


KubeCon | CloudNativeCon

North America 2023

Secure transport for your software supply chain with TUF

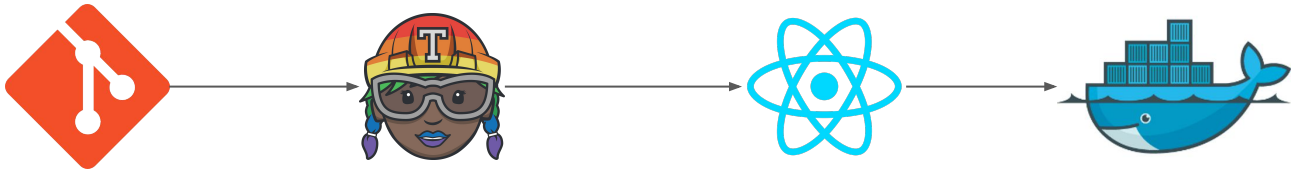
***Marina Moore** (NYU)*

***Trishank Karthik Kuppusamy** (Datadog)*

Software supply chain

software supply chain, noun

“a collection of systems, devices, and people which produce a final software product”



Source: https://docs.lib.purdue.edu/ecepubs/160/

Supply chain attacks

ESET RESEARCH

Mandiant: JumpCloud breach led to supply chain attack

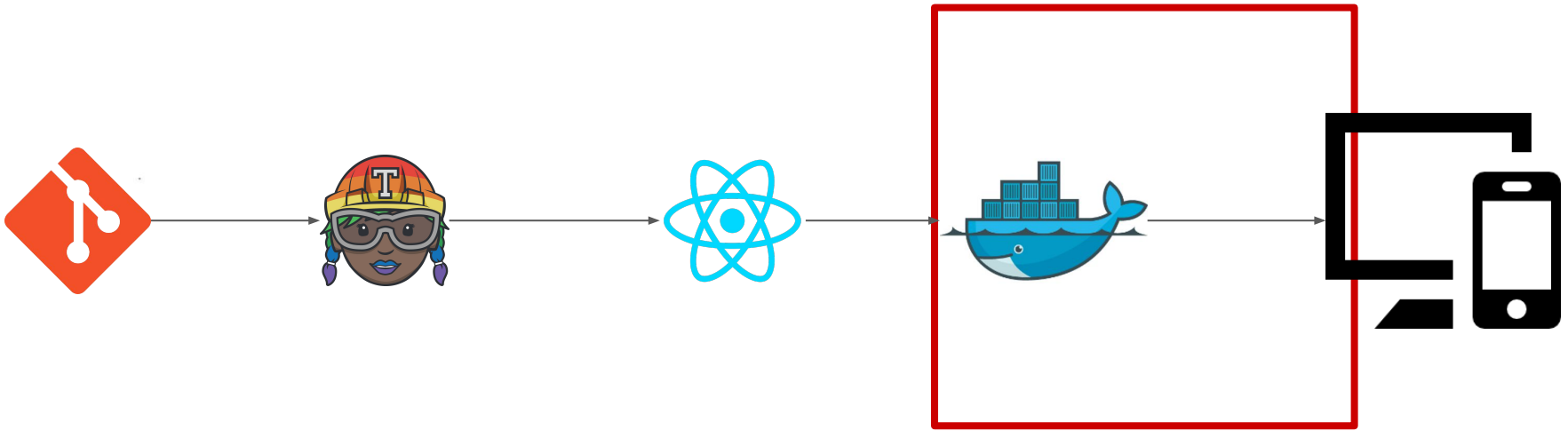
ANDY GREENBERG SECURITY APR 20, 2023 8:00 AM

The Huge 3CX Breach Was Actually 2 Linked Supply Chain Attacks

The mass compromise of the VoIP firm's customers is the first confirmed incident where one software-supply-chain attack enabled another, researchers say.

https://github.com/cncf/tag-security/tree/main/supply-chain-security/compromises

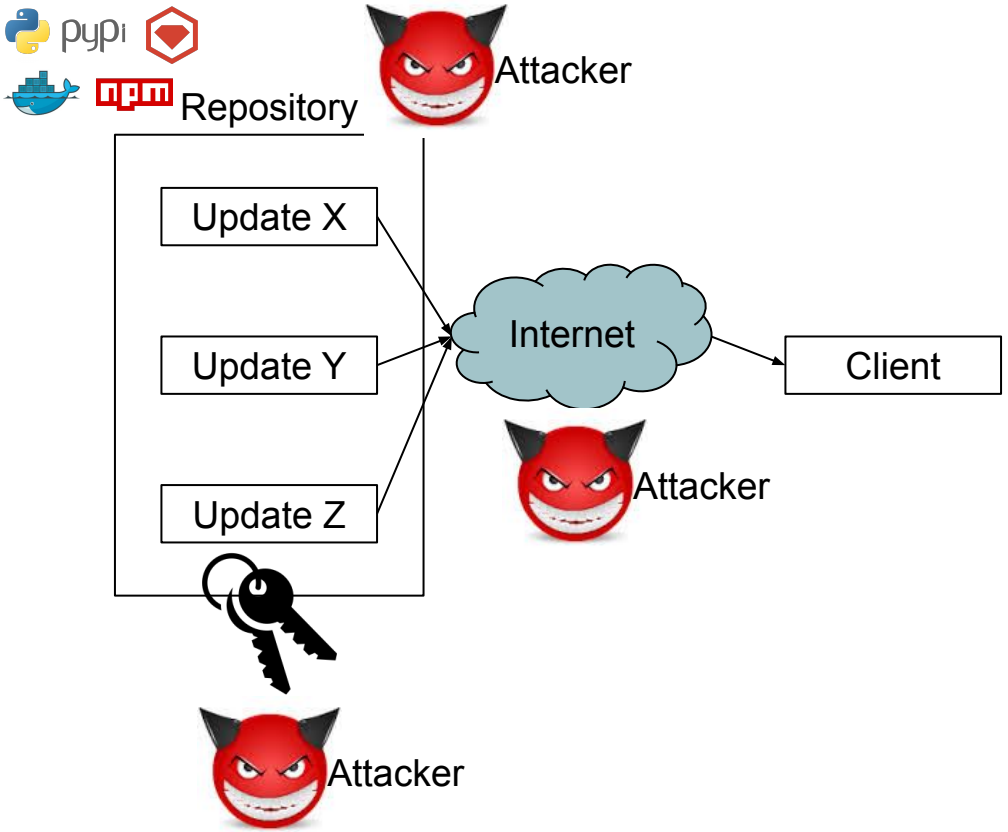
Content distribution: the last link



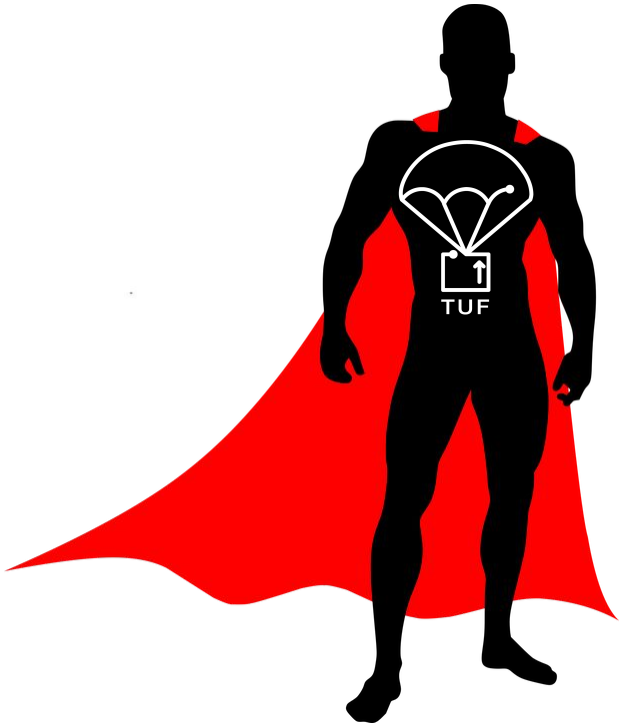
Threat model

Attackers can:

- Perform man-in-the-middle (MitM) attacks on the network
- Compromise keys used to sign updates
- Compromise repositories / servers



Goal of TUF



Protect **freshness**, **consistency**, and **integrity**

Compromise-resilience: repositories, keys, developer accounts, etc. can be compromised

