Enhancing Legal Document Security and Accessibility with TAF

Renata Vaderna, Dušan Nikolić, Patrick Zielinski, David Greisen, BJ Ard, Justin Cappos

Bio: Renata

- Former TAF lead developer (2021-2025)
- PhD, University of Novi Sad
- Former postdoc @ New York University

Law is under attack!

The authenticity and integrity of digital legal records are not guaranteed

Evidence #1: Destruction

Daryna Antoniuk

May 15th, 2025

Attack claimed by pro-Ukraine hackers reportedly erases a third of Russian court case archive

A cyberattack on Russia's national case management and electronic court filing system wiped out about a third of its case archive, according to a report by the Russian Audit Chamber.

The system, known as "Pravosudiye" (meaning "justice" in Russian), was hacked last October and was down for a month, disrupting the operation of Russian court websites, communication networks, and email services.

Source: https://therecord.media/russia-court-system-hack-third-of-case-files-deleted

Evidence #2: Compromise

US federal court filing system breached in sweeping hack, Politico reports

By **Reuters**

August 7, 2025 4:50 AM GMT+2 · Updated August 7, 2025

WASHINGTON, Aug 6 (Reuters) - The U.S. federal judiciary's electronic case filing system has been compromised in a sweeping hack that is believed to have exposed sensitive court data in several states, Politico reported on Wednesday, citing two people with knowledge of the incident.

Politico said the incident had affected the judiciary's federal case management system, which includes the Case Management/Electronic Case Files, or CM/ECF, which legal professionals use to upload and manage case documents; and Public Access to Court Electronic Records, or PACER, which provides the public with pay-for access to some of the same data.

Source: https://www.reuters.com/world/us/us-federal-court-filing-system-breached-sweeping-hack-politico-reports-2025-08-07/

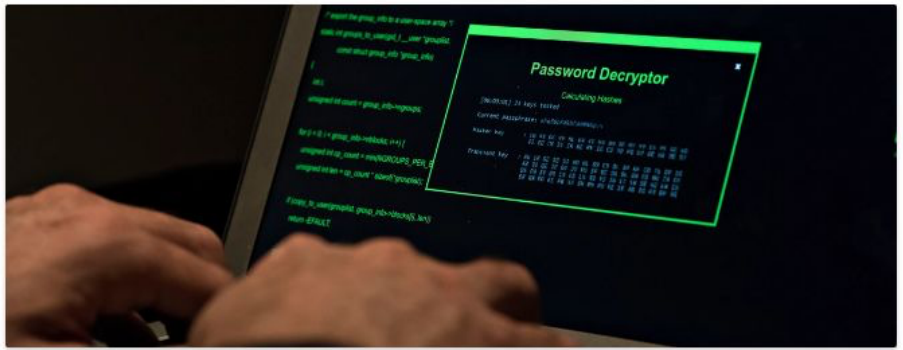
Evidence #3: Fallout

Source: https://news.bloomberglaw.com/us-law-week/judiciary-restricts-access-to-sealed-records-after-cyber-hack

Judiciary Restricts Access to Sealed Records After Cyber Hack

Sept. 24, 2025, 9:04 PM GMT+2

Suzanne Monyak
Reporter



Photographer: Daniel Acker/Bloomberg

Listen

Federal trial courts are issuing new orders restricting access to sealed documents, following a directive from the judiciary's administrative office to address escalated cyberattacks targeting the courts' case system.

Official legal systems can silently fail too

UK: Government covered up court service IT glitch

11 August, 2025

NEWS – "without comment"

Government covered up court service IT glitch which lost thousands of family court files holding evidence

08 Aug 2025

Posted by Natasha in Researching Reform

The government covered up a series of serious IT faults which affected the HM Courts & Tribunals Service (HMCTS) resulting in the loss of court files holding evidence, including thousands of files linked to family court cases.

