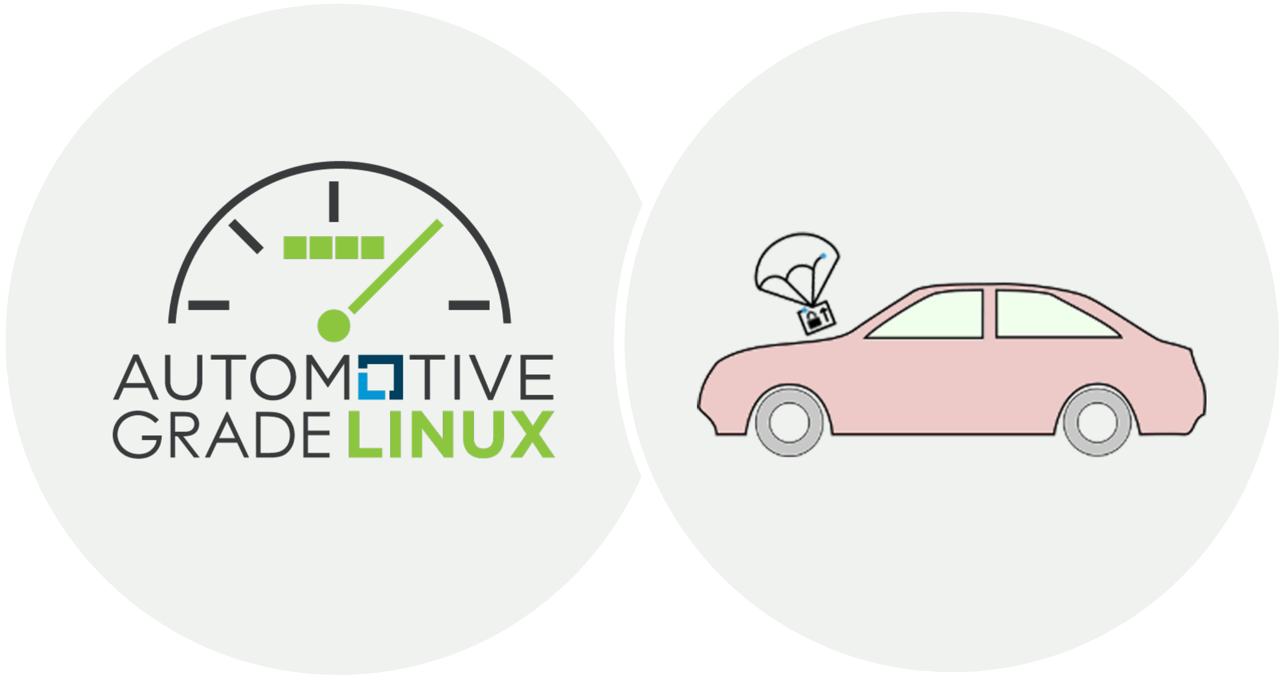
Building on that base, ATS developed its own commercial offering in 2016, OTA Plus.

The need for rapid prototyping and a turnkey solution led to the development of the OTA SaaS platform ATS Garage in 2017.

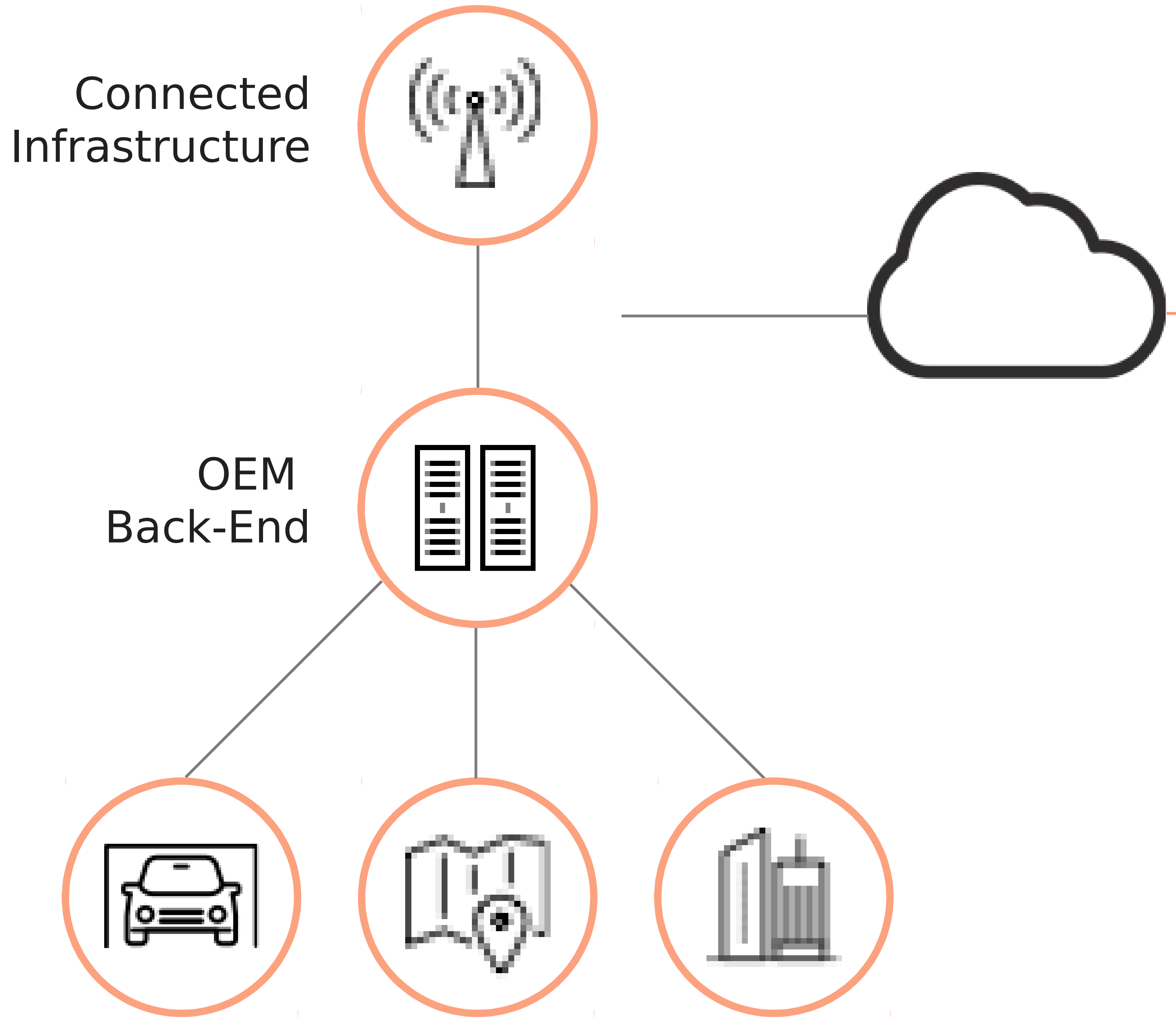
ATS still leads over-the-air update activities in GENIVI and, since 2016, also within Toyota-backed Automotive Grade Linux (AGL).

MAGNETI MARELLI
NISSAN
Pioneer
HONDA
The Power of Dreams
GENIVI
ERICSSON
VOLVO
Volvo Cars
FUJITSU
RENAULT

GENIVI MEMBERS (SELECTION)



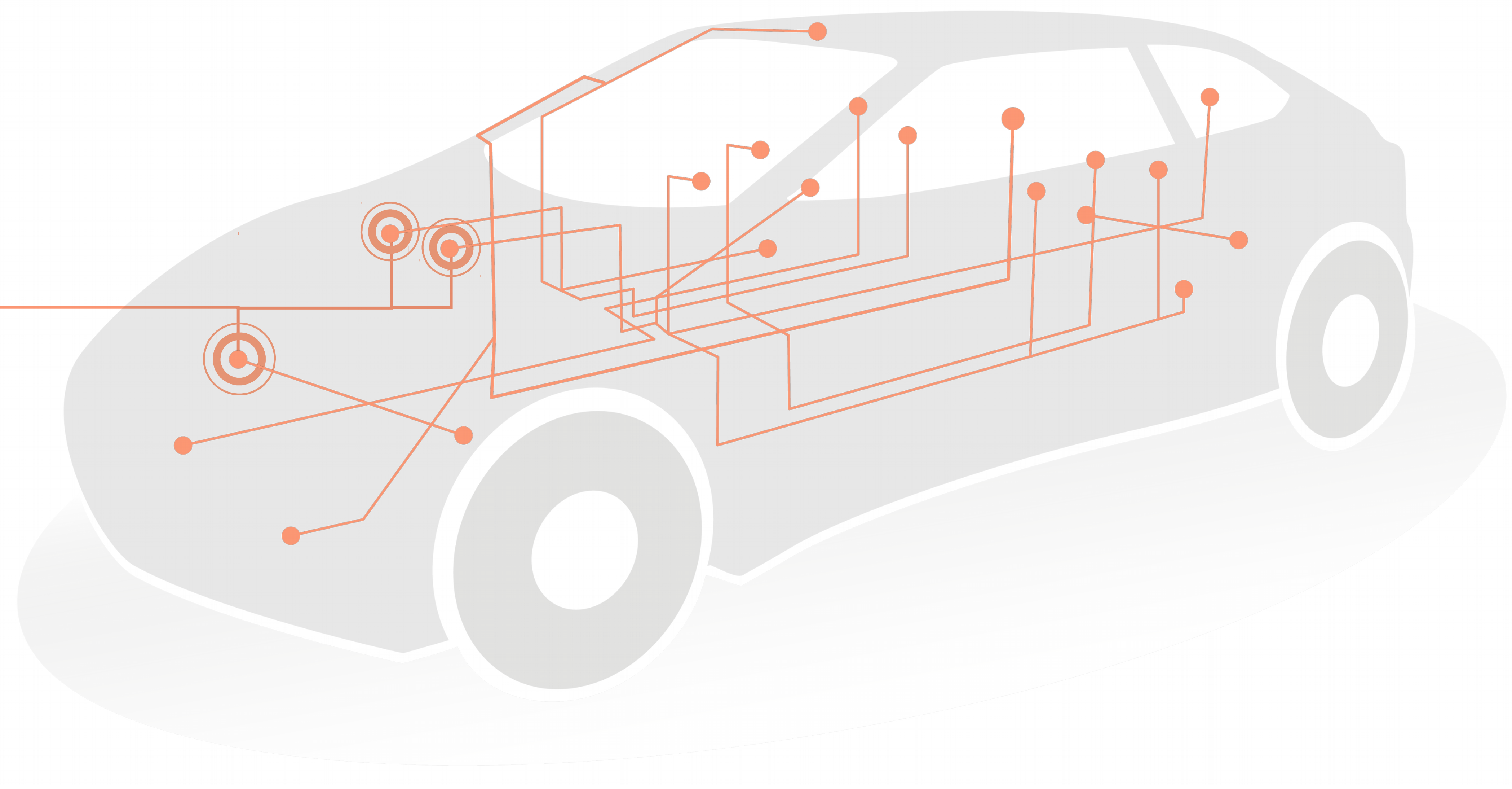
OTA Plus - More than Software Updates.