- Reduce **impact** of compromise
- Allow **secure** recovery from a compromise

TUF design

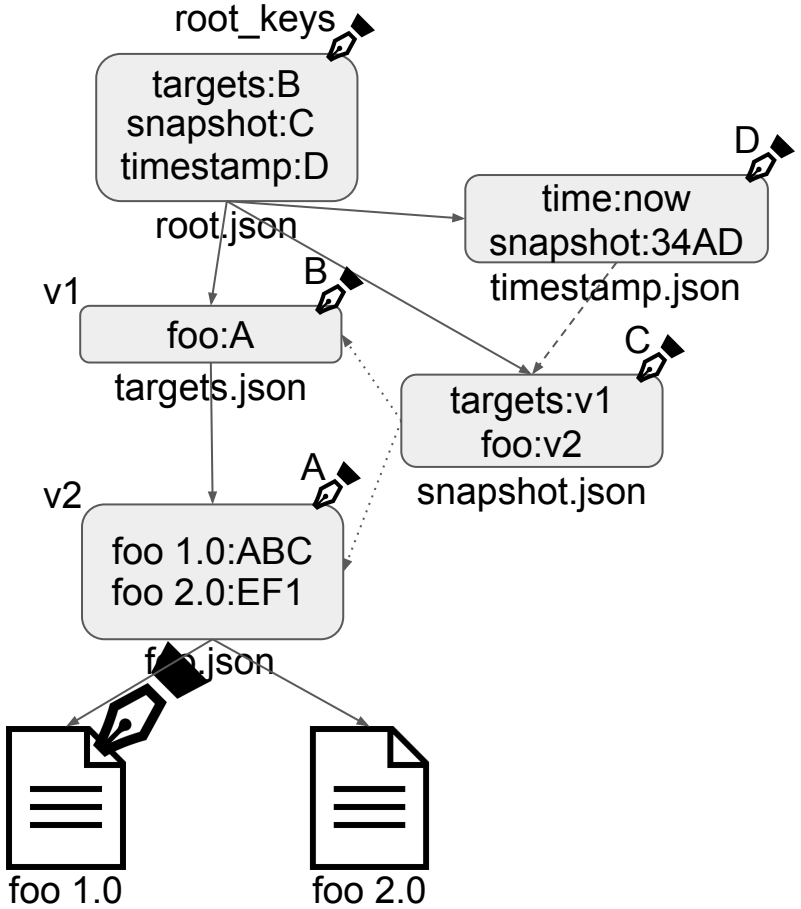
Content **integrity**

Determine trusted key

Multi-signature trust

Repository **consistency**

Freshness

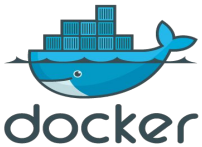


TUF Project

1 **specification**

8+ **implementations**

20+ **deployments**



Project updates

New repository implementations:

- **RSTUF**: high-volume
- **TUF-on-CI**: high-security low-volume

RSTUF

REPOSITORY SERVICE FOR TUF

go-tuf-metadata: re-write of go-tuf

gittuf: trust and key management for git repositories

TUF Augmentation Proposals (TAPs)

New features and proposals for TUF

TUF Augmentation Proposals (TAPs)

Accepted

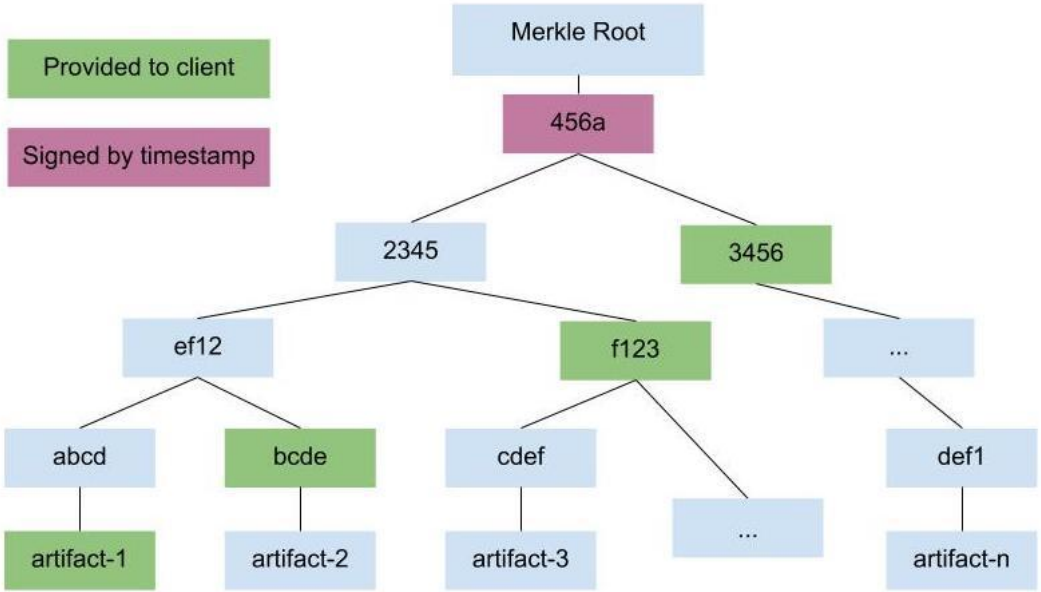
- TAP 1: TAP Purpose and Guidelines
- TAP 2: TAP template
- TAP 3: Multi-role delegations
- TAP 4: Multiple repository consensus on entrusted targets
- TAP 6: Include specification version in metadata
- TAP 9: Mandatory metadata signing schemes
- TAP 10: Remove native support for compressed metadata
- TAP 11: Using POUFs for Interoperability
- TAP 12: Improving keyid flexibility
- TAP 15: Succinct hashed bin delegations

Draft

- TAP 8: Key rotation and explicit self-revocation
- TAP 13: User Selection of the Top-Level Target Files Through Mapping Metadata
- TAP 14: Managing TUF Versions
- TAP 16: Snapshot Merkle Trees
- TAP 17: Remove Signature Wrapper from the TUF Specification
- TAP 18: Ephemeral identity verification using sigstore's Fulcio for TUF developer key management
- TAP 19: Content Addressable Systems and TUF

https://github.com/theupdateframework/taps

TAP 16

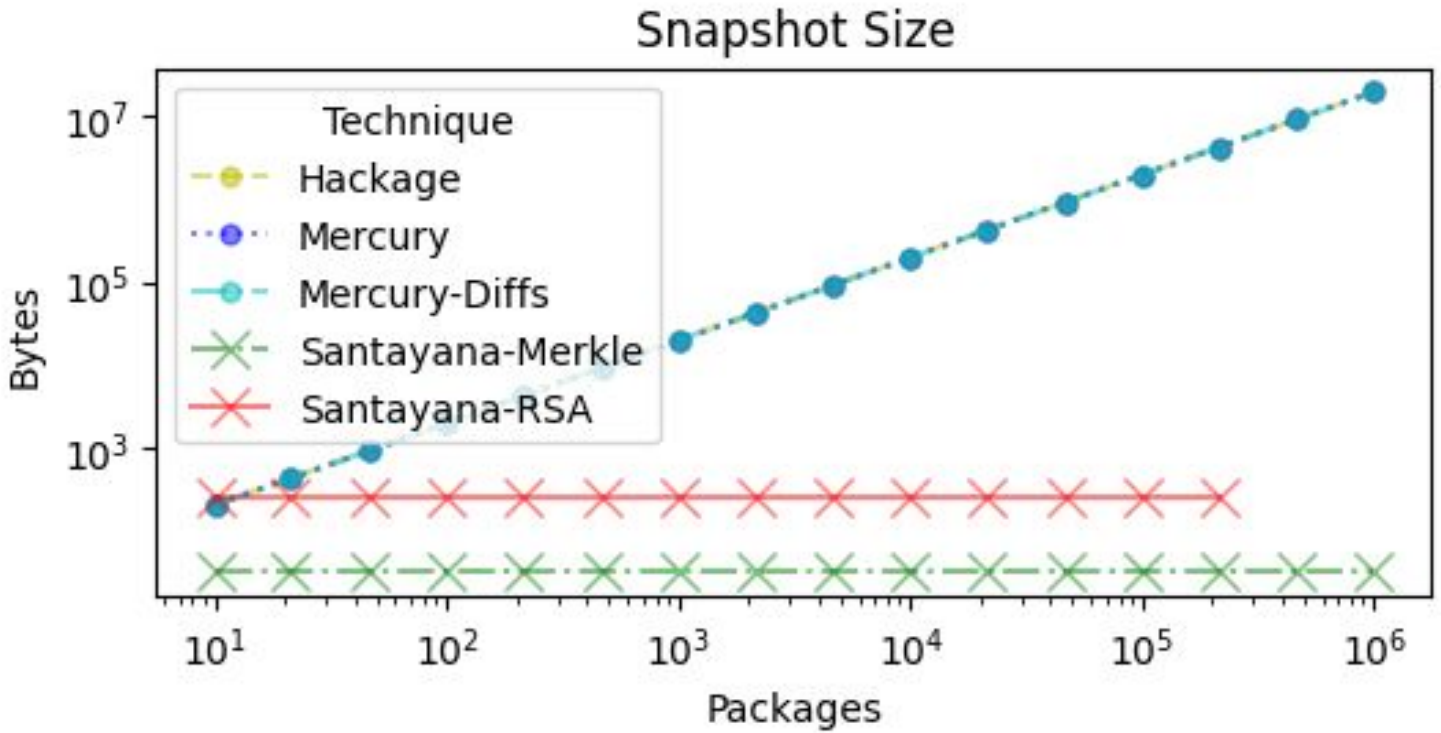


Snapshot Merkle Trees

Making snapshot metadata efficient at scale

https://github.com/theupdateframework/taps/blob/master/tap16.md

TAP 16


Snapshot Size
Technique
Hackage
Mercury
Mercury-Diffs
Santayana-Merkle
Santayana-RSA
Bytes
10^7
10^5
10^3
10^1
10^2
10^3
10^4
10^5
10^6
Packages