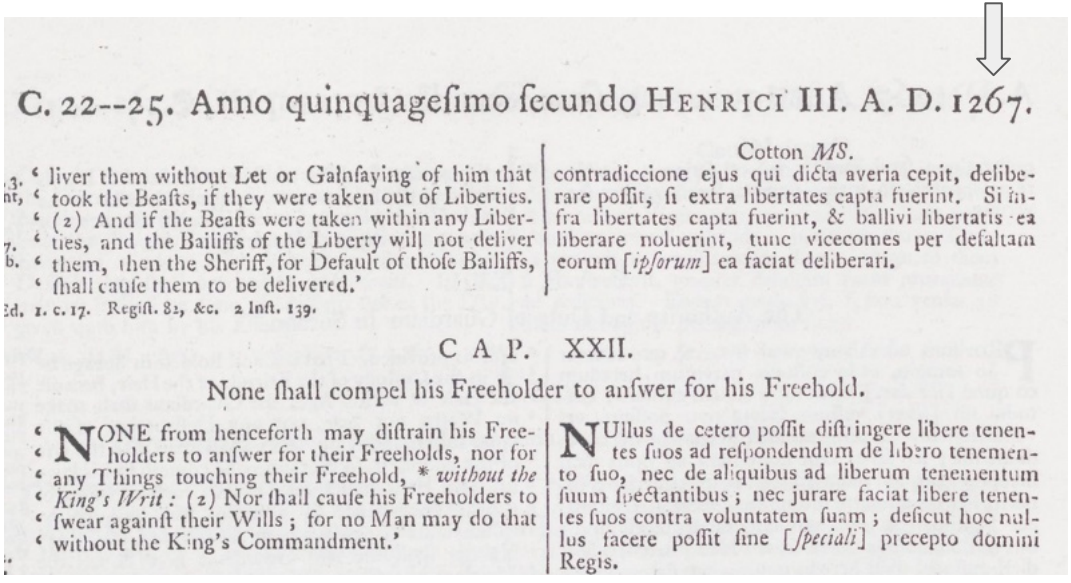
Source: https://wapi.org/uk-government-covered-up-court-service-it-glitch/

From paper law to digital law

- For over a millennium, law was written, preserved, and disseminated on paper
- Legal systems developed mature practices for authenticity, preservation, and trust
  - (seals, signatures, archives, redundancy)
- Securing paper law was never trivial - we are simply very experienced at it
- Digital documents: only decades of experience
- Digital law: even less

Law operates on a different time scale

- Legal collections can span centuries
  - The DC Council's legal code includes English law dating back to the 13th century
- Past versions of the same law remain legally relevant for decades
  - People and institutions rely on the exact wording in force at a given time



C. 22--25. Anno quinquageſimo ſecundo HENRICI III. A. D. 1267.

Cotton *MS.*

liver them without Let or Gainſaying of him that took the Beaſts, if they were taken out of Liberties. (2) And if the Beaſts were taken within any Liberties, and the Bailiffs of the Liberty will not deliver them, then the Sheriff, for Default of thoſe Bailiffs, ſhall cauſe them to be delivered.'

contradiccione ejus qui dicta averia cepit, deliberare poſſit, ſi extra libertates capta fuerint. Si infra libertates capta fuerint, & ballivi libertatis ea liberare noluerint, tunc vicecomes per defaltam eorum [*ipſorum*] ea faciat deliberari.

Ed. 1. c. 17. Regiſt. 82, &c. 2 Inſt. 139.

CAP. XXII.

None ſhall compel his Freeholder to anſwer for his Freehold.

'NONE from henceforth may diſtrain his Freeholders to anſwer for their Freeholds, nor for any Things touching their Freehold, * *without the King's Writ*: (2) Nor ſhall cauſe his Freeholders to ſwear againſt their Wills; for no Man may do that without the King's Commandment.'

NUllus de cetero poſſit diſtringere libere tenentes ſuos ad reſpondendum de libero tenemento ſuo, nec de aliquibus ad liberum tenementum ſuum ſpectantibus; nec jurare faciat libere tenentes ſuos contra voluntatem ſuam; deficut hoc nullus facere poſſit ſine [*ſpeciali*] precepto domini Regis.

