Uptane

Uptane: Virtual Workshop

“A Conversation on End-to-End Secure Automotive Software Updates”

https://uptane.github.io

2023-03-31

Uptane Development Timeline

Uptane

Alignment with Standards and Regulations

Standards		Regulations
ISO/SAE 21434 Road vehicles — Cybersecurity engineering	⟷	**UN R155** Cybersecurity and cybersecurity management system (CSMS)
ISO 24089 Road Vehicles – Software Update Engineering Base requirements for SUMS	⟷	**UN R156** Uniform provisions concerning the approval of vehicles with regards to **software update** and **software update management systems** (SUMS)

Threat Categories

Read the contents of updates to discover confidential information, reverse-engineer firmware, or identify security fixes to determine the fixed security vulnerability.

Deny installation of updates to prevent vehicles from fixing software problems.

Disrupt ECUs in the vehicle, denying use of the vehicle or of certain functions.

Control ECUs within the vehicle, and possibly the vehicle itself.

Uptane Goals

- Prevent known attacks on software update systems
- Provide compromise resilience and security by design
- Minimize damage from a compromised signing key or repository

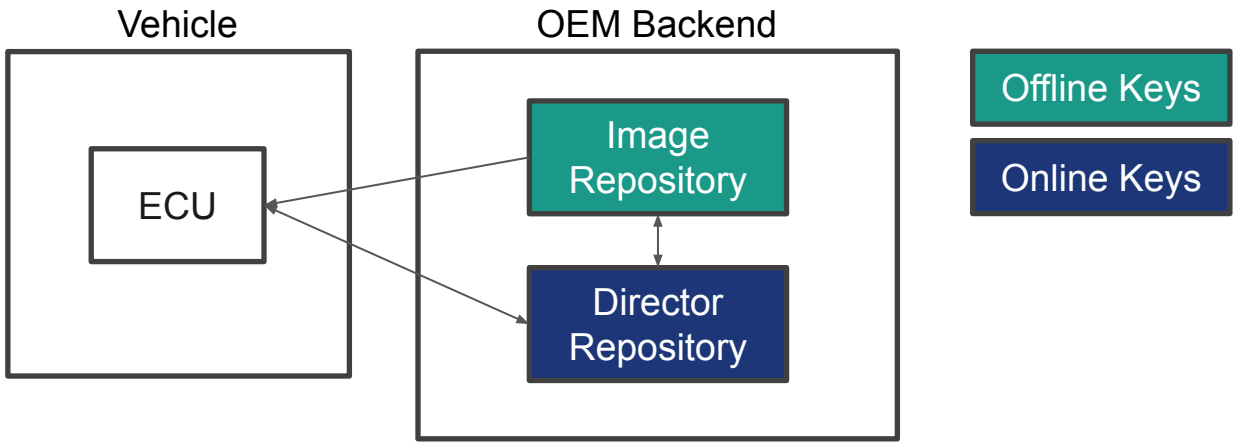
Offline and Online Key Benefits

The OEM needs to tell ECUs which software is authentic and should be installed

Online Keys	**Offline Keys**
Interactive signing	One-time signing
Addresses real-time security requirements	Strong compromise resistance

Uptane

Offline and Online Keys

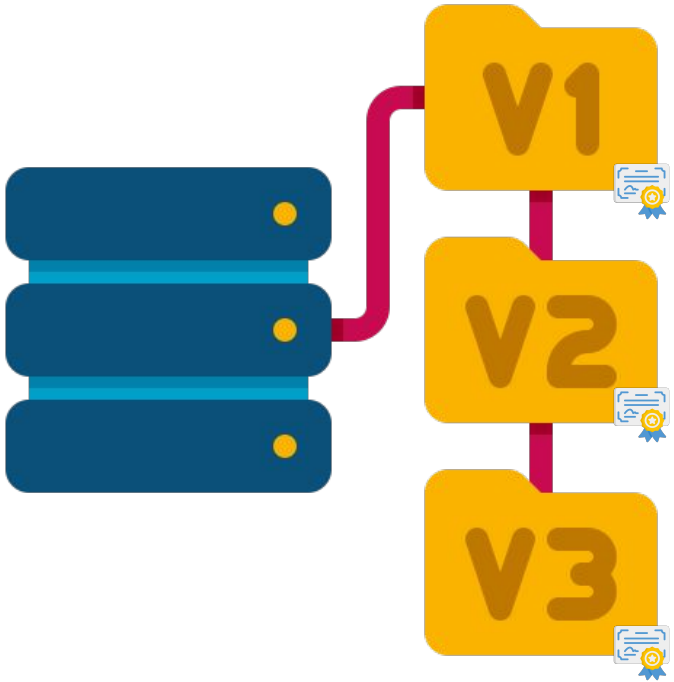


Uptane uses two repositories to provide OEMs with both **security** and **flexibility**!