Connected Infrastructure

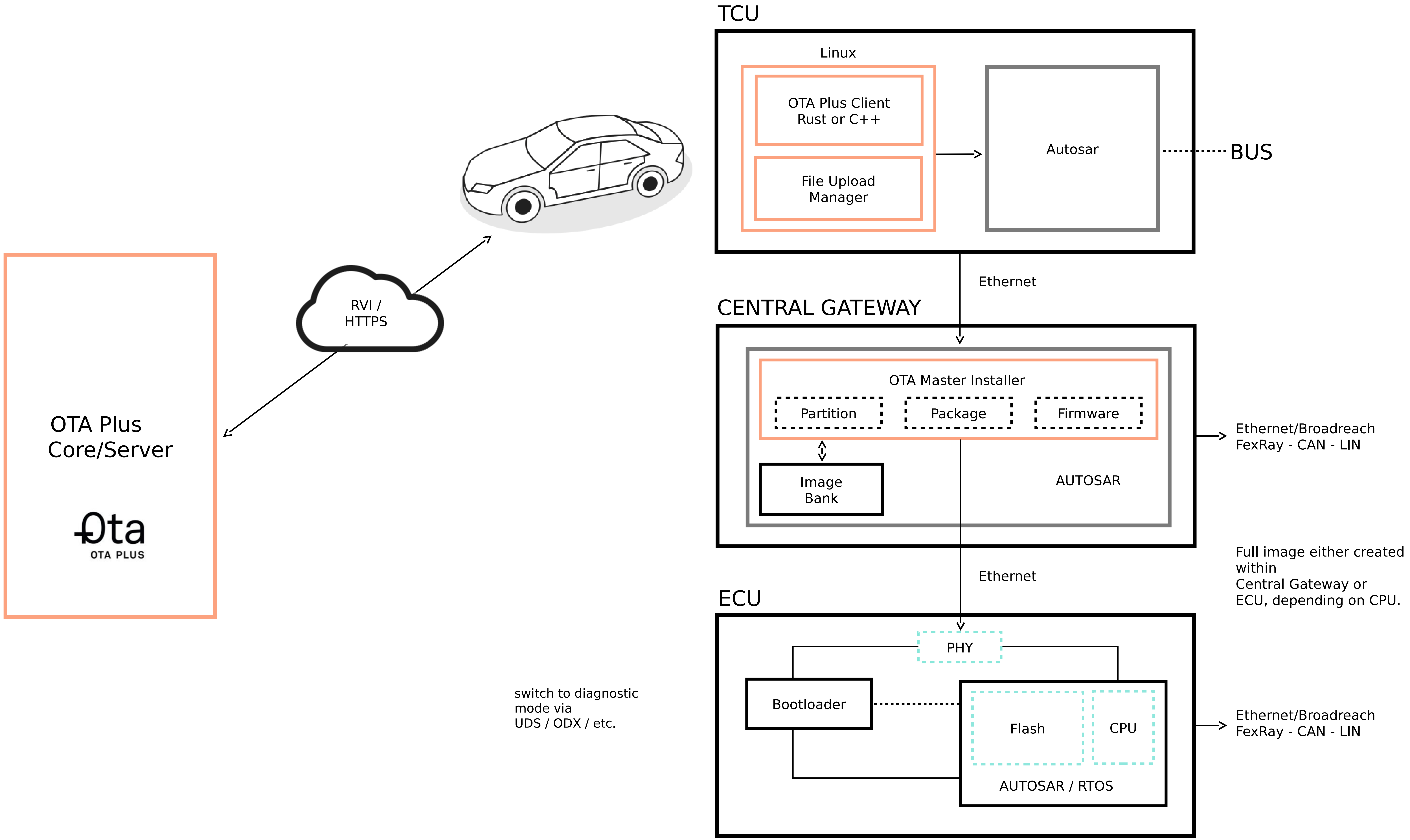
OEM Back-End

SW Supplier & Service Provider



OTA tackles the highly sensitive interface between the ECUs in the vehicle, the back-end systems of the OEM,
and thus the interface to suppliers, service providers and connected infrastructure. Without constantly syncing data and software, autonomous driving in a highly connected environment will be impossible.

Vehicle Architecture.



OTA Plus Core/Server

Ota OTA PLUS

RVI / HTTPS

TCU

Linux

OTA Plus Client Rust or C++

File Upload Manager

Autosar

BUS

Ethernet

CENTRAL GATEWAY

OTA Master Installer

Partition

Package

Firmware

Image Bank

AUTOSAR

Ethernet/Broadreach
FexRay - CAN - LIN

Ethernet

Full image either created
within
Central Gateway or
ECU, depending on CPU.

ECU

PHY

Bootloader

Flash

CPU

AUTOSAR / RTOS

Ethernet/Broadreach
FexRay - CAN - LIN

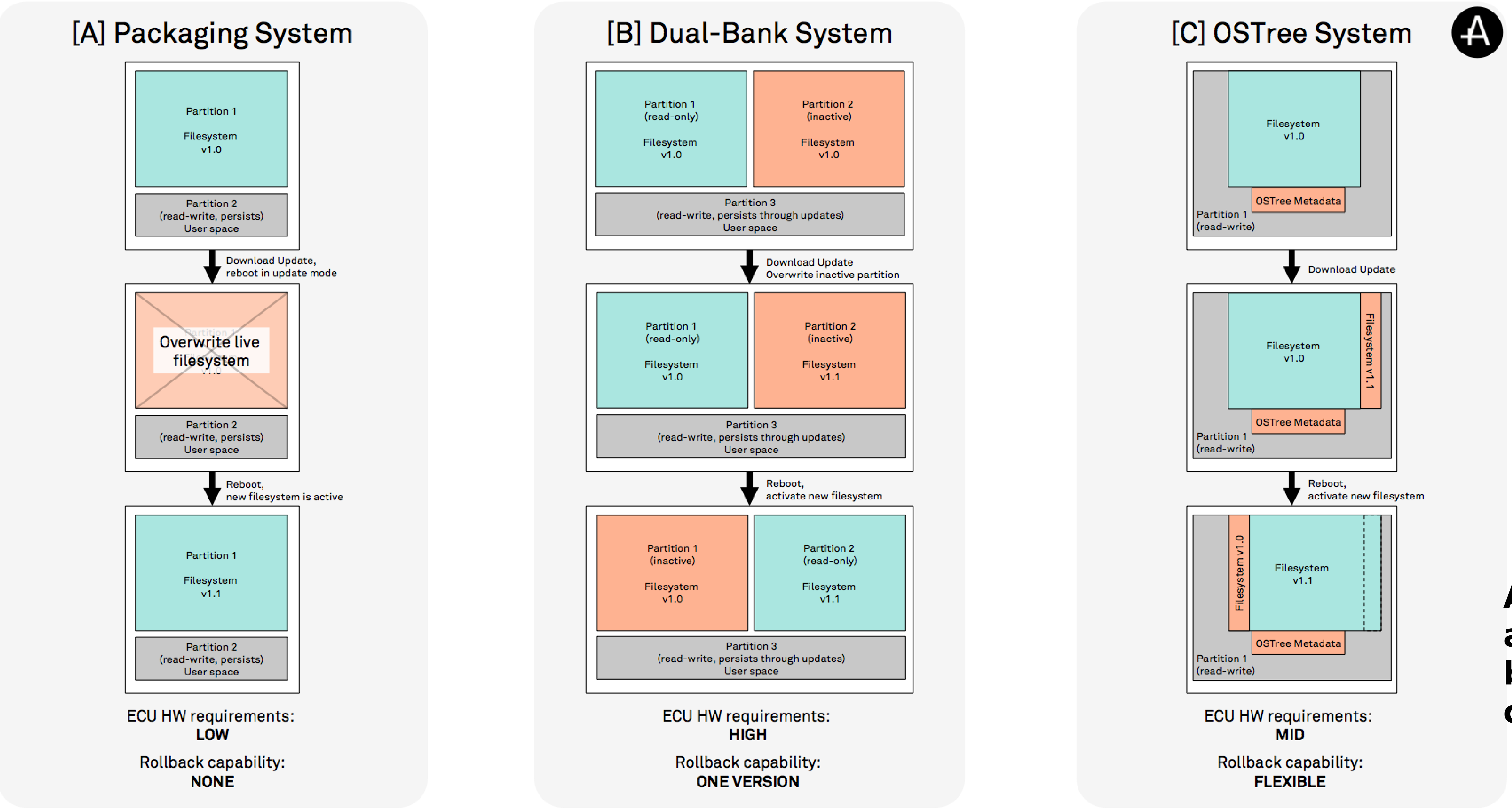
switch to diagnostic
mode via
UDS / ODX / etc.

OSTree - Differential Updates.

🟦 Active: used for root filesystem

🟧 Inactive: used for root filesystem

⬜ Space available for storage



[A] Packaging System

Partition 1

Filesystem v1.0

Partition 2 (read-write, persists) User space

Download Update, reboot in update mode

Overwrite live filesystem

Partition 2 (read-write, persists) User space

Reboot, new filesystem is active

Partition 1

Filesystem v1.1

Partition 2 (read-write, persists) User space

ECU HW requirements: **LOW**

Rollback capability: **NONE**

[B] Dual-Bank System

Partition 1 (read-only) Filesystem v1.0

Partition 2 (inactive) Filesystem v1.0

Partition 3 (read-write, persists through updates) User space

Download Update Overwrite inactive partition

Partition 1 (read-only) Filesystem v1.0

Partition 2 (inactive) Filesystem v1.1

Partition 3 (read-write, persists through updates) User space

Reboot, activate new filesystem

Partition 1 (inactive) Filesystem v1.0

Partition 2 (read-only) Filesystem v1.1

Partition 3 (read-write, persists through updates) User space

ECU HW requirements: **HIGH**

Rollback capability: **ONE VERSION**

[C] OSTree System

Filesystem v1.0

OSTree Metadata

Partition 1 (read-write)

Download Update

Filesystem v1.0

Filesystem v1.1

OSTree Metadata

Partition 1 (read-write)

Reboot, activate new filesystem

Filesystem v1.0

Filesystem v1.1

OSTree Metadata

Partition 1 (read-write)

ECU HW requirements: **MID**

Rollback capability: **FLEXIBLE**

Content addressed object store that manages full file system,

provides atomic incremental updates, works like GIT.
New filesystem can be downloaded in the background, whereas only changes from previous version get transmitted

and runs once system gets rebooted.

Old versions, and all previous once are accessible.
When an update is available, Treehub sends a small metadata file with a commit identifier, client pulls than the appropriate version (only new files and binary diffs) from server based Treehub.

Advantages
a. more dynamic built process
b. lower cost as no dual bank necessary and
c. simple roll-back to various versions

III

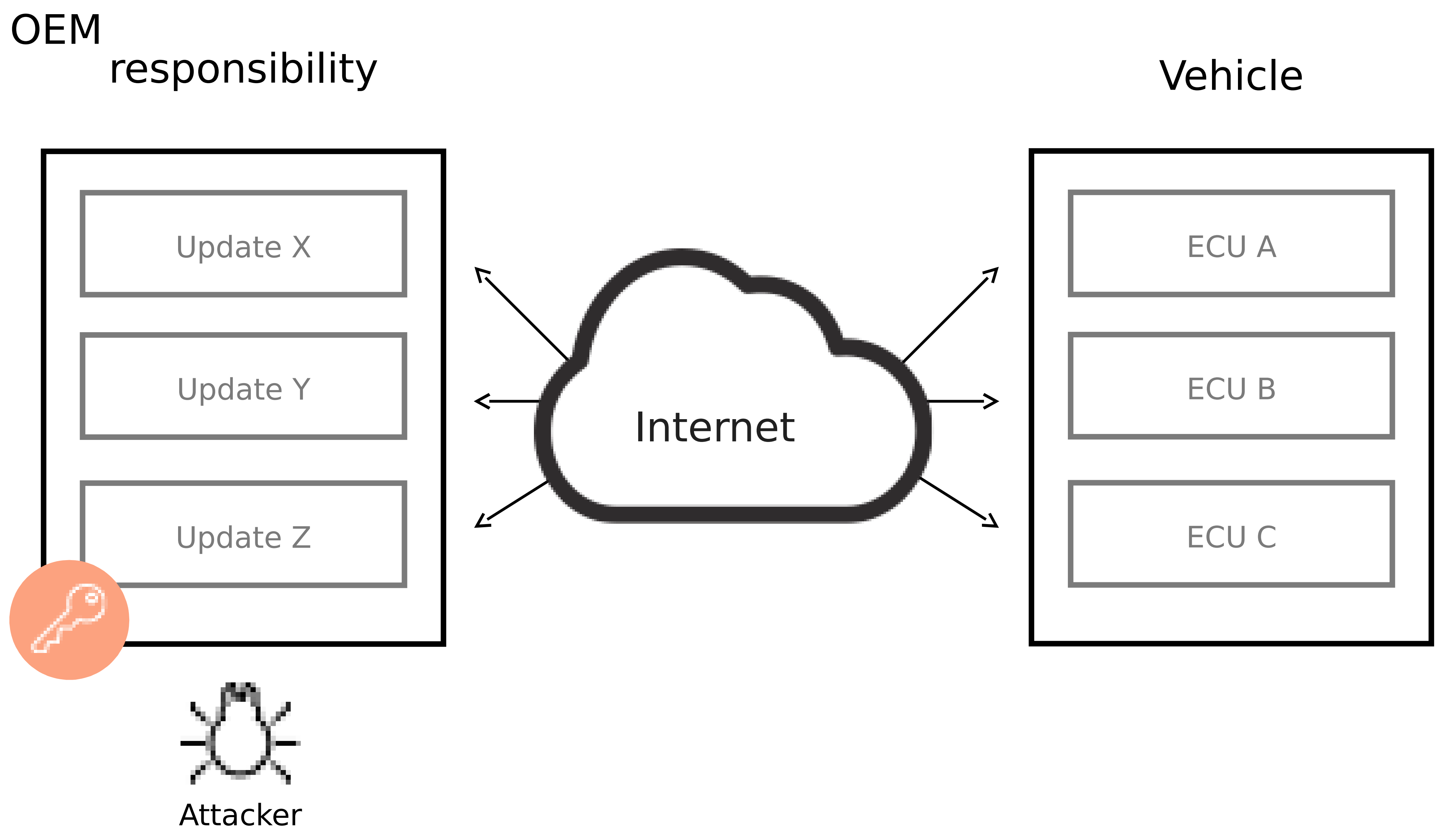
Introduction
Uptane Security Framework.