Why law is different from other digital content

- Law is not a collection of independent documents, but an interconnected system
- Errors or tampering can directly affect legal decisions

Requirements

Requirements

Version
Authenticity and
Access

Requirements

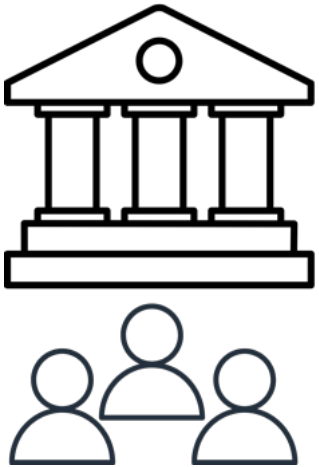
Version Authenticity and Access

Tamper Evidence and Institutional Independence

Requirements

Version Authenticity and Access

Tamper Evidence and Institutional Independence

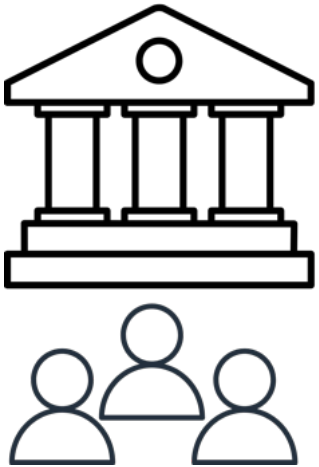


Usable in real publishing workflows

Requirements

Version Authenticity and Access

Tamper Evidence and Institutional Independence



Usable in real publishing workflows

UELMA

The Uniform Electronic Legal Material Act

Existing approaches fall short

- There are established archival systems, such as LOCKSS and DSpace
- Designed to ensure availability, replication, and long-term access
- They are excellent at keeping files safe
- But law needs guarantees about authorship and version history
- It also requires easy access to the full corpus, including any prior version of it

Requirements

How can we satisfy these requirements?