TAP 18

Ephemeral identity verification using sigstore's Fulcio for TUF developer key management

Simplify developer signatures

https://github.com/theupdateframework/taps/blob/master/tap18.md
https://github.com/gittuf/ci-demo

TAP 19

Content Addressable Systems and TUF

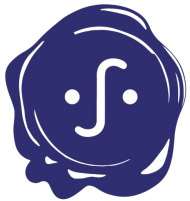
Use TUF with systems like git, IPFS, OSTree

https://github.com/theupdateframework/taps/blob/master/tap19.md

Case studies

DATADOG

Uptane

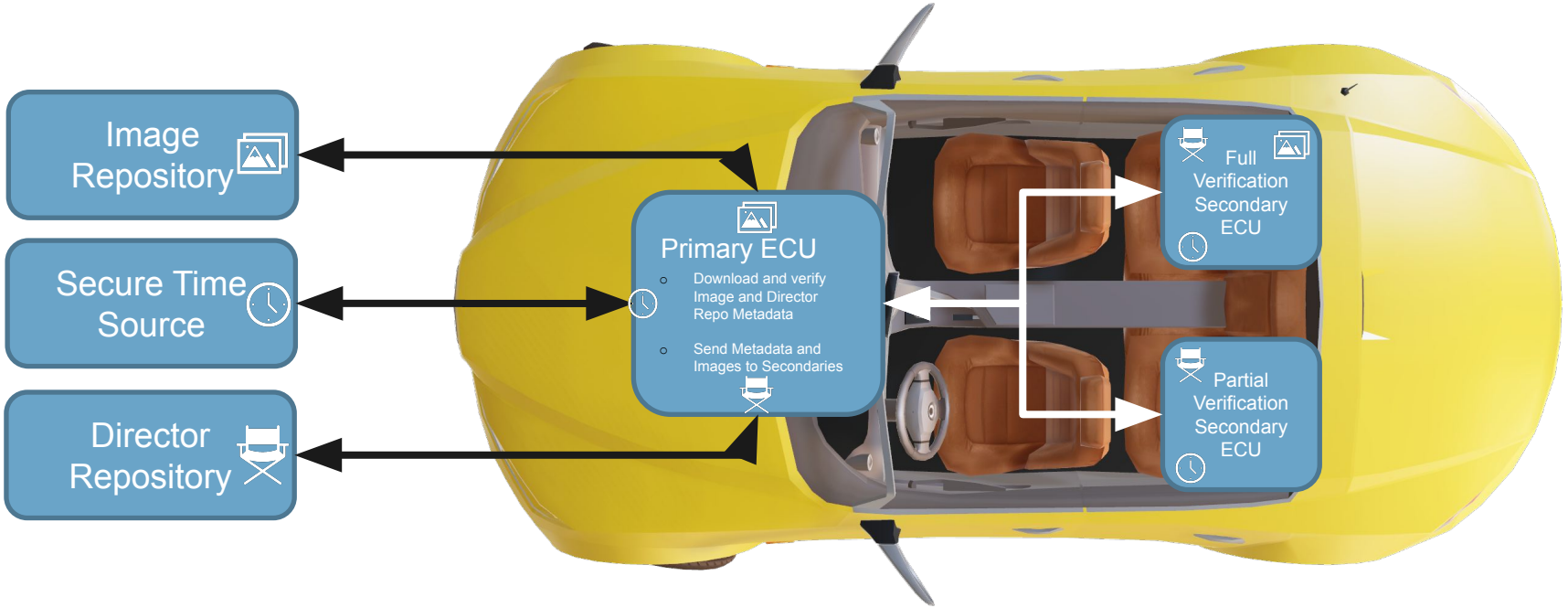


sigstore

docker

OpenPubkey

Uptane: Automotive software updates



Uptane

The Archive Framework (TAF)

Law School
University of Wisconsin-Madison

Search

All Features In the Media Faculty Students Alumni Library

UW Law's BJ Ard Helps Lead National Science Foundation Project To Safeguard U.S. Laws Against Cyberattacks

University of Wisconsin Law School is helping lead the way to develop new technologies that secure the "digital legal supply chain" – the processes by which laws and legal information are recorded, stored, updated and distributed electronically – thanks to a $1.2 million grant from the National Science Foundation (NSF).

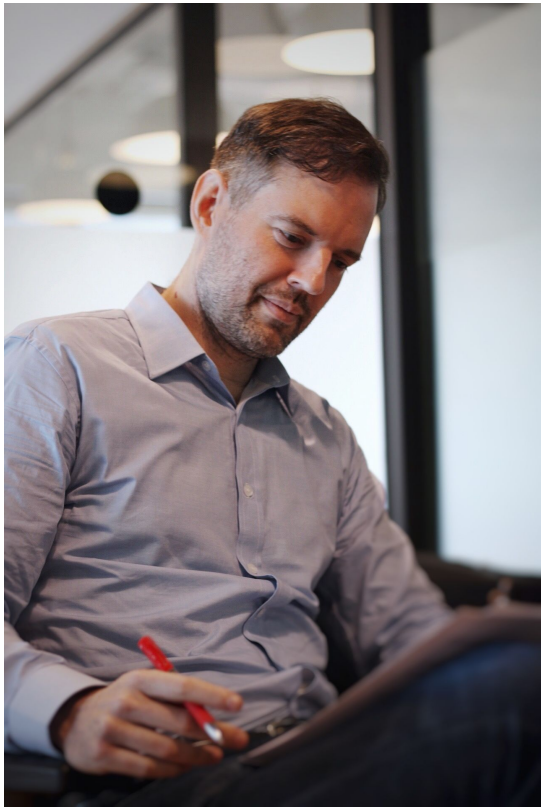
BJ Ard, associate professor at UW Law School, will be collaborating with Justin Cappos, associate professor at the New York University's Tandon School of Engineering, and the Open Law Library on the four-year project, "Defending the Supply Chain of Democracy: Towards a Cryptographically Verified and Authenticated Network of Laws."

This project builds on tools pioneered by Cappos. Extending his prior security framework, The Update Framework (TUF), Cappos began collaborating with the non-profit Open Law Library to create The Archive Framework (TAF) in 2019. TAF is a variation of TUF specifically designed to enhance the security of legal materials published by Open Law Library – a digital platform for governments to publish laws online – protecting them from cyberattacks and potential threats from within.

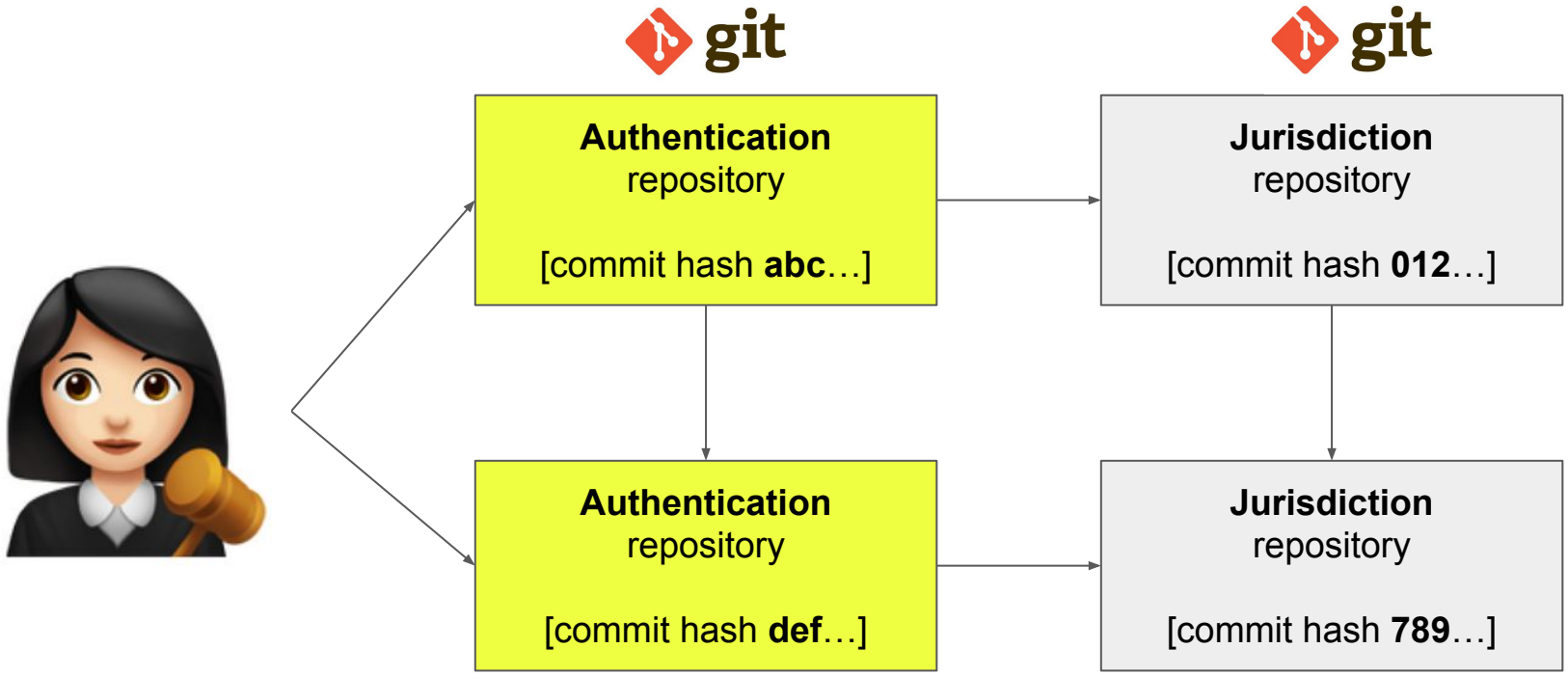
Seven U.S. jurisdictions, including the District of Columbia and the City of San Mateo, currently use TAF through partnerships with Open Law Library, with another four jurisdictions pending.