Image Repository

Repository of validated and released software images

1) Human managed
2) Offline keys
3) Infrequent updates
4) Provides flexible delegation for image signing



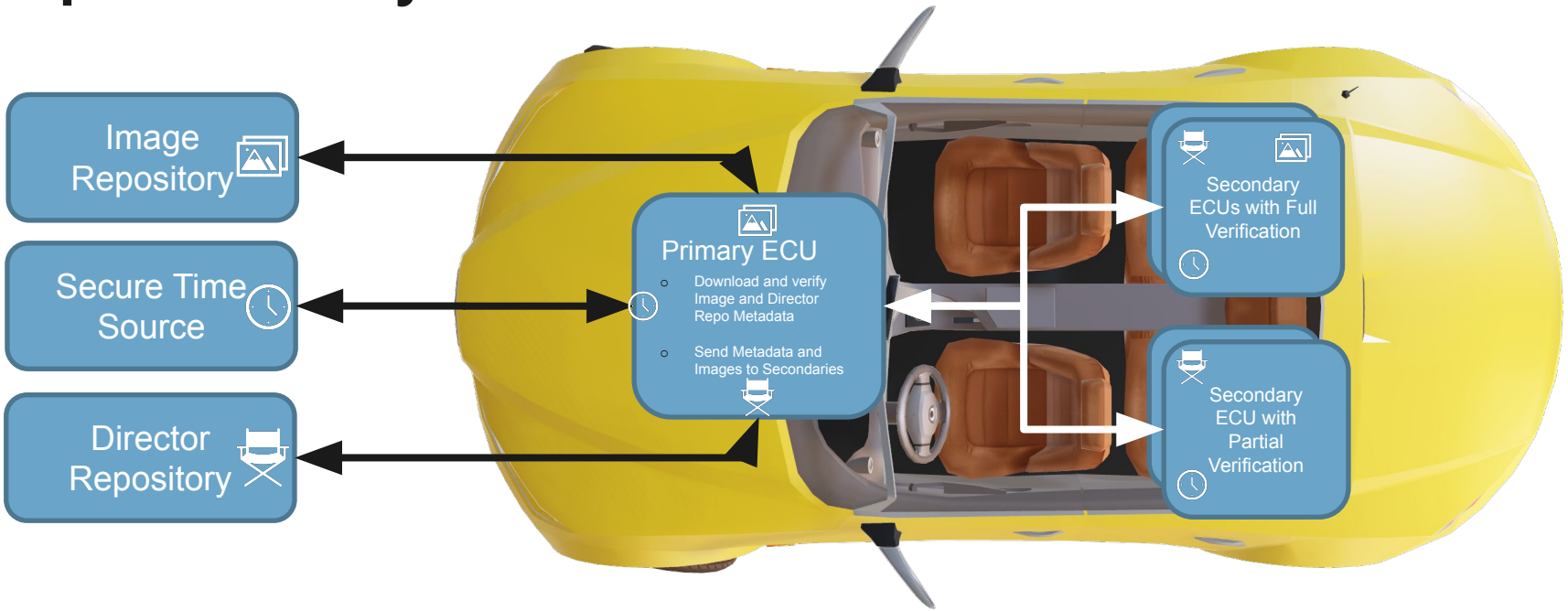
Director Repository

Allows OEM to control which software should be installed in which vehicle

1) Automated
2) Online keys
3) Frequent requests
4) Generates signed vehicle specific manifest
5) Works in coordination with a Vehicle Configuration Database