Focus: Repository Compromise.

Attackers can:

Perform man-in-the-middle (MitM)

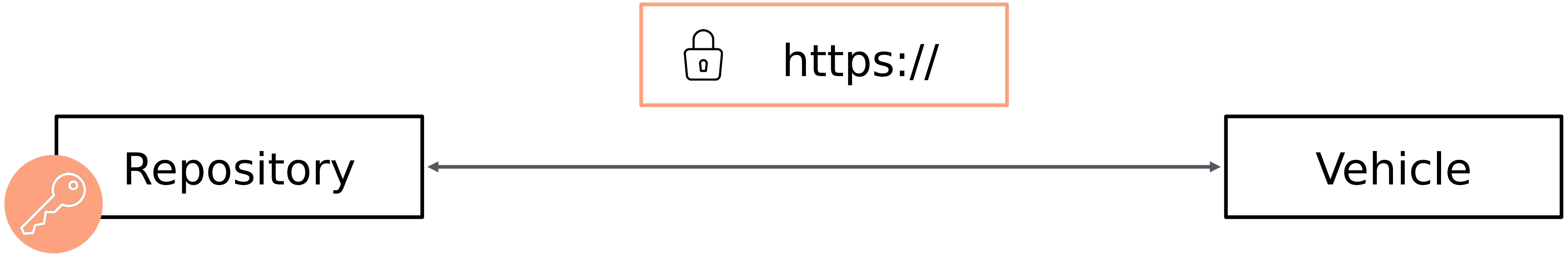
- attacks outside or inside vehicle
- Compromise ECUs in a vehicle
- Compromise keys used to sign updates,
- or servers that store these keys



Previous Security Systems.

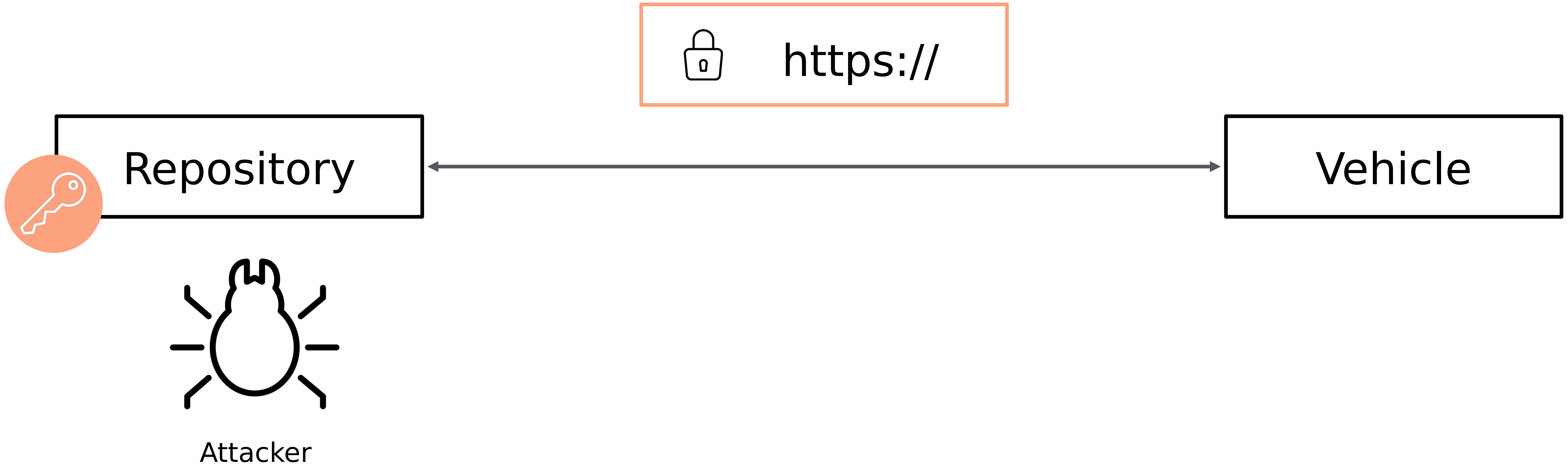
Signing All Metadata with an Online Key.

- Use a single online key to sign all metadata (e.g., using SSL / TLS)
- Protects ECUs from man-in-the-middle attacks between repository and vehicle
- Allows on-demand customization of updates for vehicles



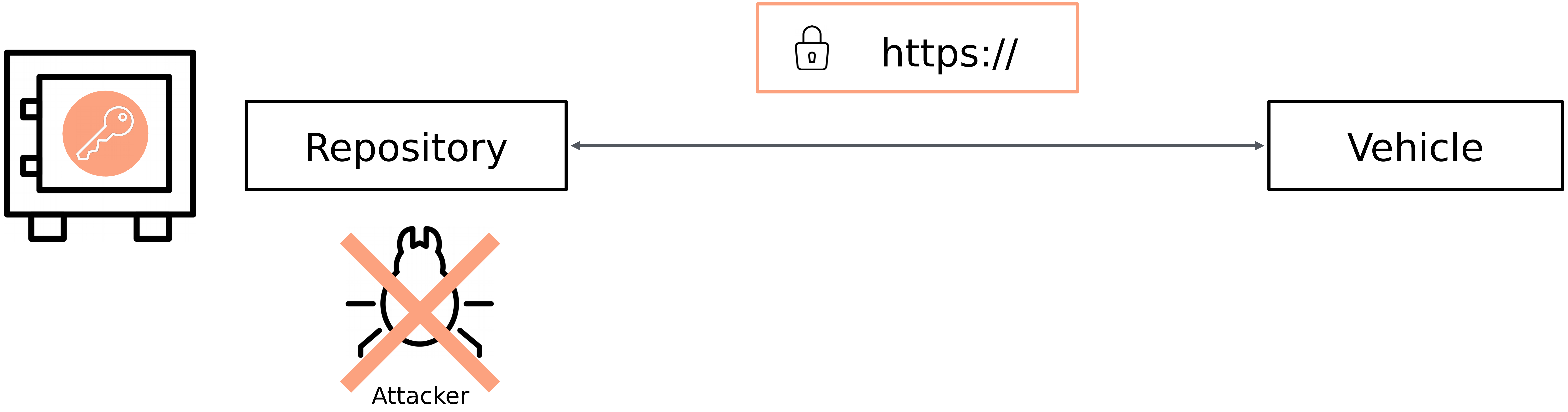
Signing All Metadata with an Online Key.

- Doesn’t say anything about the security of the server: just that you are talking to it
- Single point of failure: easy to compromise
- If repository is compromised, attacker can install malware and control vehicles



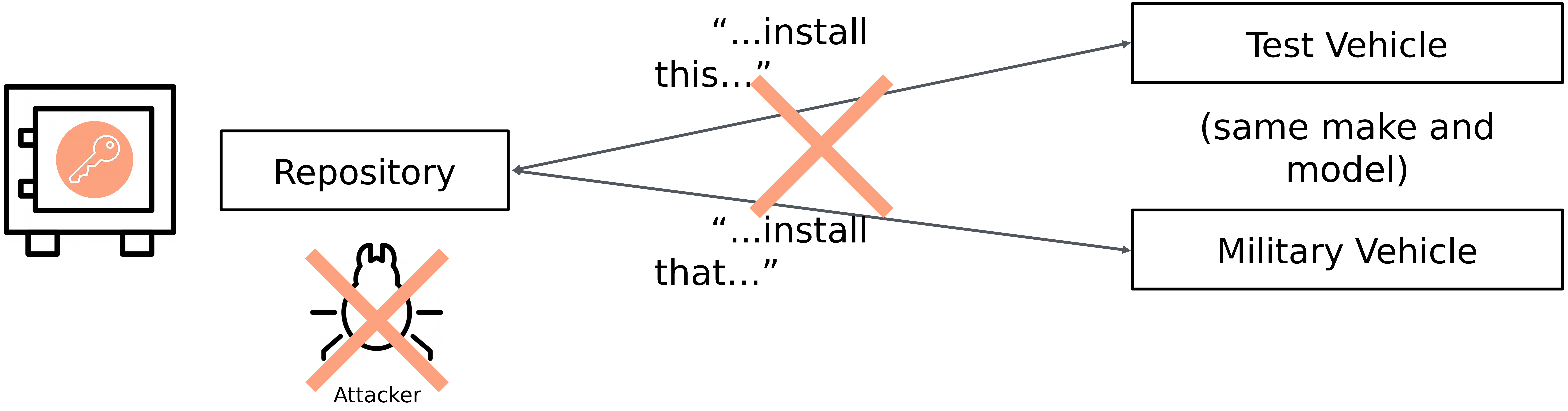
Signing All Metadata with an Online Key.

- Use a single offline key to sign all metadata (e.g., using GPG or RSA)
- Compromise-resilient, because attackers cannot tamper with metadata without being detected



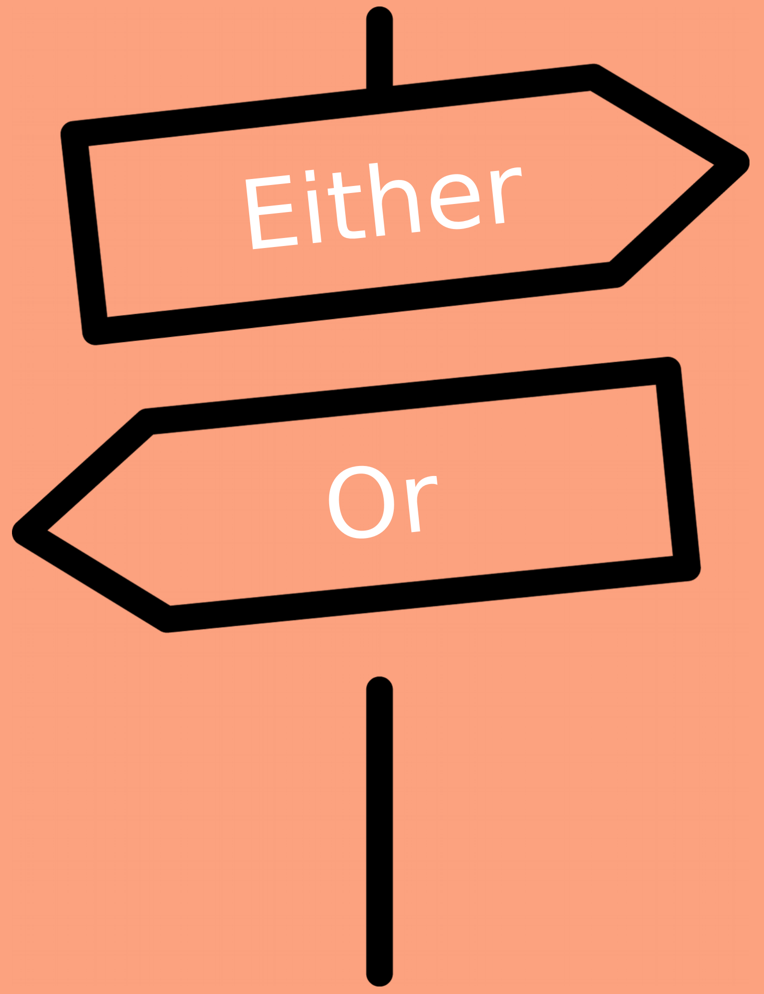
Signing All Metadata with an Online Key.