Under the new NSF grant, the team will introduce improvements within TAF. Team members will focus on finding long-term solutions for securely distributing, archiving and accessing authenticatable laws. Additionally, they plan to integrate authentication systems into the legislative process, providing auditable assurances that passed laws align with the intentions of elected officials.

The Archive Framework (TAF)

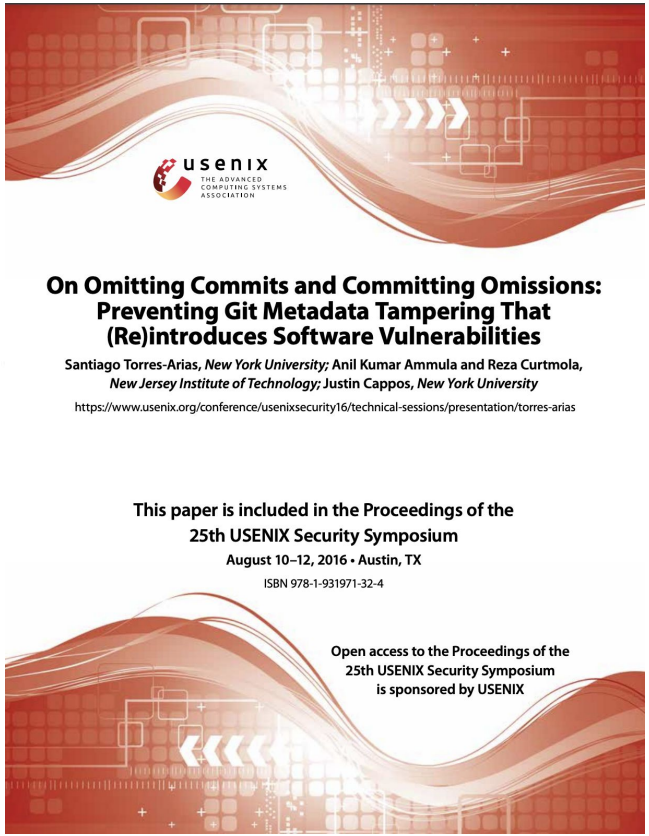


TAF: Authorized git updates



The Archive Framework (TAF)

gittuf



usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

On Omitting Commits and Committing Omissions: Preventing Git Metadata Tampering That (Re)introduces Software Vulnerabilities

Santiago Torres-Arias, *New York University;* Anil Kumar Ammula and Reza Curtmola, *New Jersey Institute of Technology;* Justin Cappos, *New York University*

https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/torres-arias

This paper is included in the Proceedings of the 25th USENIX Security Symposium

August 10–12, 2016 • Austin, TX

ISBN 978-1-931971-32-4

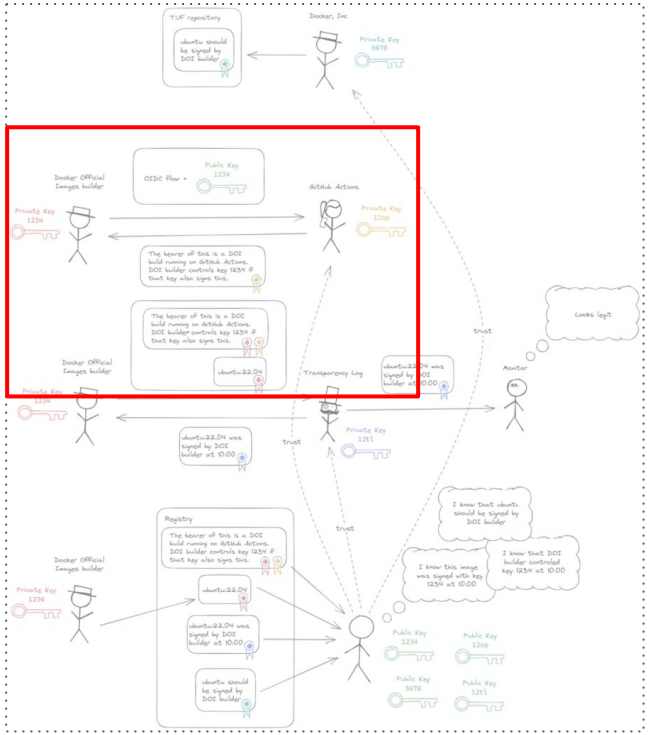
Open access to the Proceedings of the 25th USENIX Security Symposium is sponsored by USENIX

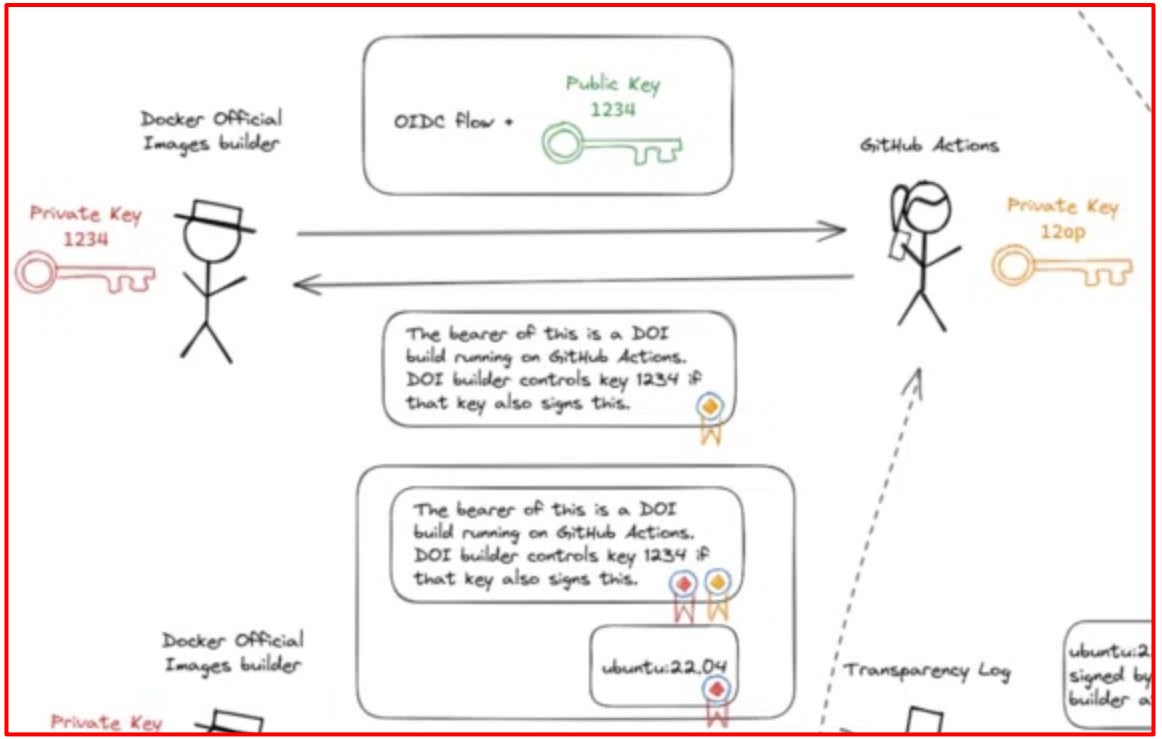
[gittuf]


```
{
    "keys": {
        "aditya@saky.in::https://github.com/login/oauth": {
            "keyid_hash_algorithms": null,
            "keytype": "sigstore-oidc",
            "keyval": {
                "identity": "aditya@saky.in",
                "issuer": "https://github.com/login/oauth"
            },
            "scheme": "fulcio",
            "keyid": "aditya@saky.in::https://github.com/login/oauth"
        }
    },
    "roles": [
        {
            "name": "protect-main",
            "paths": [
                "git:refs/heads/main"
            ],
            "terminating": false,
            "keyids": [
                "aditya@saky.in::https://github.com/login/oauth"
            ],
            "threshold": 1
        },
        {
            "name": "gittuf-allow-rule",
            "paths": [
                "*"
            ],
            "terminating": true,
            "keyids": [],
            "threshold": 1
        }
    ]
}
```