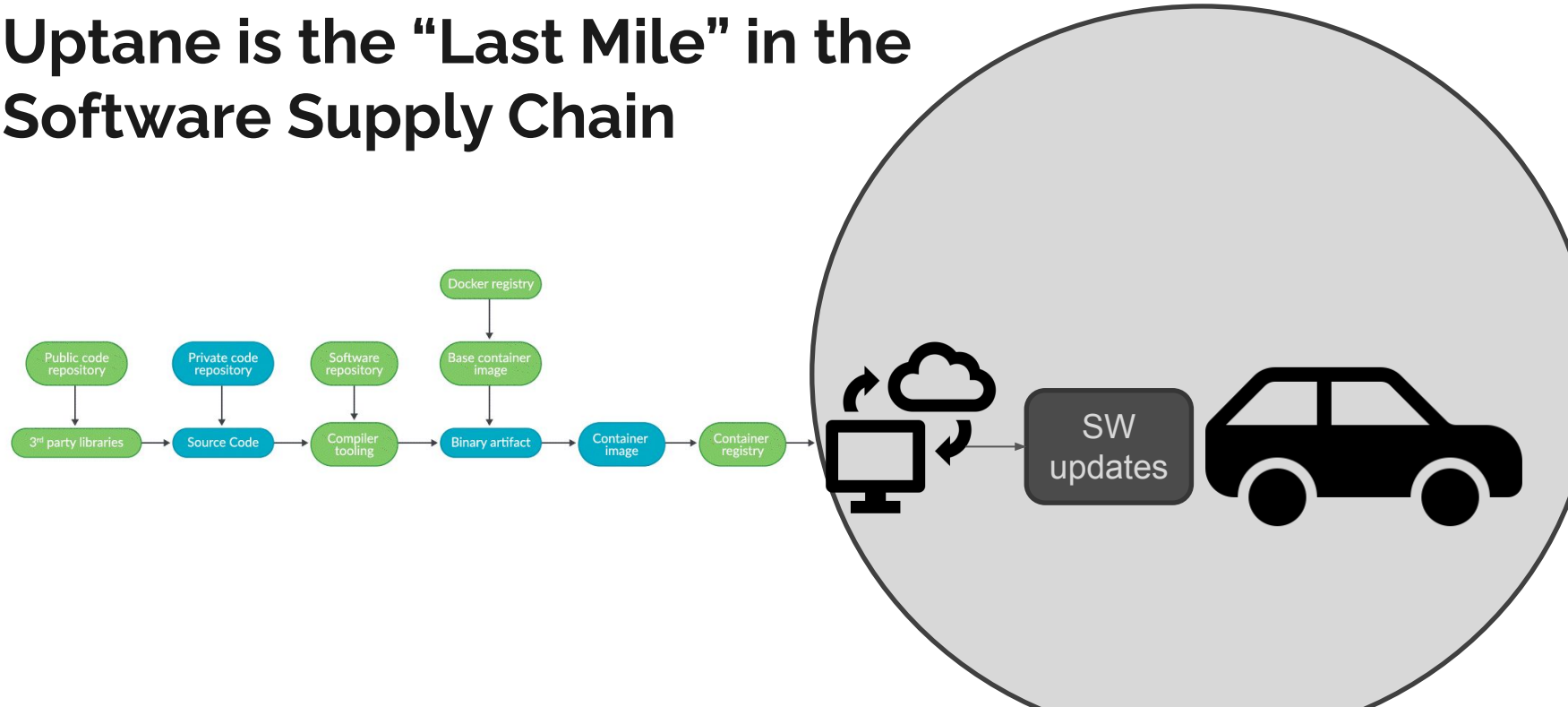
Uptane

Uptane Ecosystem



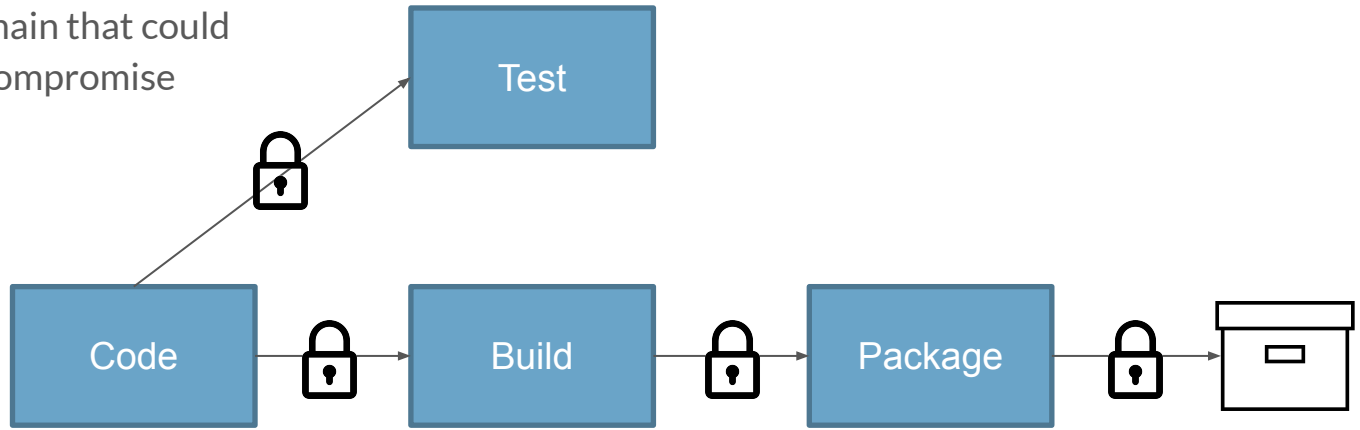
Uptane

Uptane is the “Last Mile” in the Software Supply Chain



Threat Targets in the Software Supply Chain

Verifiably protect steps in software supply chain that could be vulnerable to compromise