- Difficult to customize updates on-demand for vehicles
- Difficult to install different updates on vehicles of same make and model,
  - but with different requirements
  - Cannot instantly blacklist only buggy updates
- In practice, this risks becoming previous system



Takeaway: Either-Or....

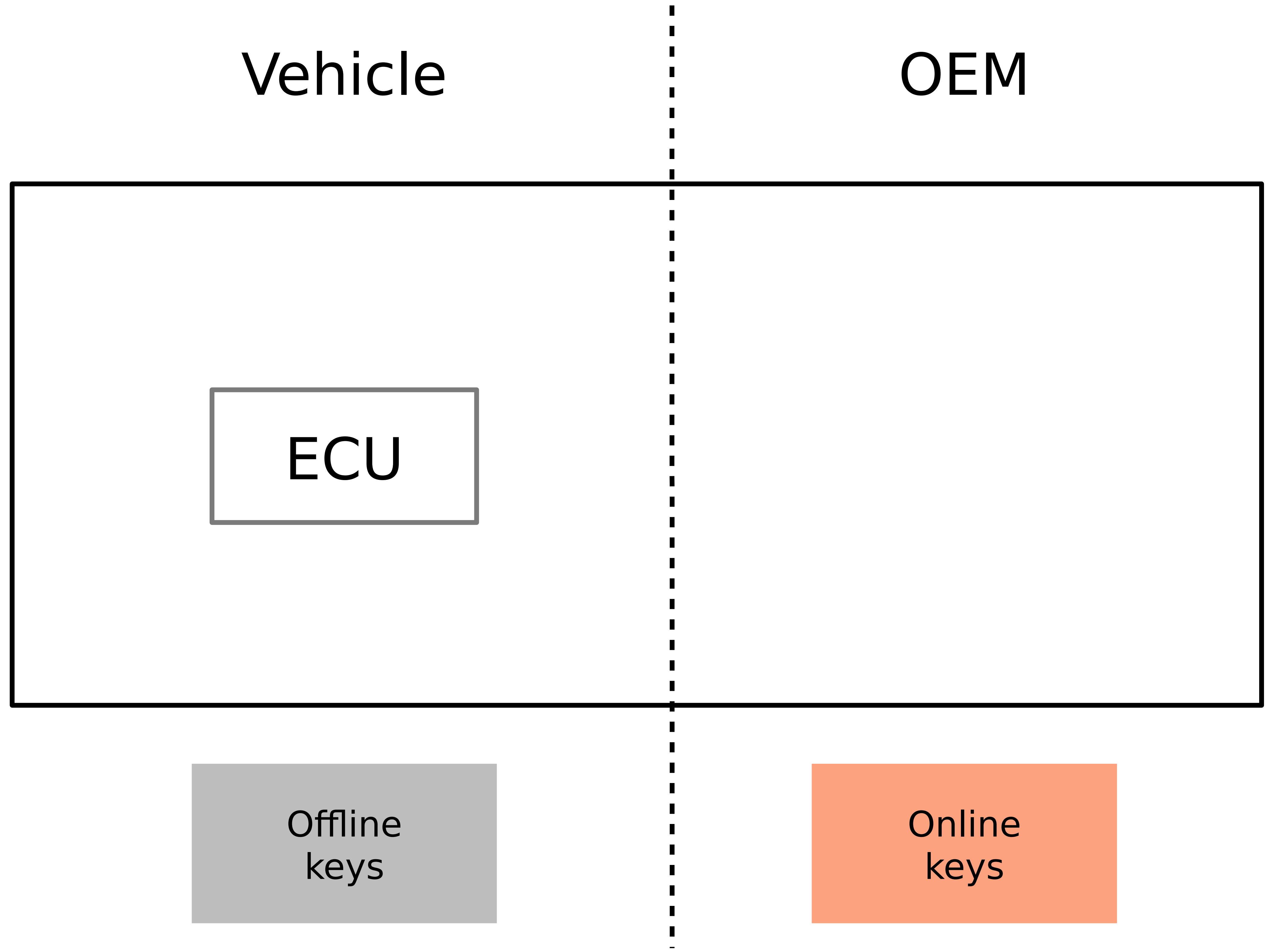
Previous security systems force repositories to choose either on-demand customization of vehicles, or compromise-resilience.



Uptane: A New Approach.

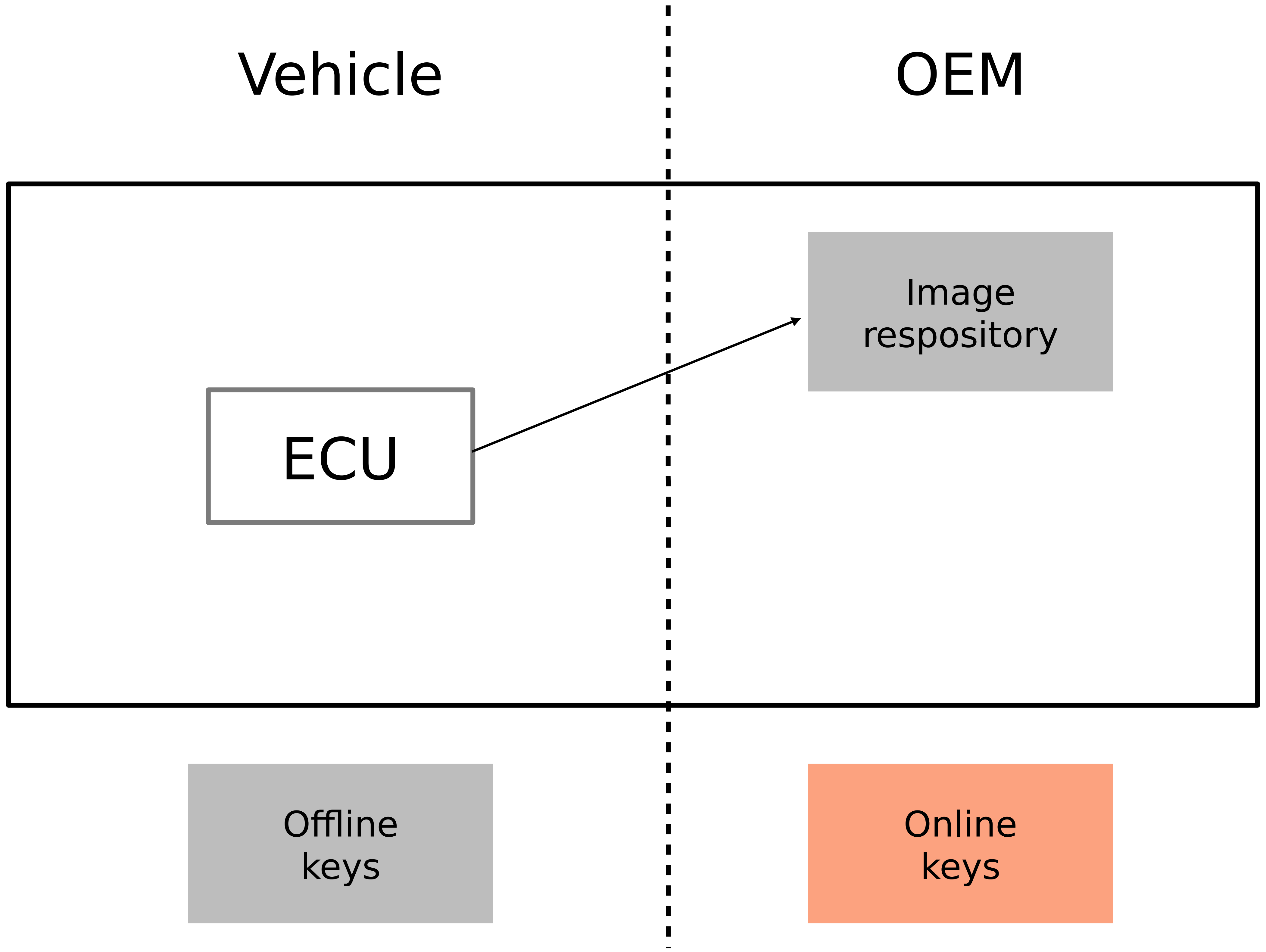
Key Idea.

- What if there are two repositories?



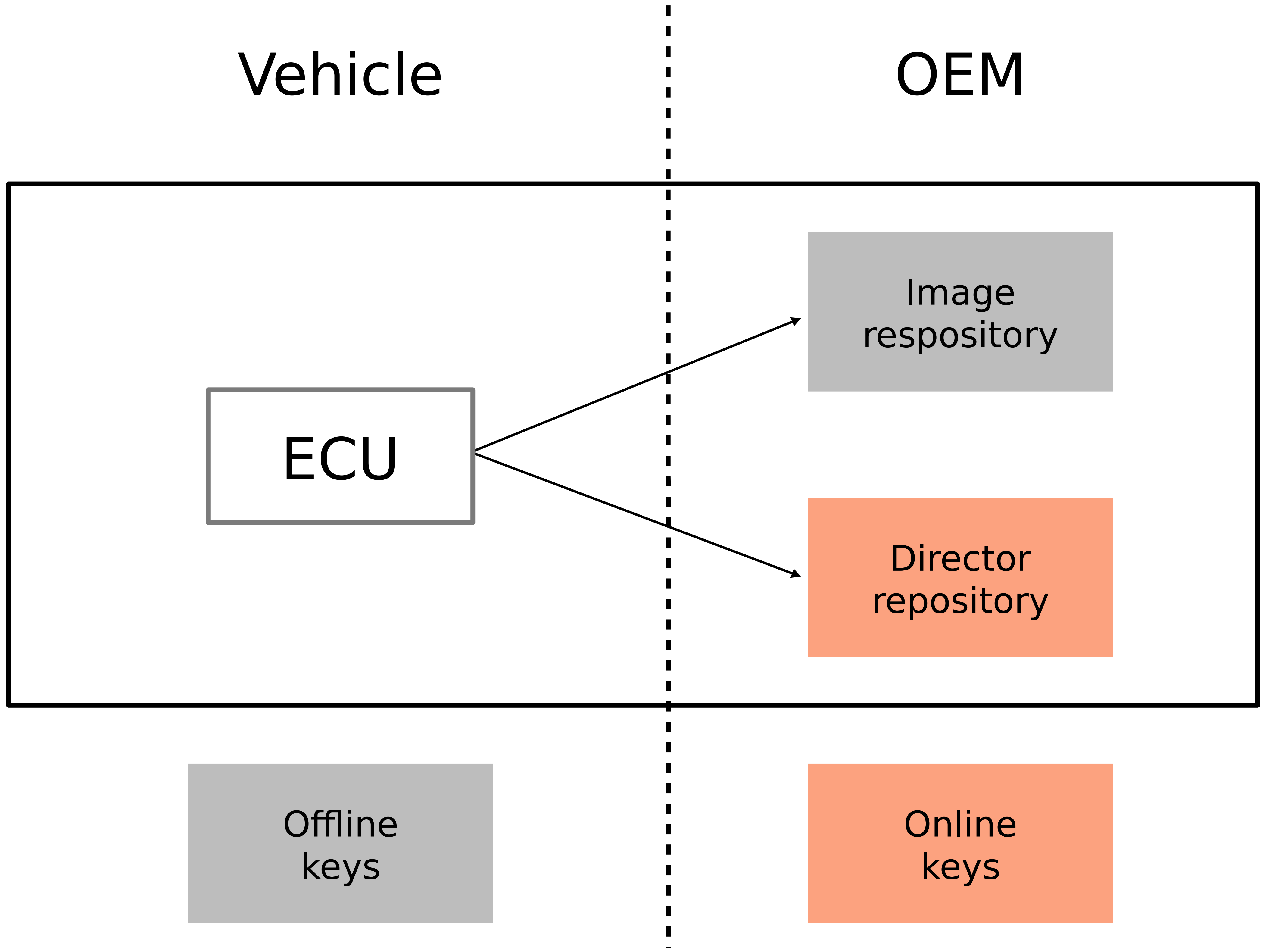
Key Idea.