Docker Official Images + OpenPubkey

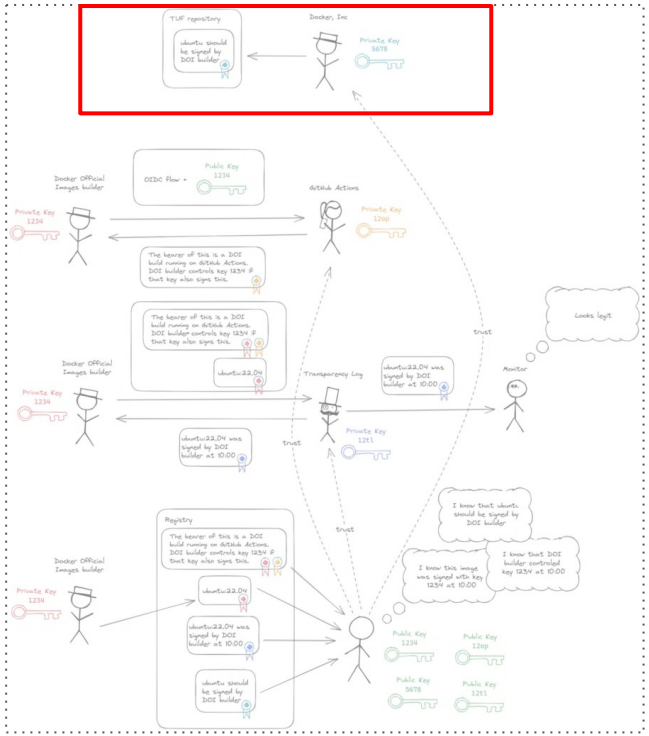
KubeCon CloudNativeCon North America 2023

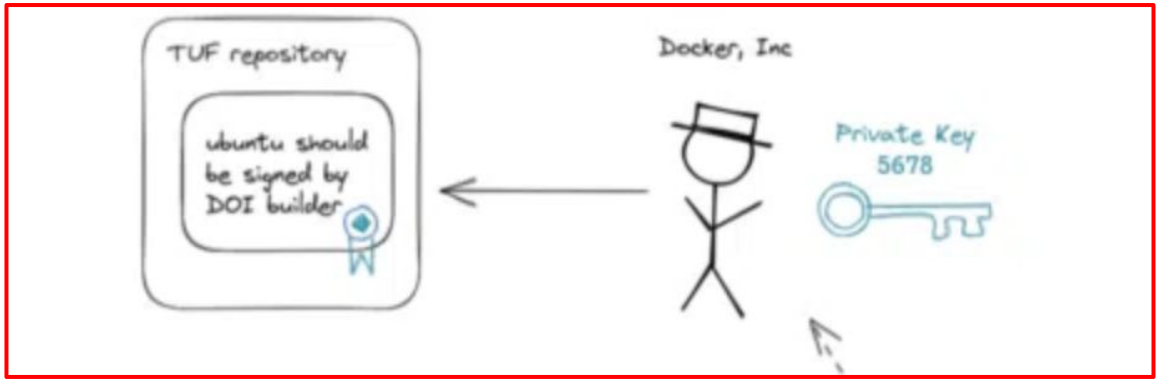




[Signing Docker Official Images Using OpenPubkey]

Docker Official Images + TUF

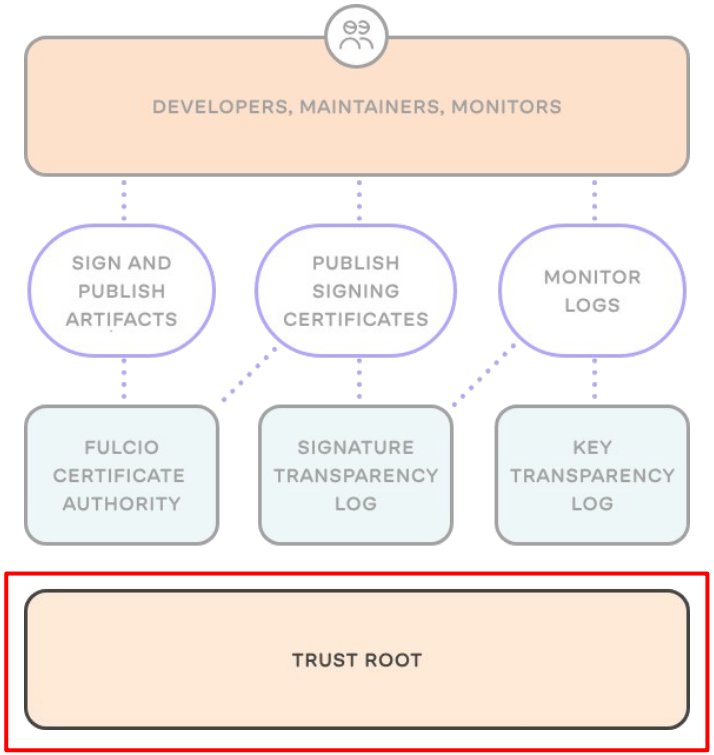


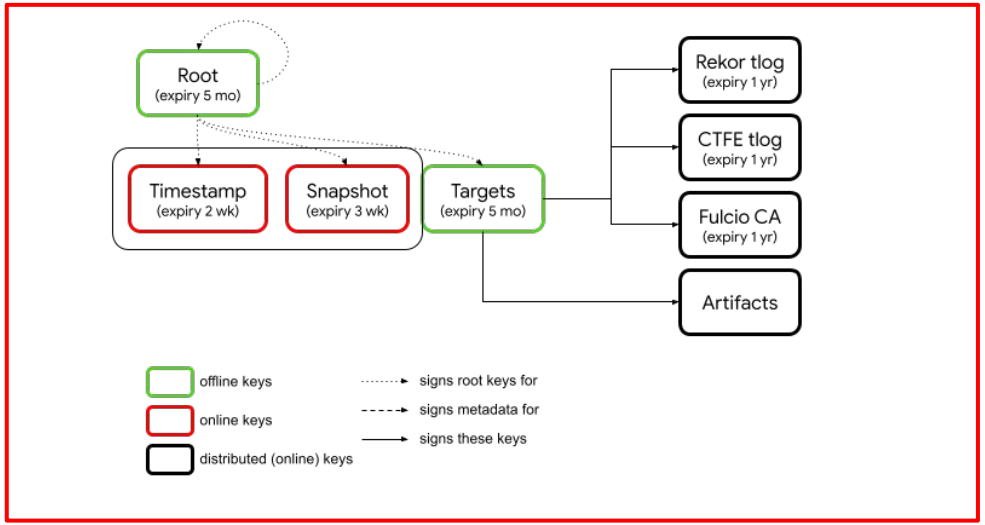


Trust policy

[Signing Docker Official Images Using OpenPubkey]

Sigstore: Trust Root



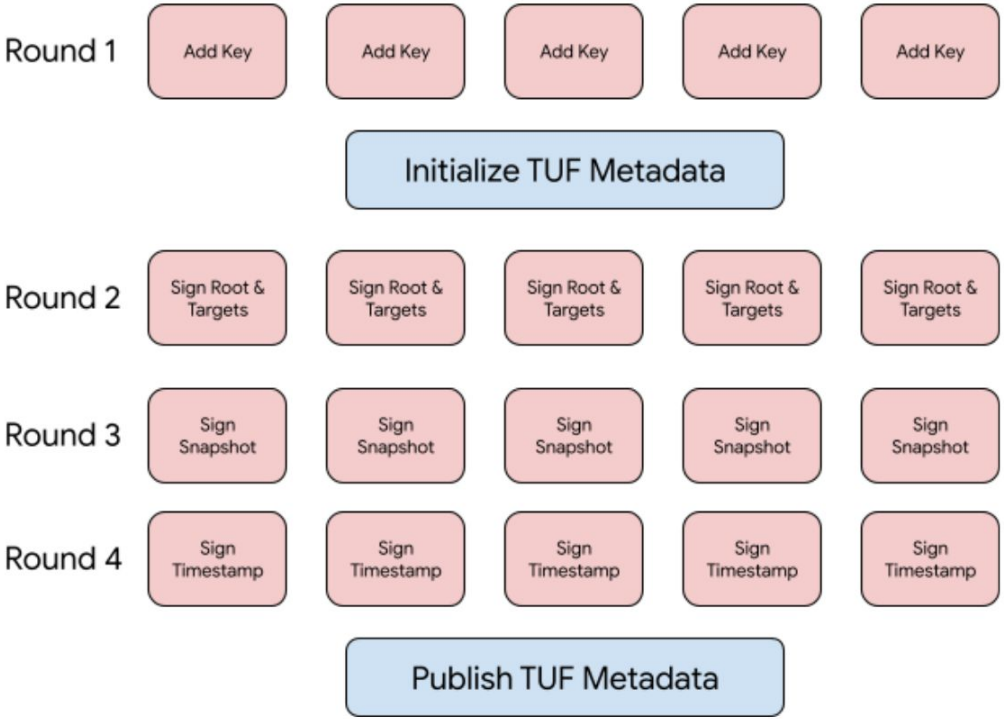


[Sigstore & TUF Root Key Ceremony]