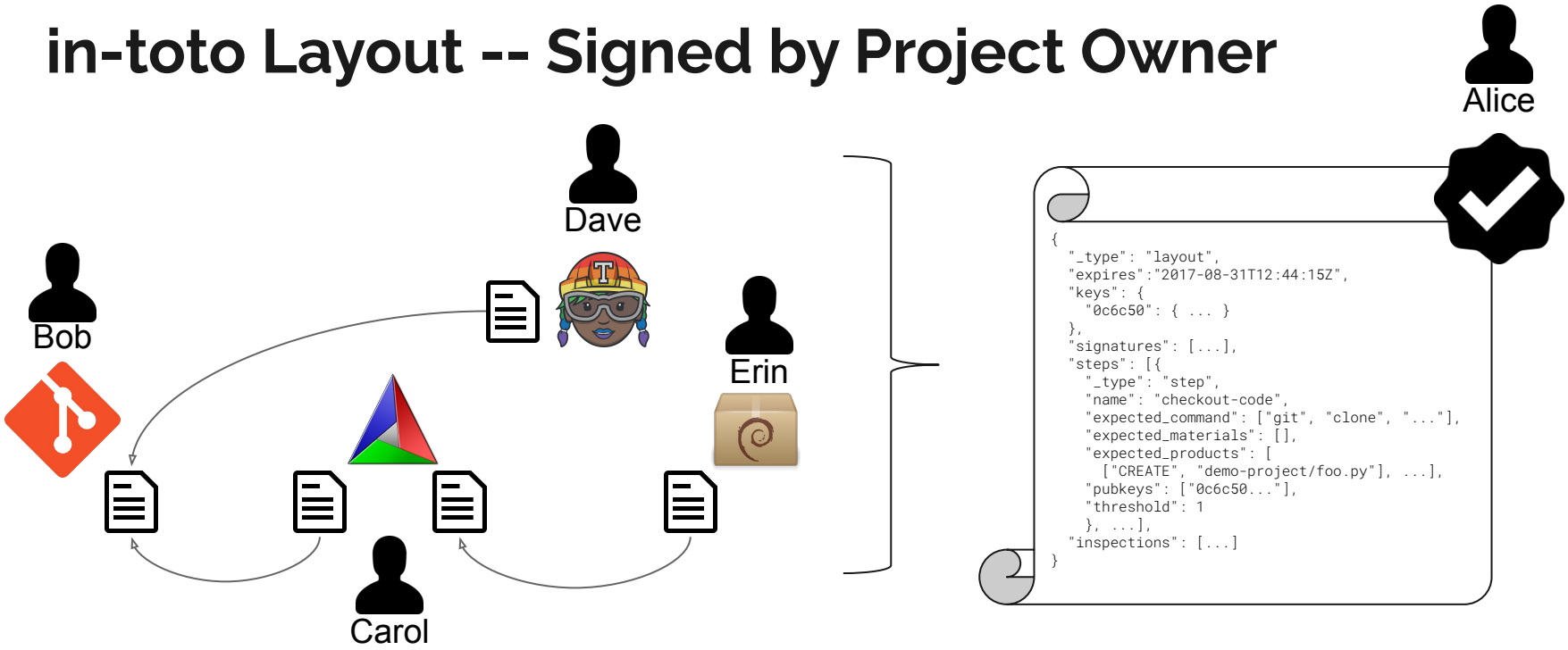


in-toto

- Verifiably define the steps of the software supply chain
- Verifiably define the authorized actors
- Guarantee everything happens according to definition and nothing else