- What if there are two repositories?
- Image repository
  - Uses offline keys
  - Provides signed metadata about all available updates for all ECUs on all vehicles



Key Idea.

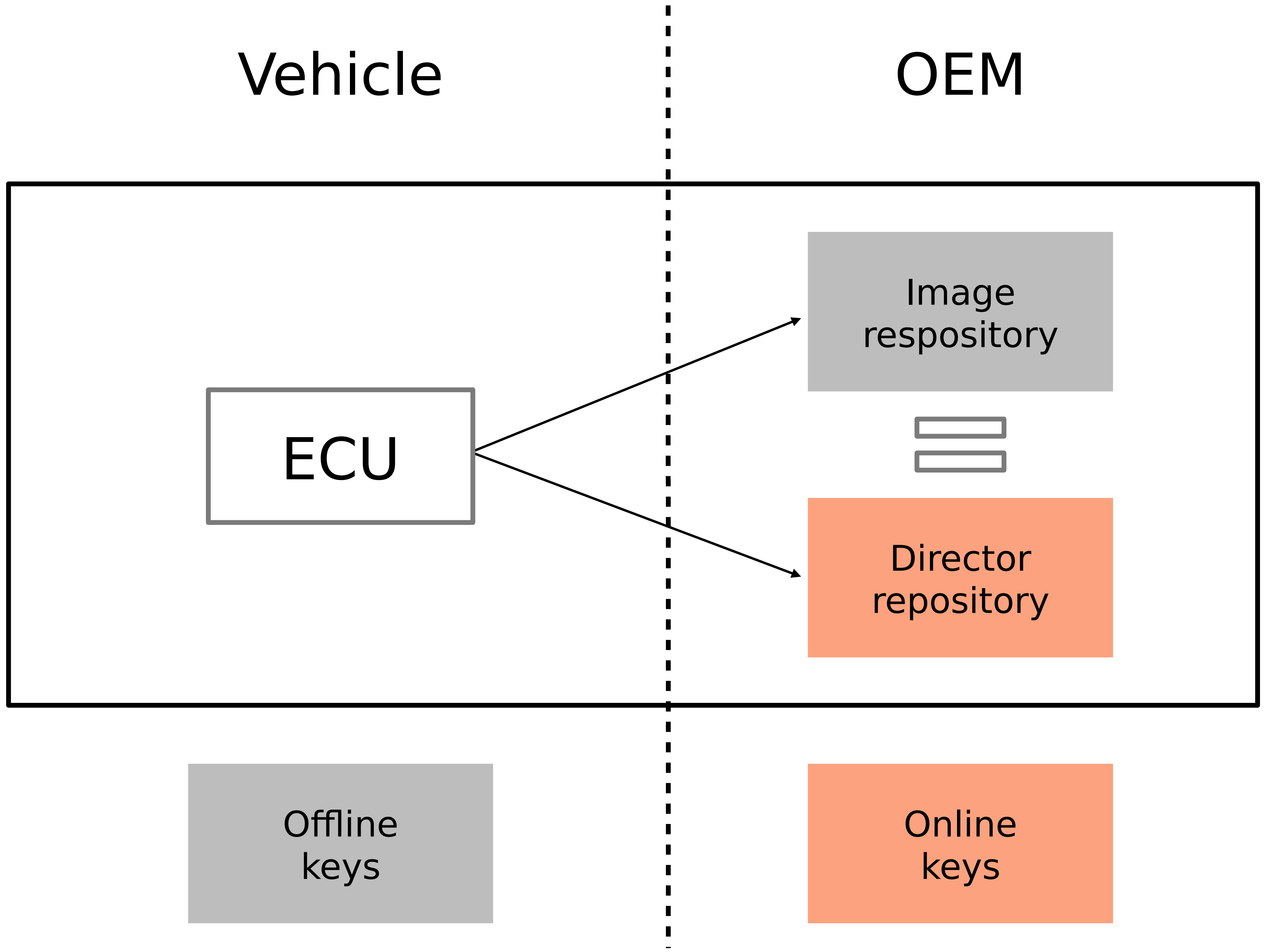
- What if there are two repositories?
- Image repository
  - Uses offline keys
  - Provides signed metadata about all available updates for all ECUs on all vehicles
- Director repository
  - Uses online keys
  - Signs metadata about which updates should be installed on which ECUs on a vehicle



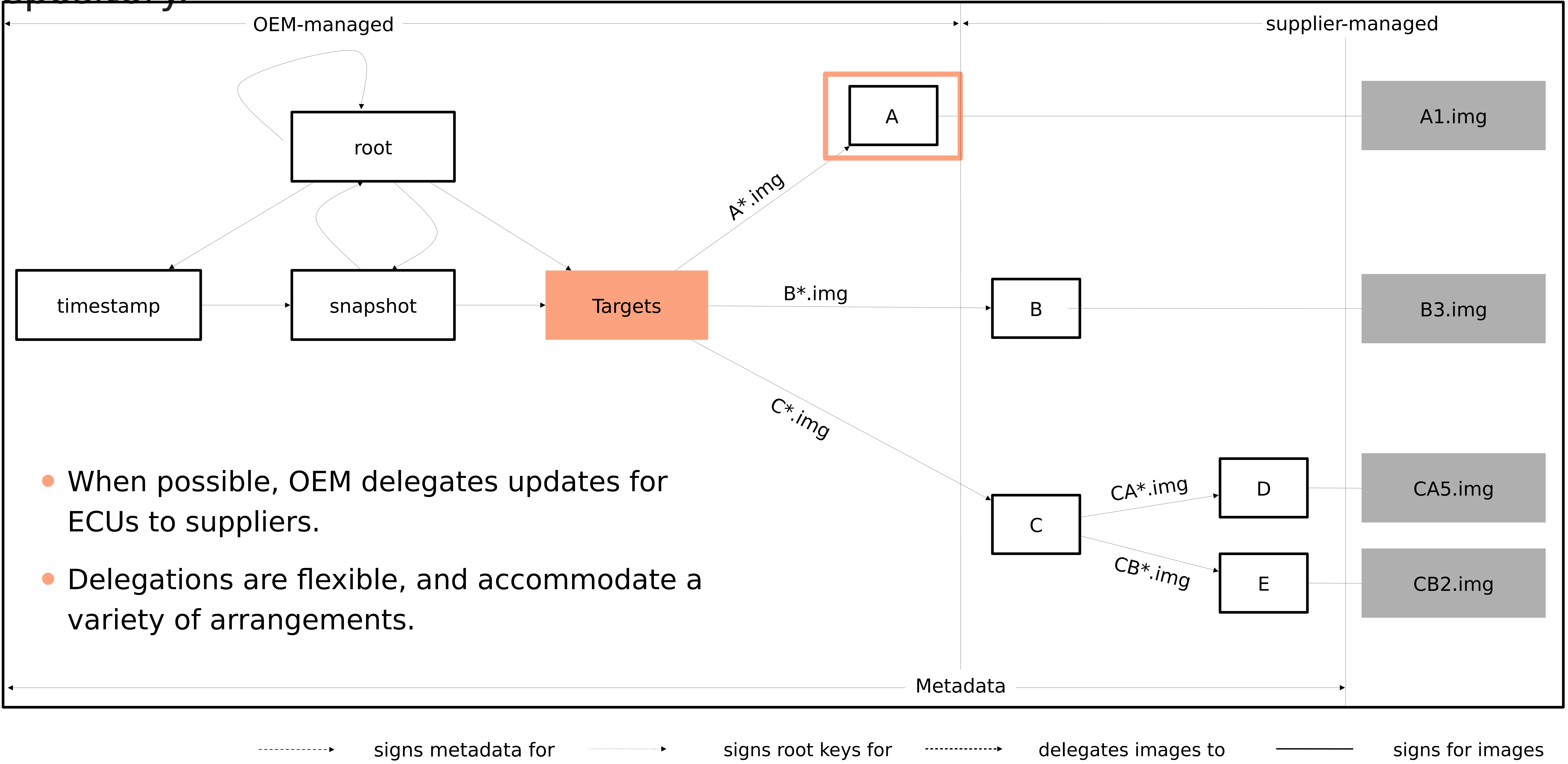
Key Idea.

- A vehicle would ensure that installation instructions from director repository matches updates from image repository.

- Using both repositories provides both on-demand customization of vehicles & compromise-resilience.

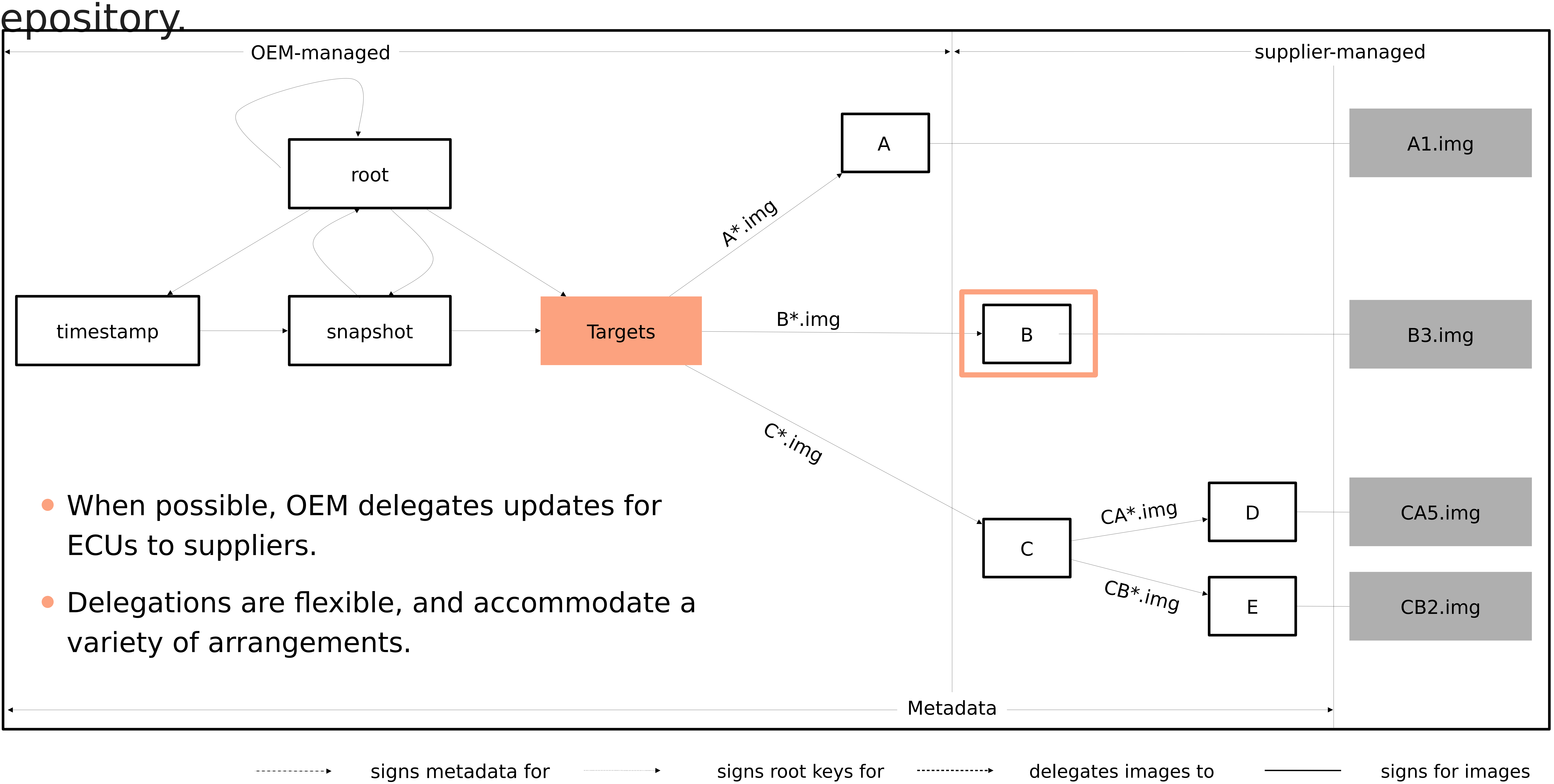


The Image Repository.