Sigstore: Trust Root key ceremony

KubeCon CloudNativeCon North America 2023

(tuf-on-ci)

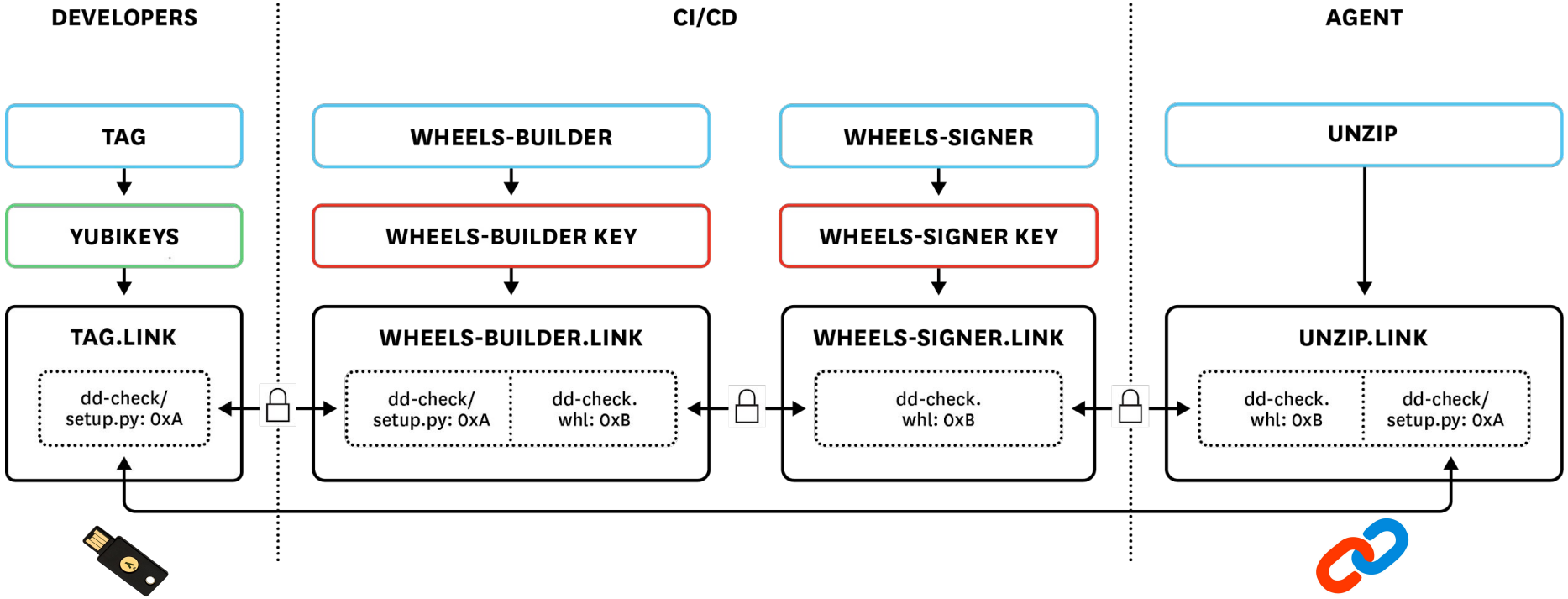


Current Keyholders

Keyholder	TUF Key ID	Yubikey Material	Term
Joshua Lock	`2e61cd0cbf4a8f45809bda9f7f78c0d33ad11842ff94ae340873e2664dc843de` (new, v5+) `75e867ab10e121fdef32094af634707f43ddd79c6bab8ad6c5ab9f03f4ea8c90` (deprecated)	18158855	July 2022 -
Bob Callaway	`7f7513b25429a64473e10ce3ad2f3da372bbdd14b65d07bbaf547e7c8bbbe62b` (new, v5+) `f505595165a177a41750a8e864ed1719b1edfccd5a426fd2c0ffda33ce7ff209` (deprecated)	15938791	June 2021 -
Dan Lorenc	`ff51e17fcf253119b7033f6f57512631da4a0969442afcf9fc8b141c7f2be99c` (new, v5+) `2f64fb5eac0cf94dd39bb45308b98920055e9a0d8e012a7220787834c60aef97` (deprecated)	13078778	June 2021 -
Marina Moore	`25a0eb450fd3ee2bd79218c963dce3f1cc6118badf251bf149f0bd07d5cabe99` (new, v5+) `eaf22372f417dd618a46f6c627dbc276e9fd30a004fc94f9be946e73f8bd090b` (deprecated)	14470876	June 2021 -
Santiago Torres-Arias	`f5312f542c21273d9485a49394386c4575804770667f2ddb59b3bf0669fddd2f` (new, v5+) `f40f32044071a9365505da3d1e3be6561f6f22d0e60cf51df783999f6c3429cb` (deprecated)	15938765	June 2021 -