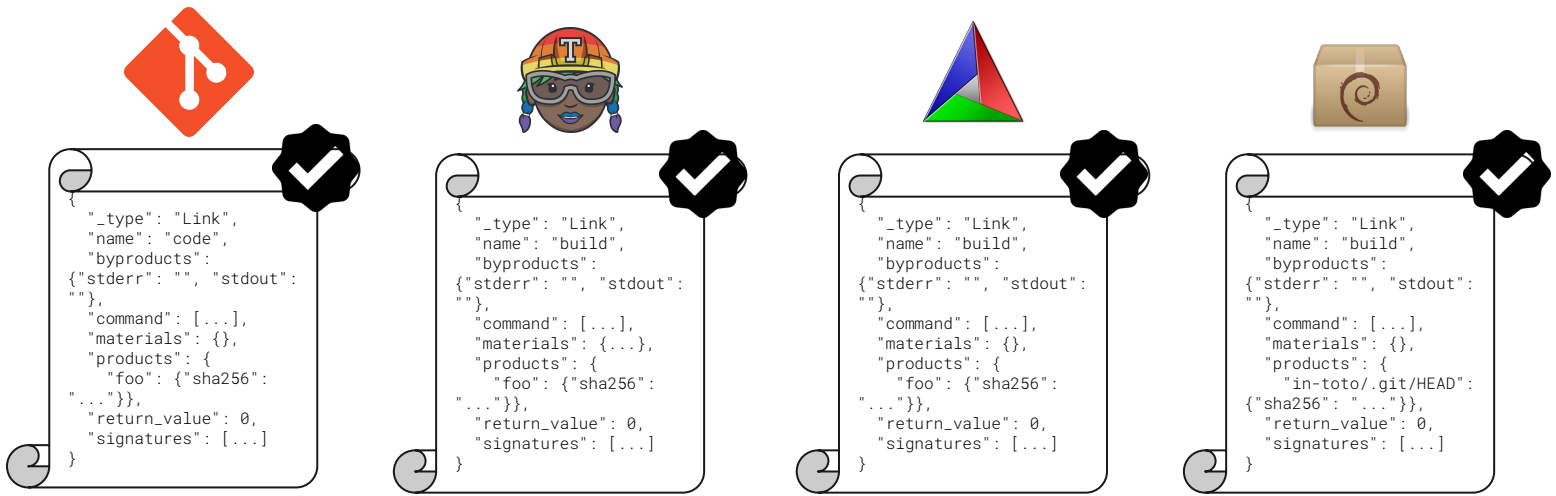
Uptane

in-toto Layout -- Signed by Project Owner



in-toto Links -- Signed Evidence for each Step

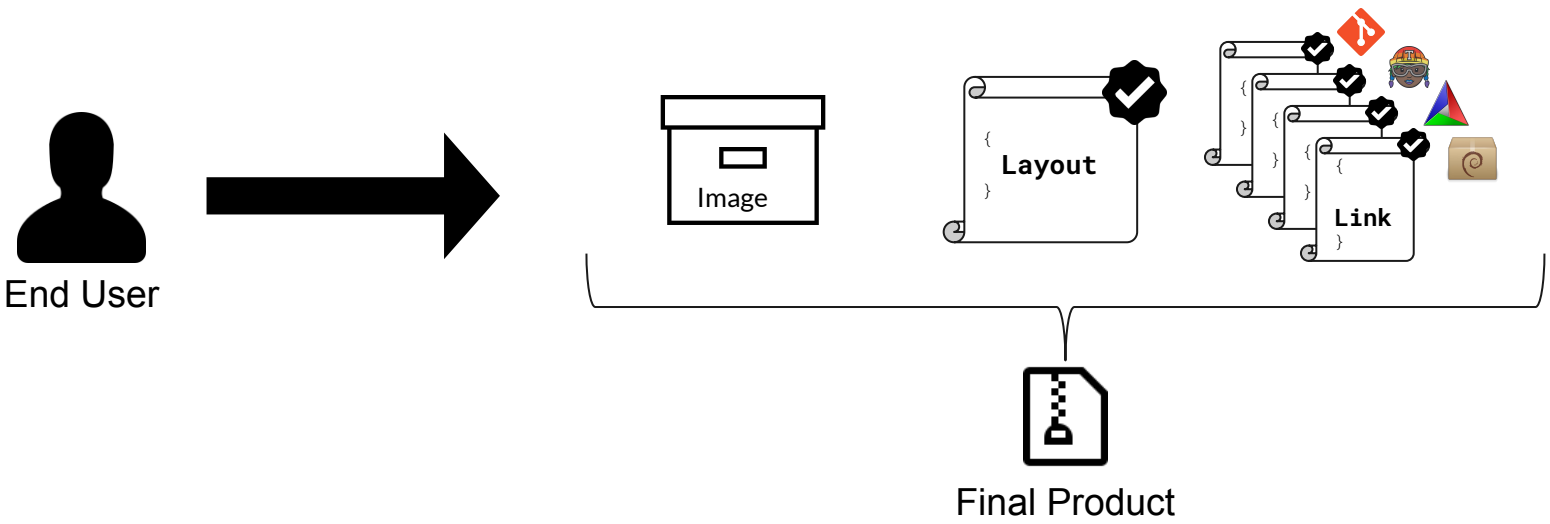
```
$ in-toto-run -- ./do-the-supply-chain-step
```