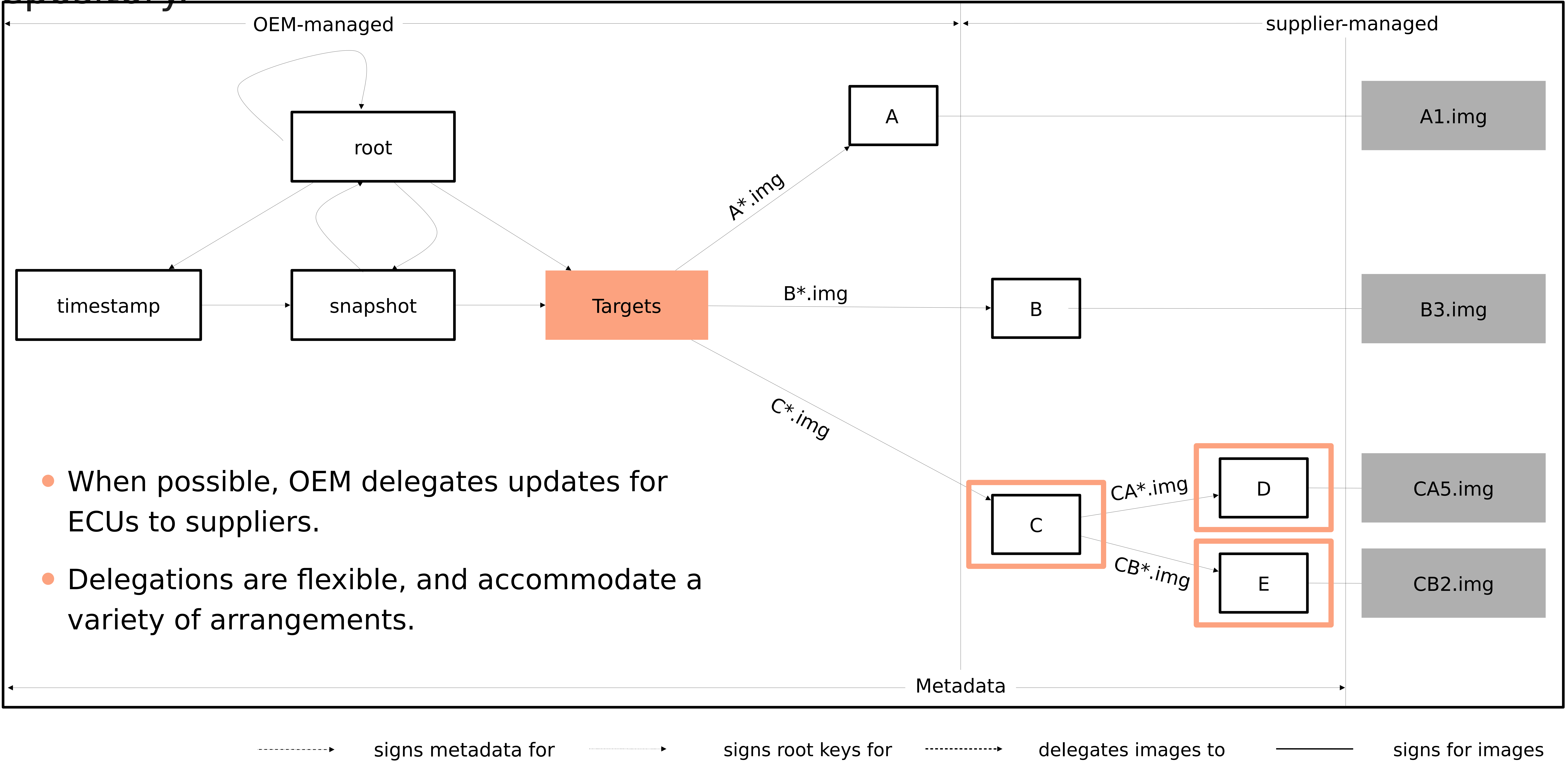
- When possible, OEM delegates updates for ECUs to suppliers.
- Delegations are flexible, and accommodate a variety of arrangements.

The Image Repository.

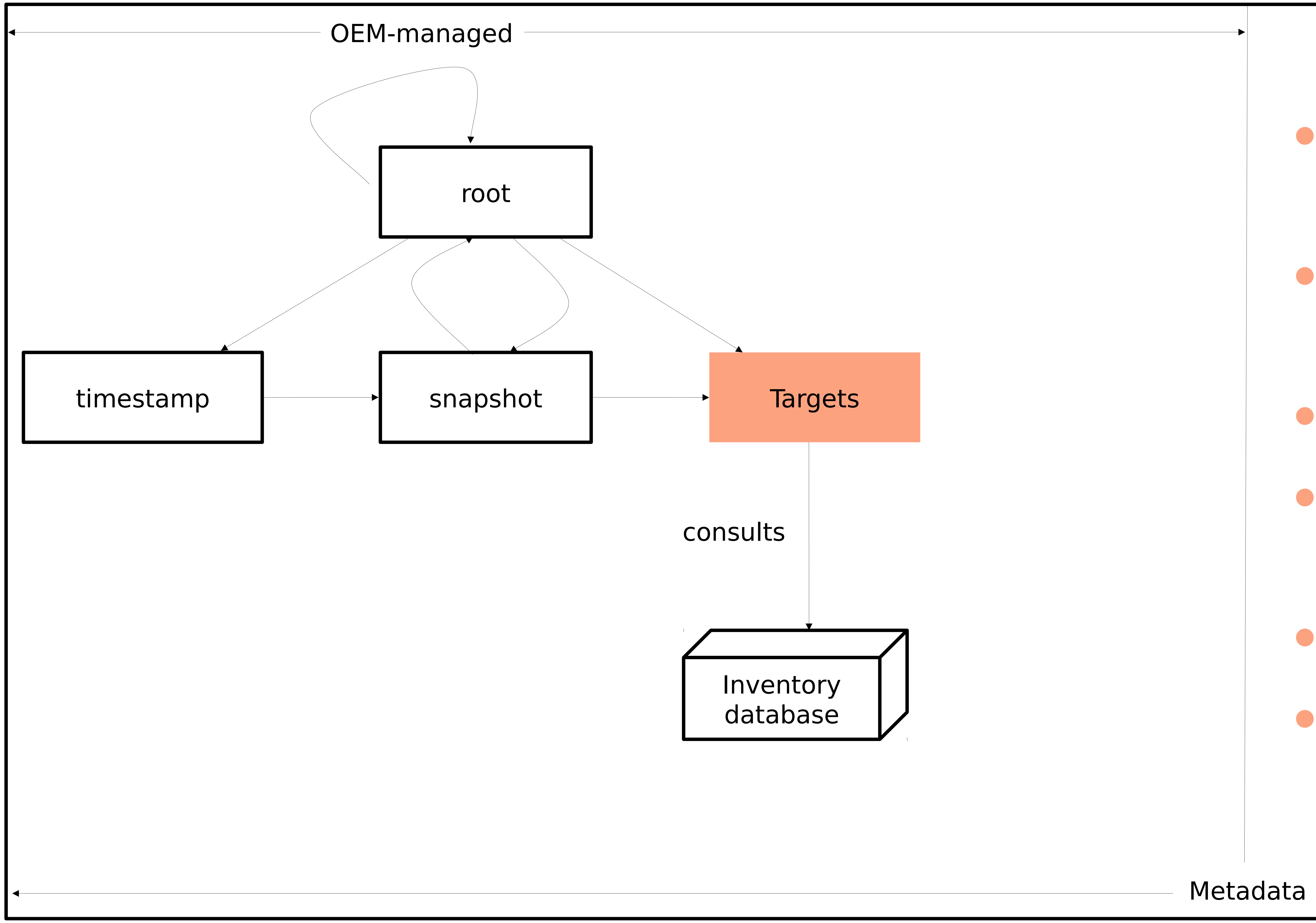


- When possible, OEM delegates updates for ECUs to suppliers.
- Delegations are flexible, and accommodate a variety of arrangements.

The Image Repository.



- When possible, OEM delegates updates for ECUs to suppliers.
- Delegations are flexible, and accommodate a variety of arrangements.

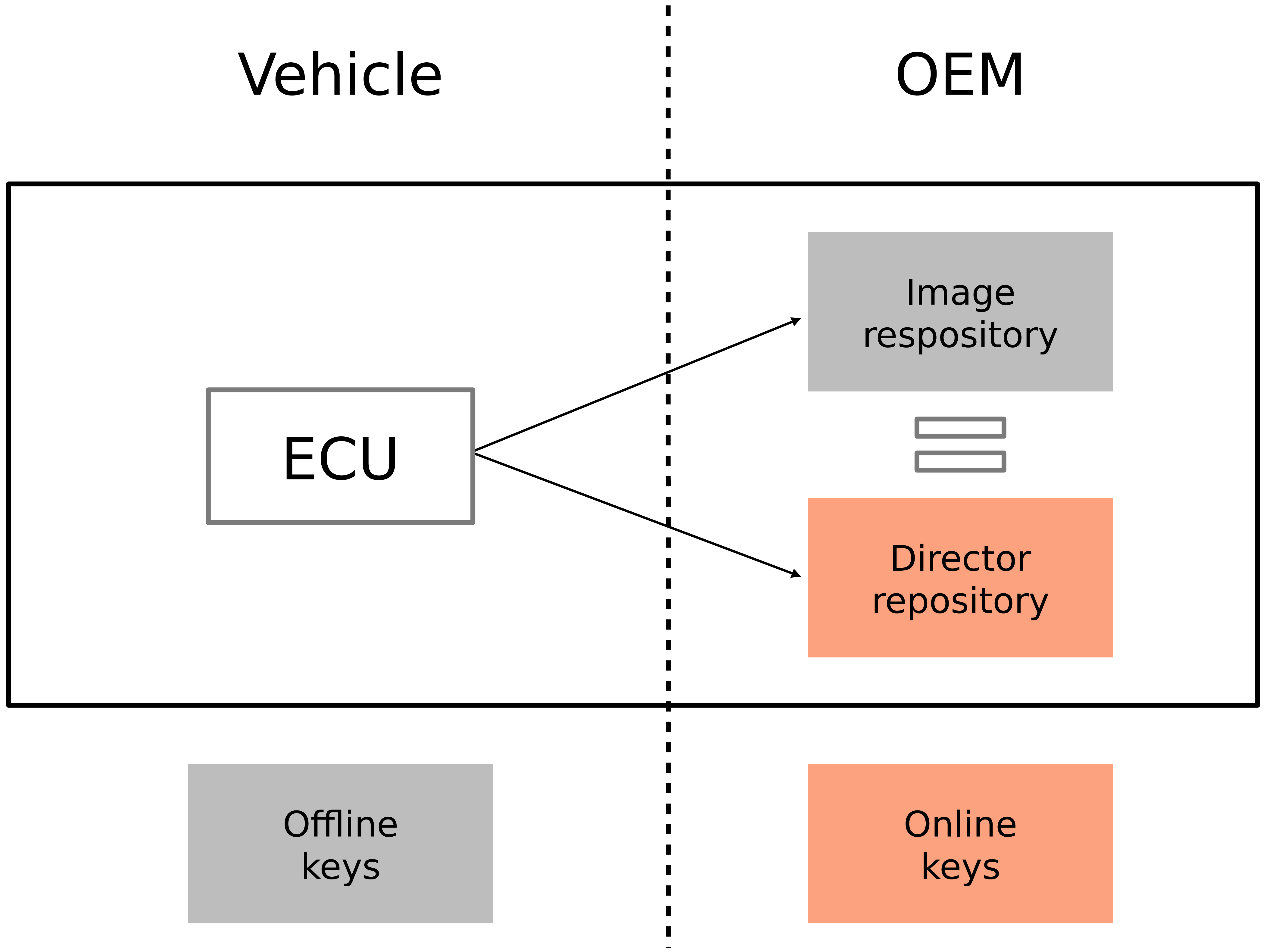


- Lets OEM control which updates are installed on which vehicles.
- Signs metadata about what images should be installed.
- Consults an inventory database
- to find out which ECUs are on a vehicle.
- Can also blacklist versions.
- Could additionally / also be run by fleet management or dealerships

Takeaway: Security & Flexibility.