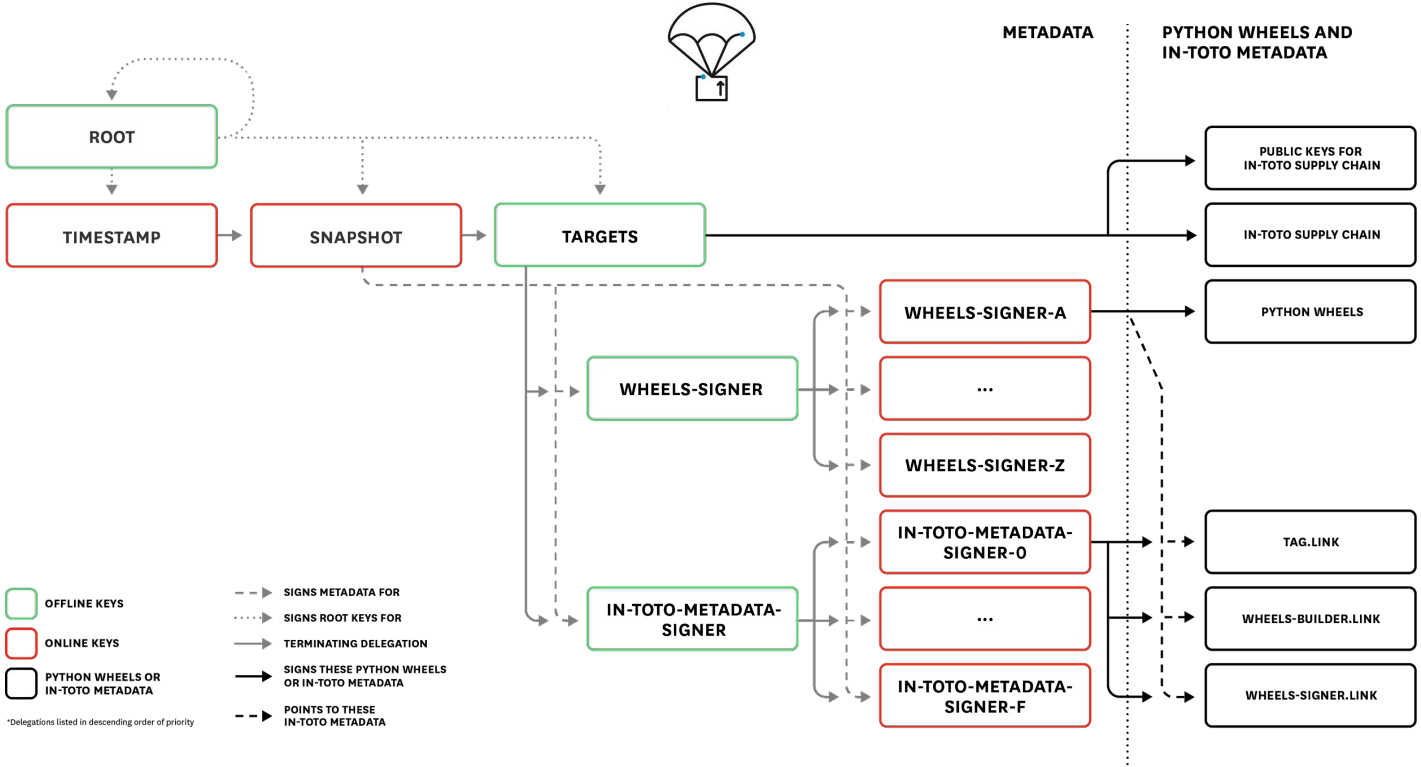
Sigstore Trust Root

Datadog: Agent Integrations



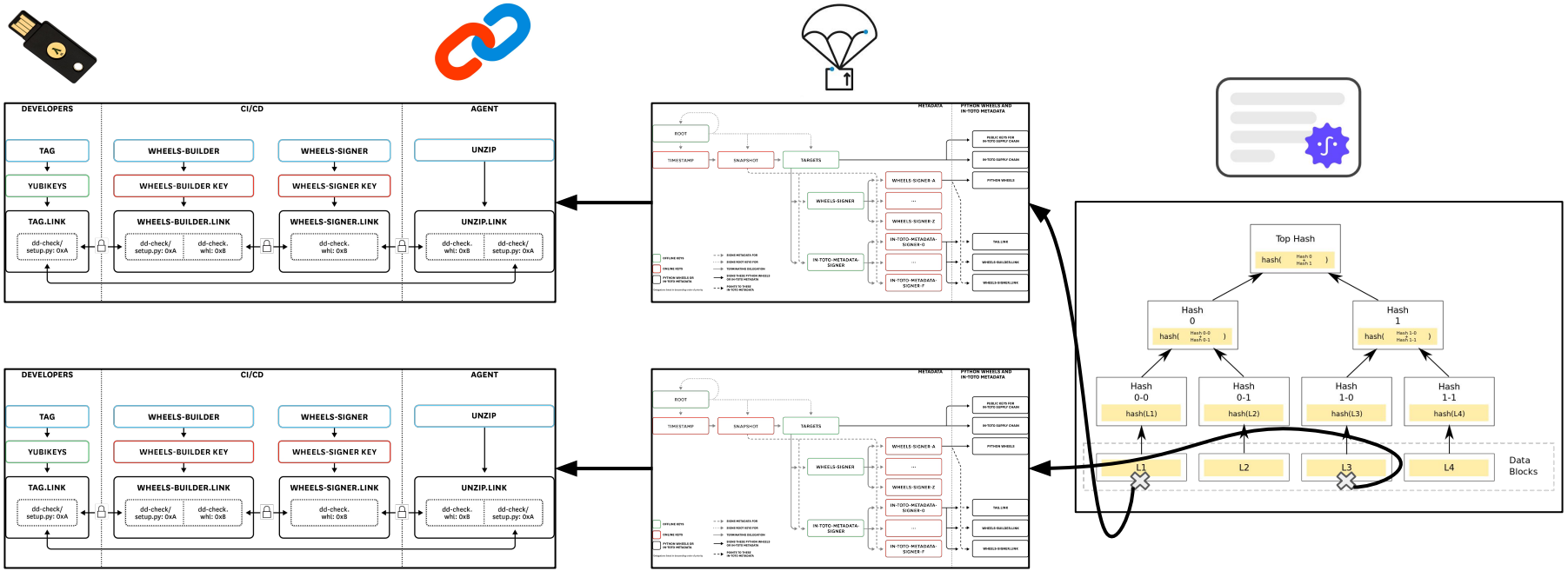
KubeCon + CloudNativeCon NA 2018 | SupplyChainSecurityCon 2021

Datadog: Agent Integrations



KubeCon + CloudNativeCon NA 2018 | SupplyChainSecurityCon 2021

Datadog: Agent Integrations



[KubeCon + CloudNativeCon NA 2018](#) | [SupplyChainSecurityCon 2021](#)

OSS package repositories: PyPI

Python Enhancement Proposals | Python » PEP Index » PEP 458

Contents

PEP 458 – Secure PyPI downloads with signed repository metadata

Author: Trishank Karthik Kuppusamy <karthik at trishank.com>, Vladimir Diaz <vladimir.diaz at nyu.edu>, Marina Moore <mm9693 at nyu.edu>, Lukas Puehringer <lukas.puehringer at nyu.edu>, Joshua Lock <jlock at vmware.com>, Lois Anne DeLong <lad278 at nyu.edu>, Justin Cappos <jcappos at nyu.edu>

Sponsor: Alyssa Coghlan <ncoghlan at gmail.com>

BDFL-Delegate: Donald Stufft <donald at stufft.io>

Discussions-To: Discourse thread

Status: Accepted

Type: Standards Track

Topic: Packaging

Created: 27-Sep-2013

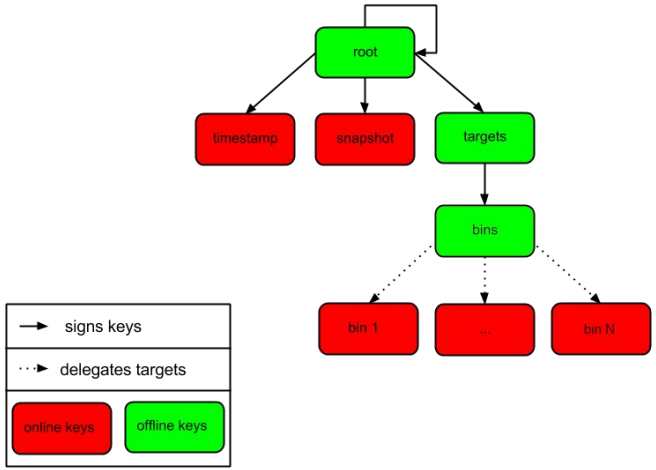
Post-History: 06-Jan-2019, 13-Nov-2019

Resolution: Discourse message

▸ Table of Contents

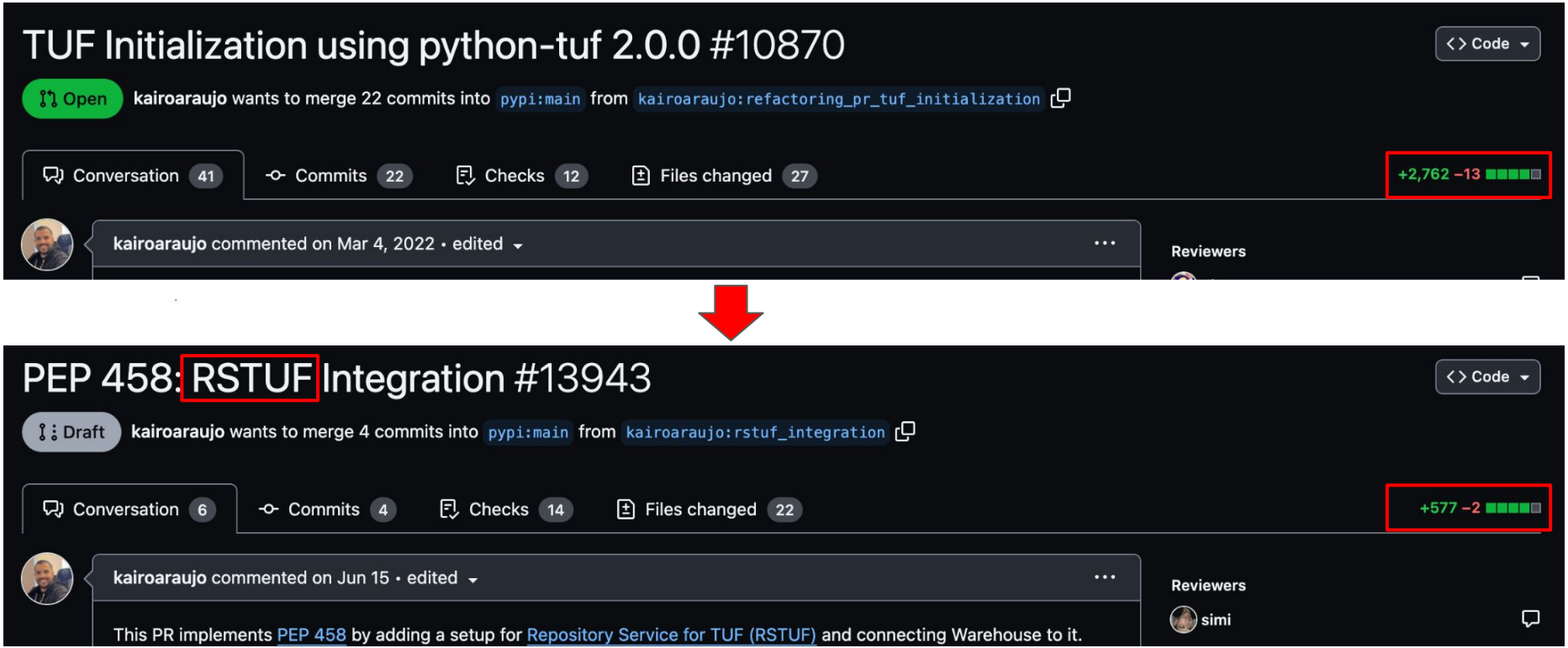
Abstract

This PEP describes changes to the PyPI infrastructure that are needed to ensure that users get valid packages from PyPI. These changes should have minimal impact on other parts of the ecosystem. The PEP focuses on communication between PyPI and users, and so does not require any action by package developers. Developers will upload packages using the current process, and PyPI will automatically generate signed repository metadata for these packages.