Uptane

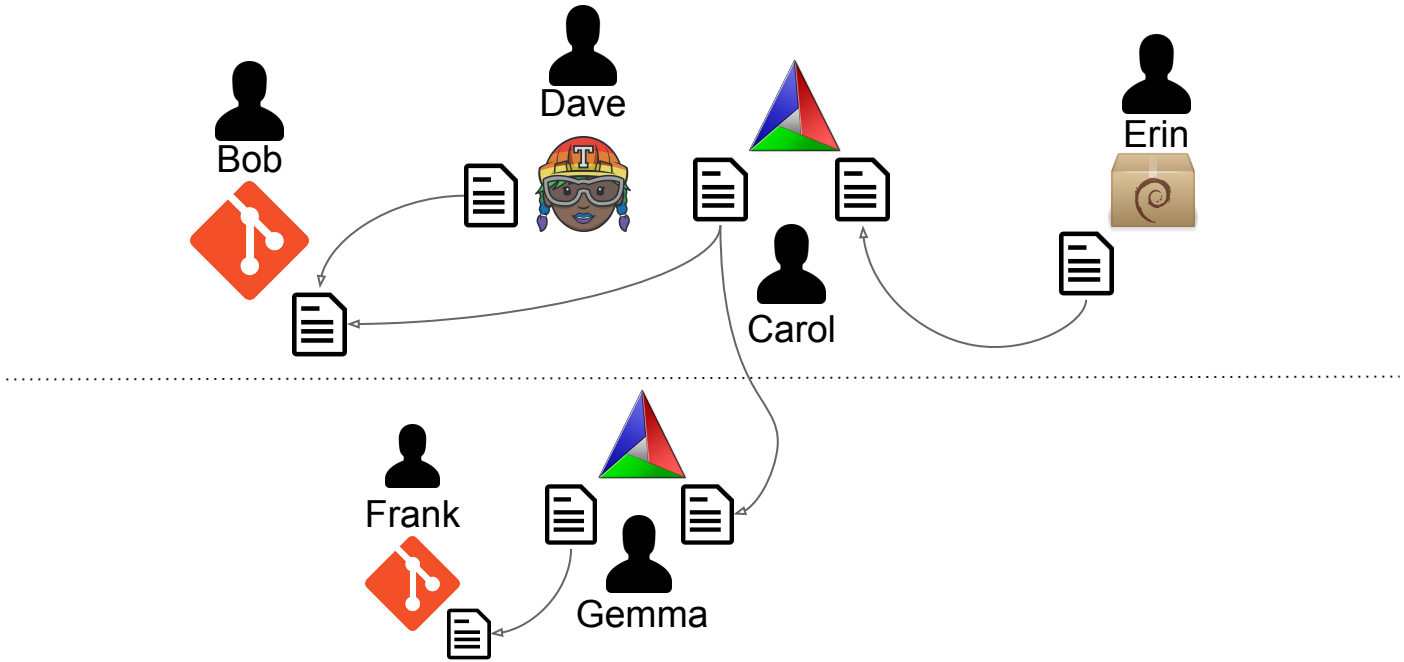
in-toto Verification

```
$ in-toto-verify --layout <layout> --key <pub key>
```



Uptane

in-toto Protects Complex Supply Chains



Scudo = in-toto + Uptane

- Delivers metadata for all images securely before installation
- Enforce policies about the flow of artifacts through the supply chain
- Identifies responsibilities for in-toto verification on vehicle ECUs
- Protects complex vendor supply chains

PURE 3 Extends Uptane with Scudo

- Adopted as a formal enhancement to the Uptane Standard in March 2023
- Integrates in-toto into the automotive supply chain
- Provides protection for vehicles with constrained ECUs
- https://github.com/uptane/pures/blob/main/pure3.md

Uptane Timeline 2023

1st quarter 2023	2nd quarter 2023	3rd quarter 2023	4th quarter 2023
This workshop	Release V.2.1.0 of Standard and Deployment Best Practices	Hold virtual workshop in connection with escar Europe)	Release V.2.2.0 of Standard and Deployment Best Practices
Launch “Uptane Experience” stories by posting the first video and soliciting other contribution	Hold in-person (or hybrid) workshop in the Detroit area in connection with escar USA (June 23, 2023)		
	Complete first batch of Uptane website revisions, including adding capability to incorporate wikis		

Uptane

Guest Speakers

Matt MacKay

Software Supply Chain

Matt leads a diverse team that focuses on governance, risk, compliance and monitoring and response activities for GM's Product Cybersecurity team. Specific responsibilities include incident response, coordinated vulnerability disclosure, cyber compliance, cyber threat intelligence analysis, OSS compliance, supply chain security, training, and process refinement.