- Uptane provides both on-demand customization of vehicles & compromise-resilience.

- Gives an OEM a powerful array of options in controlling how updates are chosen for a vehicle, and who signs for updates.



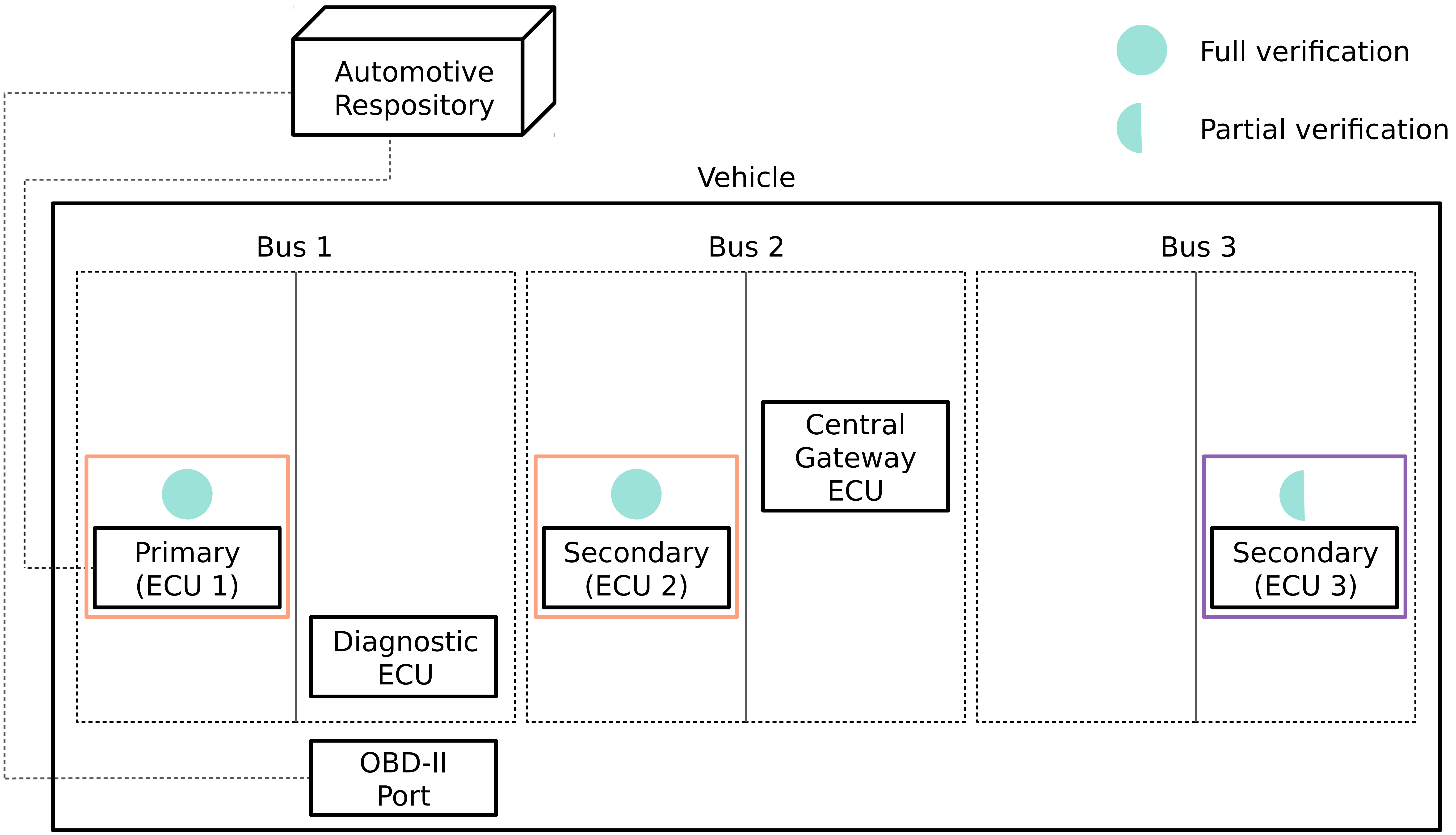
Verifying Metadata & Images on Devices.

Primaries and Secondaries.

Two types of ECUs, because:

Some ECUs are more / less

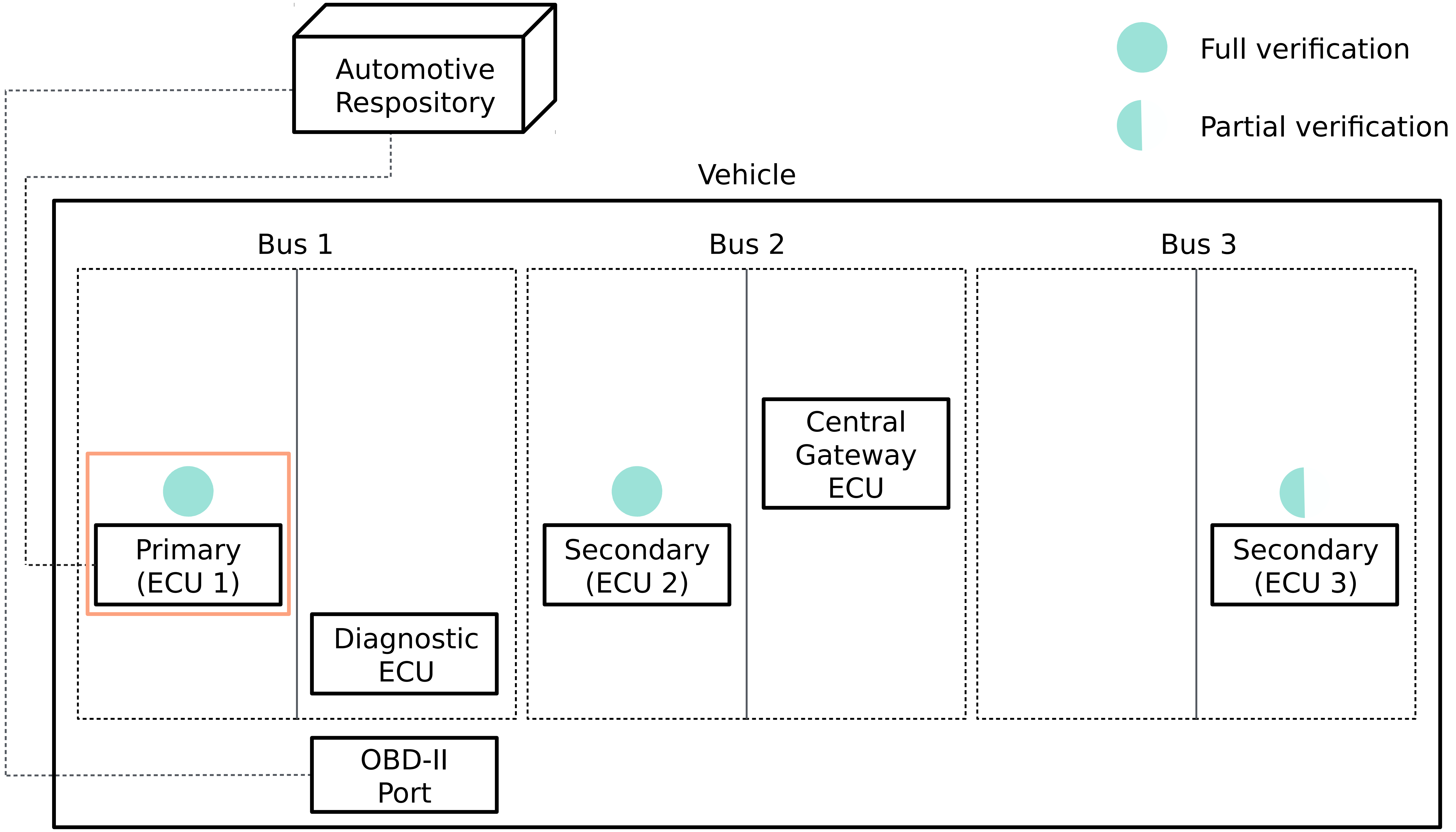
- powerful than others.
- Few ECUs have network
- connection to outside world.
- ECUs should not download
- metadata independently of
- each other.



Primaries and Secondaries.

A primary downloads, verifies, distributes metadata + images

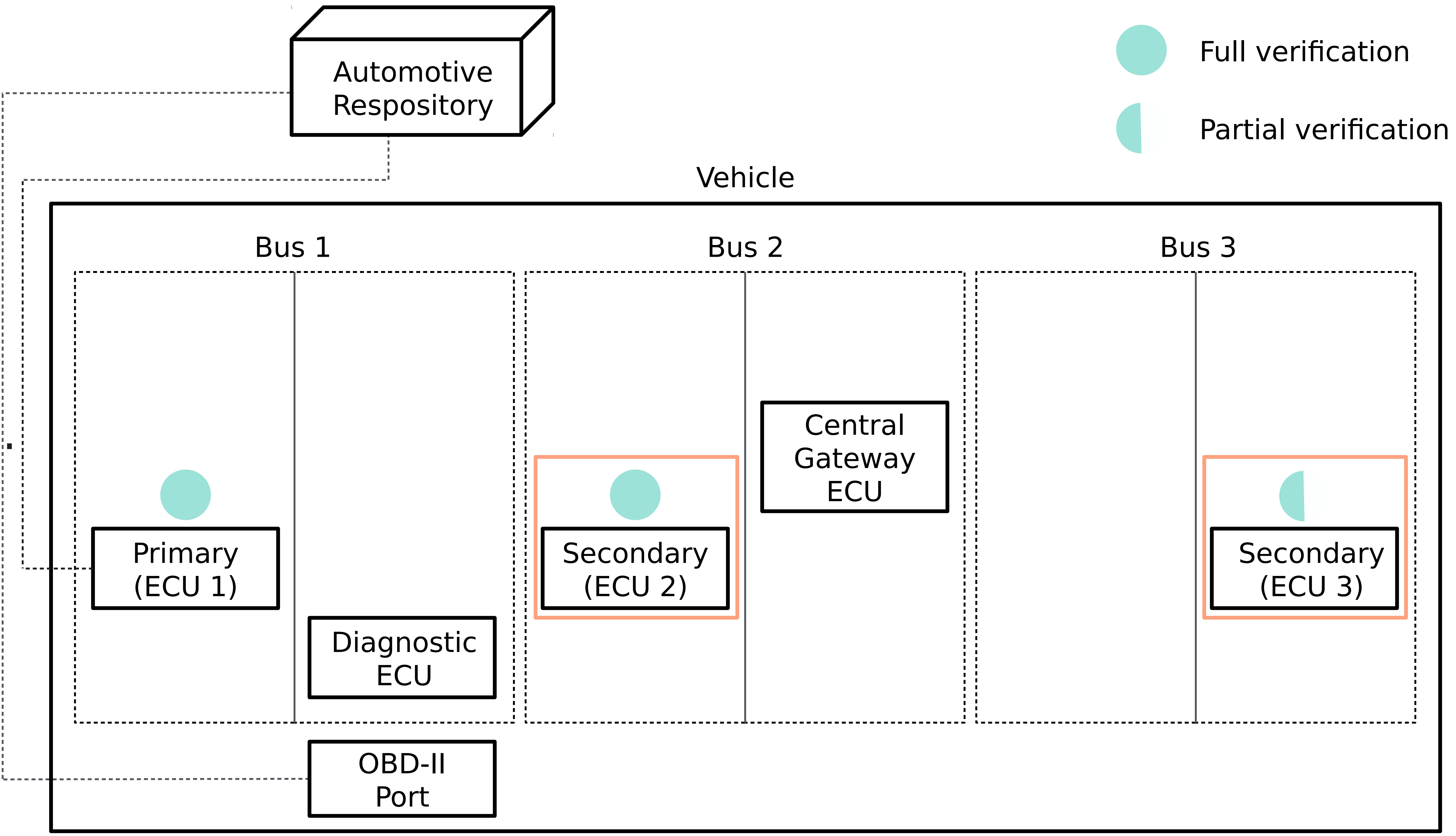
- to secondaries.