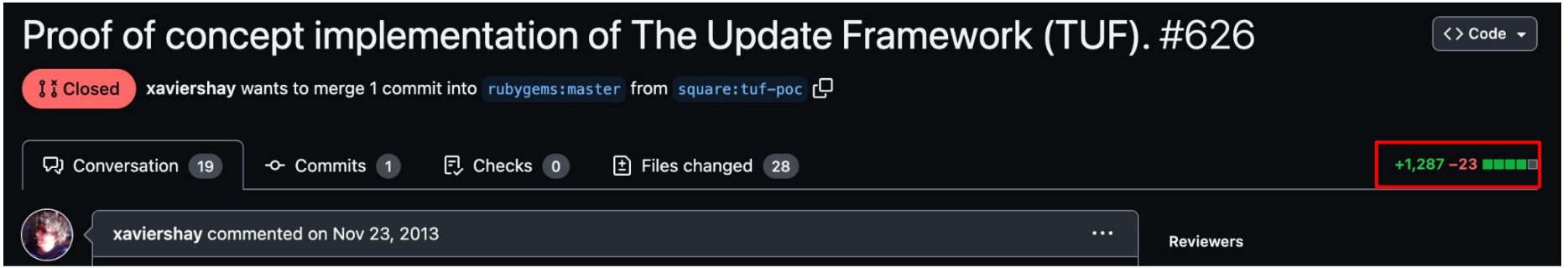
PEP 458 – Secure PyPI downloads with signed repository metadata

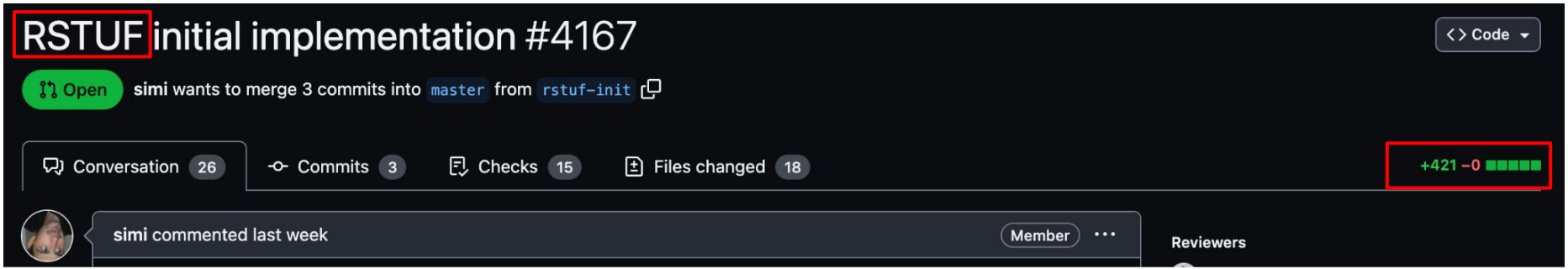
OSS package repositories: PyPI



PEP 458: RSTUF Integration #13943

OSS package repositories: RubyGems

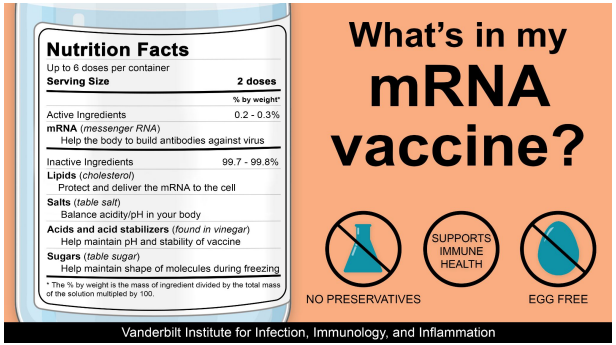




RSTUF initial implementation #4167

OSS package repositories: Robusto

KubeCon CloudNativeCon North America 2023



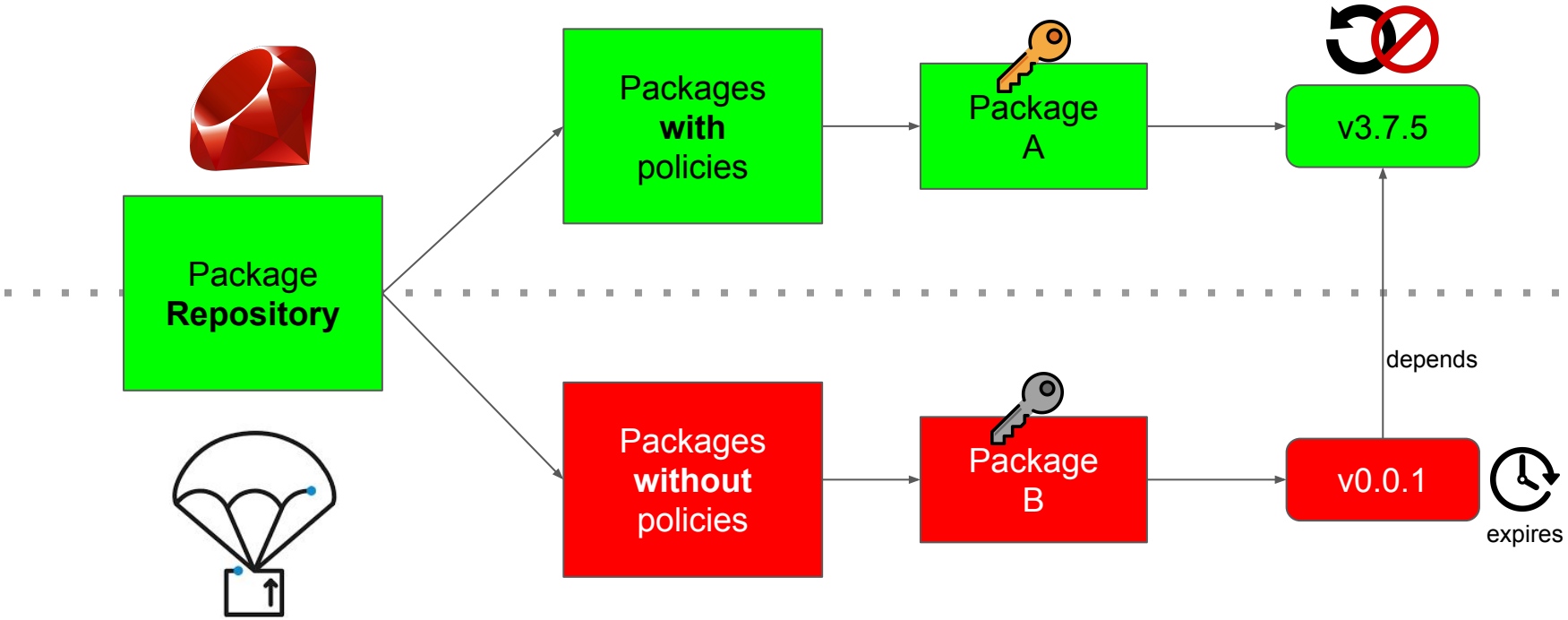
in-toto
Supply chain security

TUF
Compromise-resilience

Sigstore
Transparency

[PackagingCon 2023]

OSS package repositories: Robusto



OSS package repositories: Robusto

Feature	in-toto	TUF	Sigstore	Robusto
Attestations	✅	❌	❌	✅
Policies	✅	❌	❌	✅
Namespaces	❌	✅	❌	✅
Global **consistency**	❌	✅	❌	✅
Built-in, user-friendly **PKI**	✅	✅	❓	✅
BYOK	✅	✅	✅	✅
Ephemeral keys	❓	❓	✅	✅
Tamper-evident	✅	✅	✅	✅
Compromise-resilient	❓	✅	❓	✅
Transparency	❌	❌	✅	✅

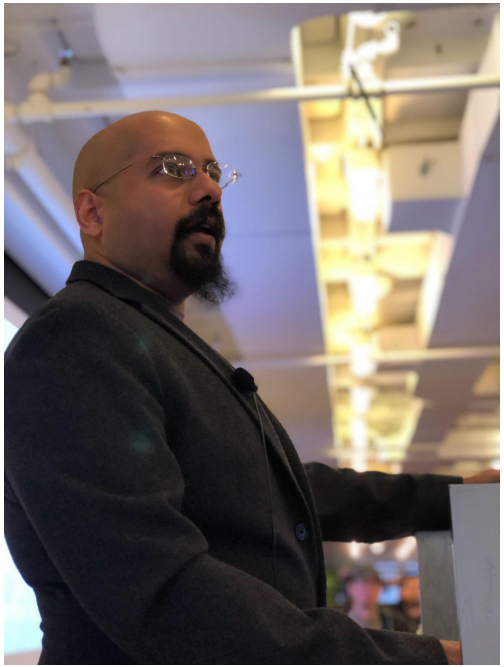
Demo

EuroPython 2023

Thanks: Q&A

NYU

marinamoore@nyu.edu



trishank@datadog.com

DATADOG