Uptane

Charles Hart

Software Bill of Materials

Charlie is a researcher on product security and supply chain integrity at Hitachi America Ltd. He is the Chair of the Automotive ISAC SBOM Working Group and is a longtime contributor to the US Department of Commerce NTIA and DHS CISA SBOM projects. Prior to his current role, Mr. Hart held several positions as a software engineer, manager, and executive.

Uptane

Open Discussion

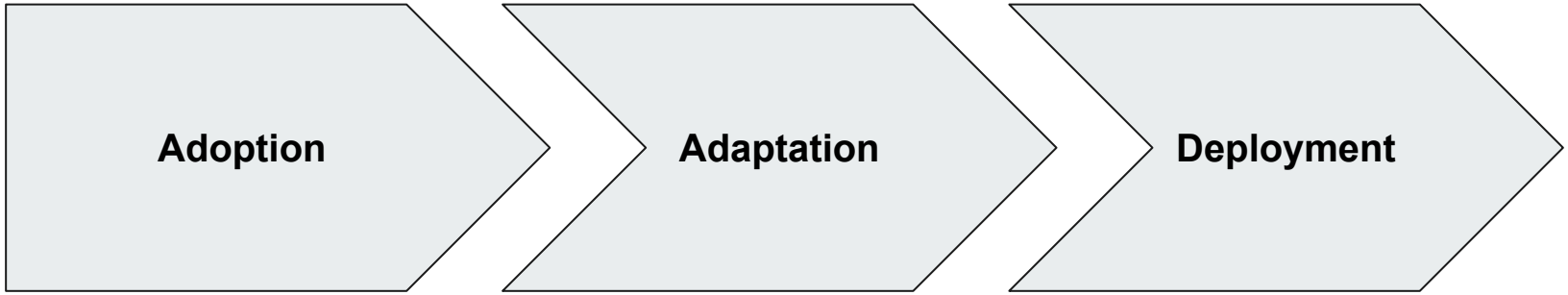
Discussion Topic Starters

Software supply chain challenges

- Software supply chain integrity
- Software supply chain tools
- Software supply chain interface agreements
- Software supply chain development chain escrow
- Reproducible builds
- Software lifecycle (end of support and decommissioning)

Next Steps

Looking Forward



Please contact us if you are interested to join, contribute and/or learn more:
https://uptane.github.io/participate.html

Uptane

Thank you.

More info at

https://uptane.github.io

Uptane

Appendix

Supplemental: Scudo = in-toto + Uptane

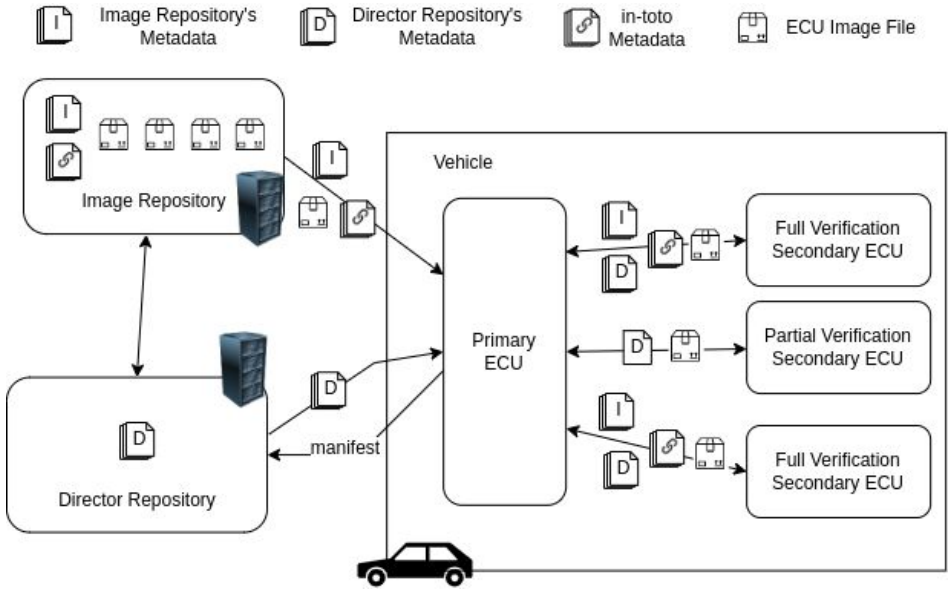
Successful integrations of in-toto and TUF in use in production:
https://www.datadoghq.com/blog/engineering/secure-publication-of-datadog-agent-integrations-with-tuf-and-in-toto/