Primaries and Secondaries.

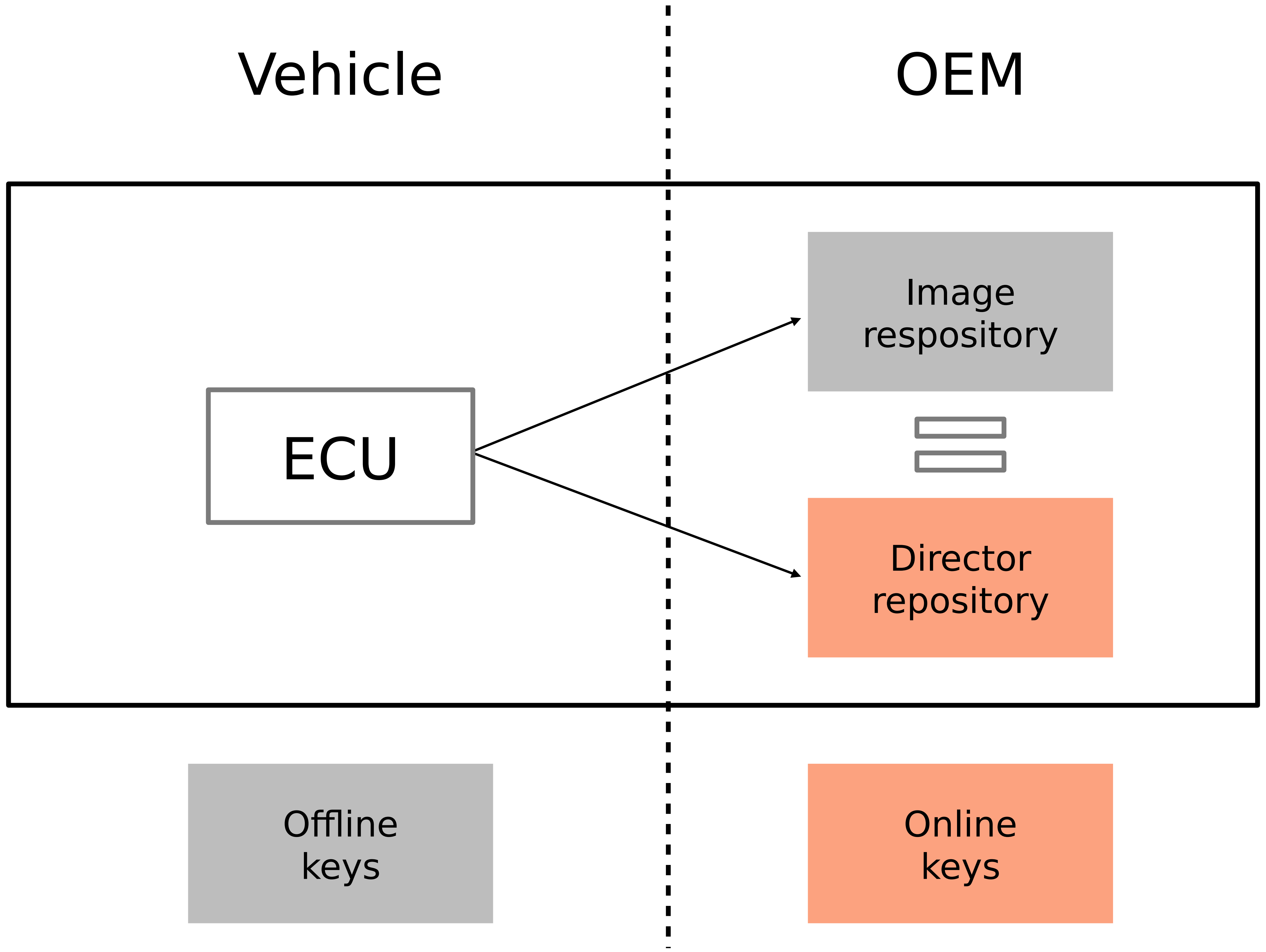
A secondary verifies metadata & image distributed by a primary,

- before updating to that image.



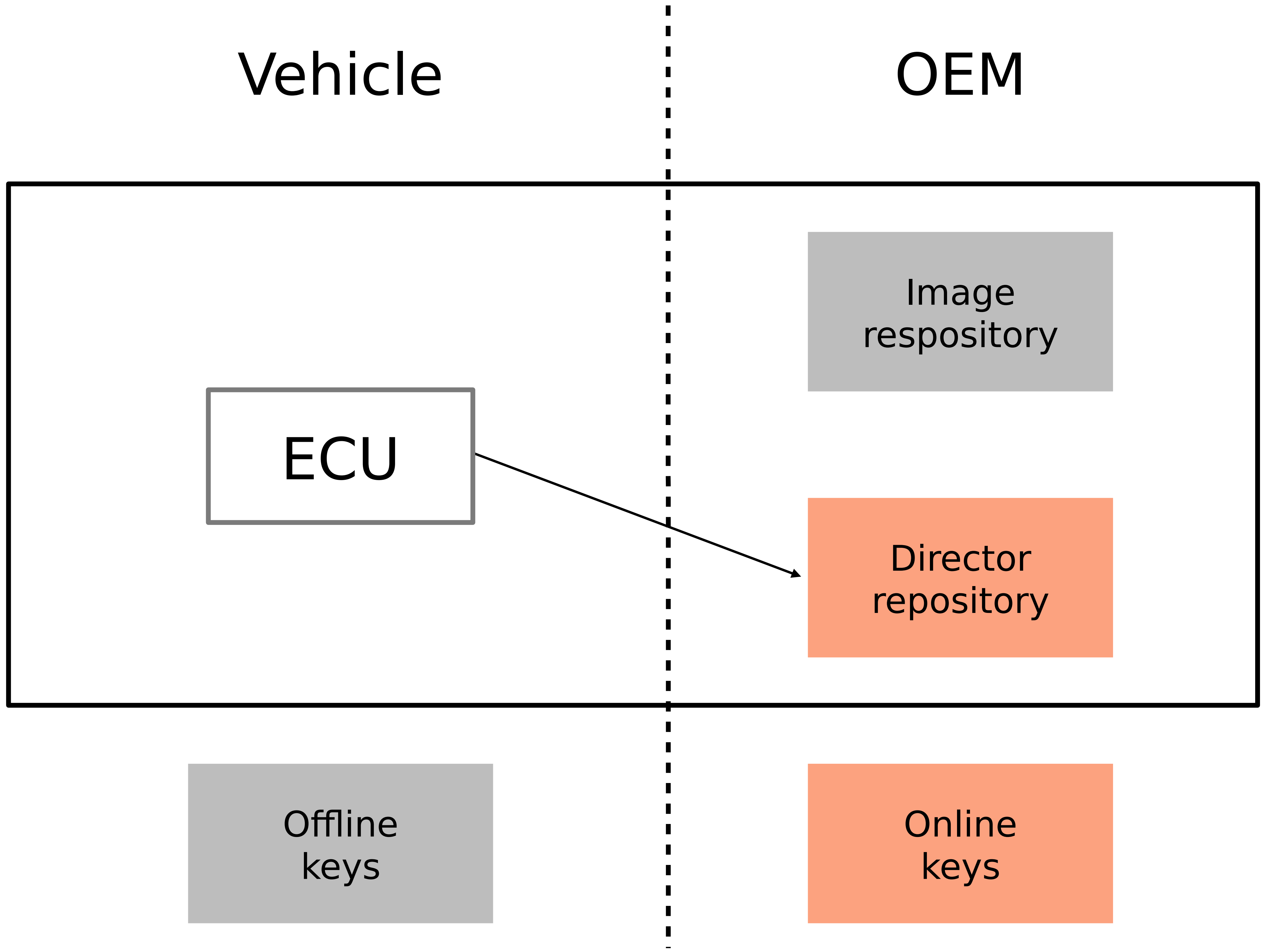
Takeaway: Security & Flexibility.

- Checking that metadata about updates chosen by the director repository matches metadata about the same updates on the image repository.
- Involves checking many signatures on many metadata files from both repositories.

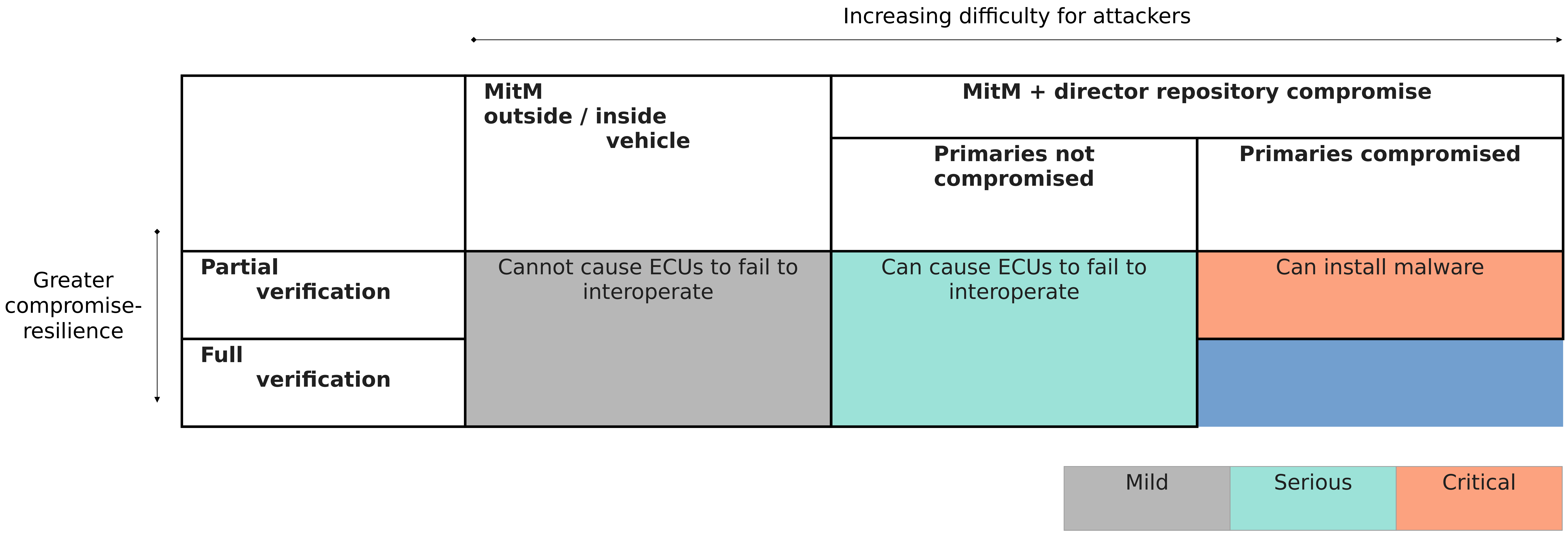


Takeaway: Security & Flexibility.

- Checking only metadata from the director repository.
- Involves checking only one signature on one metadata file.



Takeaway: Full vs Partial Verification.



Increasing difficulty for attackers

Greater compromise-resilience

	MitM outside / inside vehicle	MitM + director repository compromise	
		Primaries not compromised	**Primaries compromised**
Partial verification	Cannot cause ECUs to fail to interoperate	Can cause ECUs to fail to interoperate	Can install malware
Full verification			

Mild	Serious	Critical

Summary.

Security & Flexibility for your Over-The-Air Update System

- Compromise Resilient - but still allows for full flexibility due to two repositories.
- Adaptable Hardware Requirements - can support legacy and resource-constraint ECUs.
- Ultimate Flexibility - target any vehicle with any update at any time without compromising security.

ATS Garage.

SaaS for
over-the-air updates.

Over-the-air updates.
No compromises.

Weird things happen when you're deploying software.

But with ATS Garage, fixing it is oh so simple.

Ats
ATS GARAGE
How it works
Pricing
News
Contact
Docs
START NOW OR LOGIN ↗
⟶ Start now
FIND OUT MORE ↓

Contact Us.

ATS Advanced Telematic Systems GmbH

advancedtelematic.com

Arthur Taylor

+49 30 95 99 97 546

arthur@advancedtelematic.com