Integrated in-toto with Uptane considers the nuances of the auto industry:
https://uptane.github.io/papers/scudo-whitepaper.pdf

More advanced specification of Scudo available as an upcoming Uptane PURE:
https://github.com/uptane/pures/pull/9

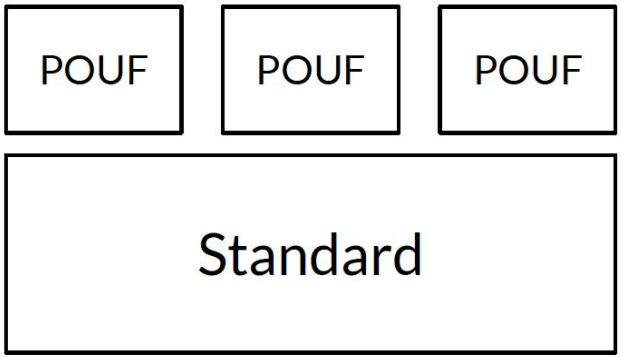
Uptane

Supplemental: Scudo = in-toto + Uptane



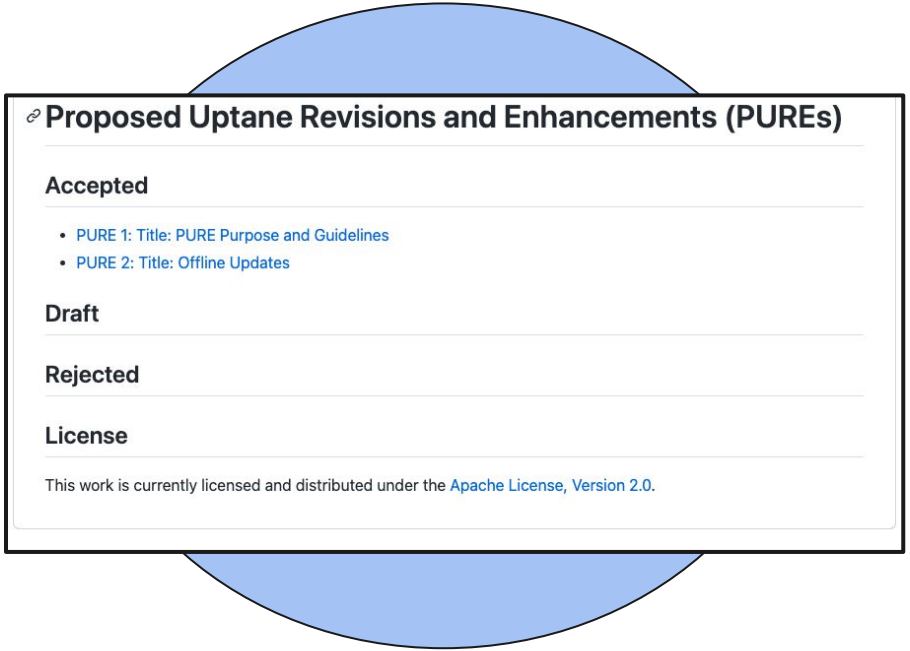
Uptane POUFs (Protocols, Operations, Usage, and Formats)

- A profile layer on top of the Uptane Standard
- Allows for interoperable Uptane implementations
- Describes an implementation
    - Choices made from the Uptane Standard and Deployment Considerations
    - Networking information, file storage and data definitions



PUREs

- Modeled on TAPs from The Update Framework
- A formal method for the community to propose additions or modifications of the Uptane Standard
- Two PUREs approved to date



Education

- Whitepapers, Videos, Tutorials, etc.
- Communicating emerging issues in automotive cybersecurity
- Promoting awareness of cybersecurity issues to the automotive community
- Addressing software supply chain issues
- Topics for upcoming whitepapers: Compliance with regulations and standards, Security issues in the use of aftermarket materials, Transitioning to Uptane