Our solution

TAF combines Git and TUF

Our solution

TAF combines Git and TUF

Version Control

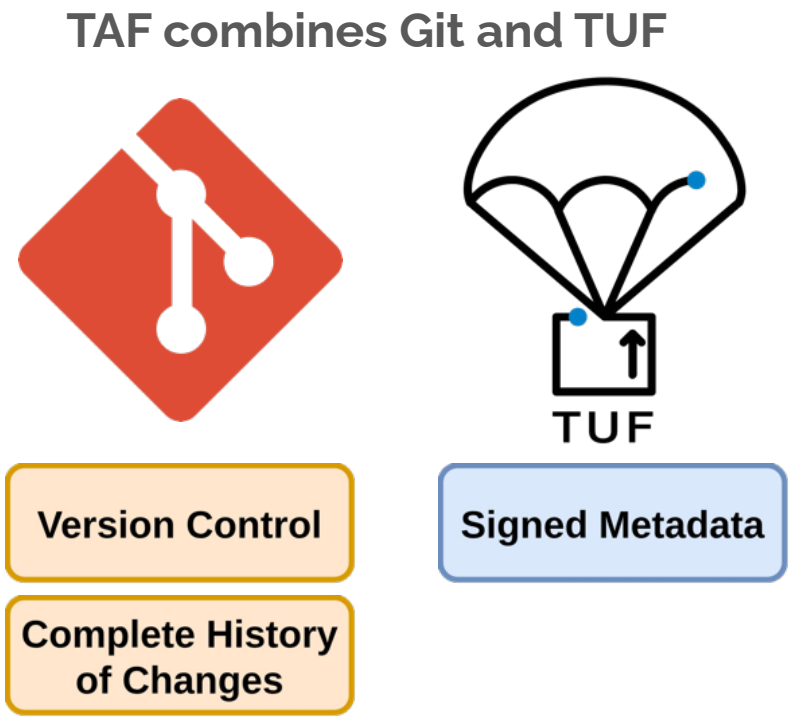
Our solution

TAF combines Git and TUF

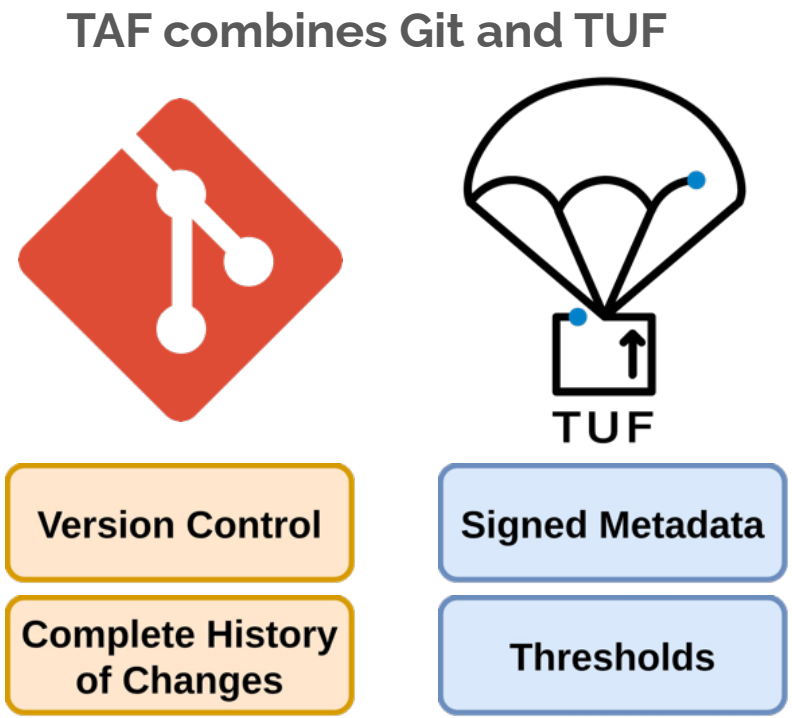
Version Control

Complete History of Changes

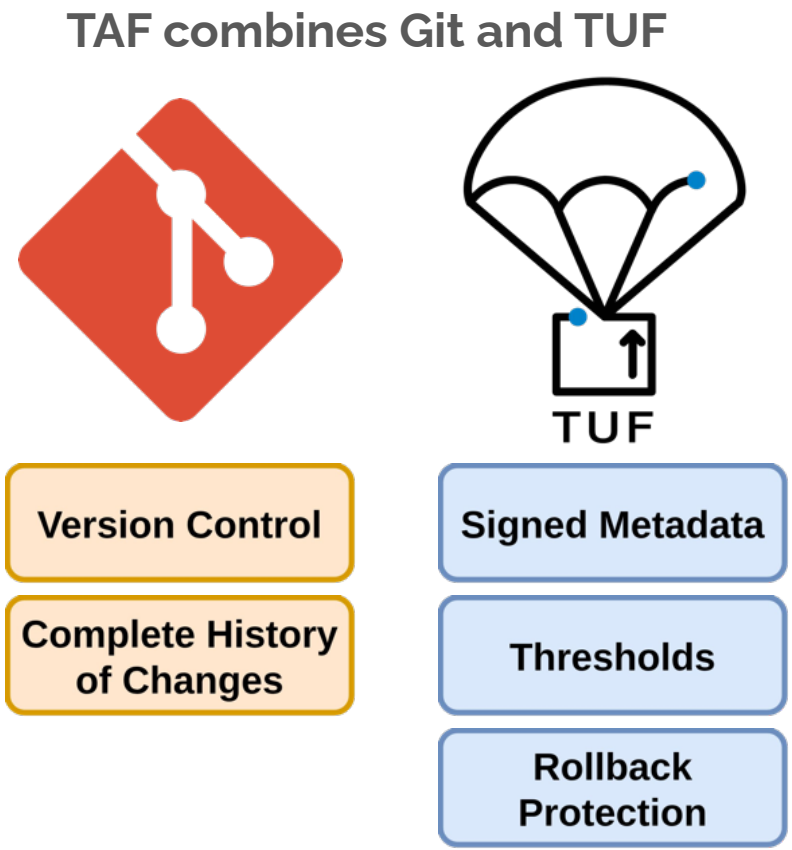
Our solution



Our solution



Our solution



Our solution

TAF combines Git and TUF

Version Control

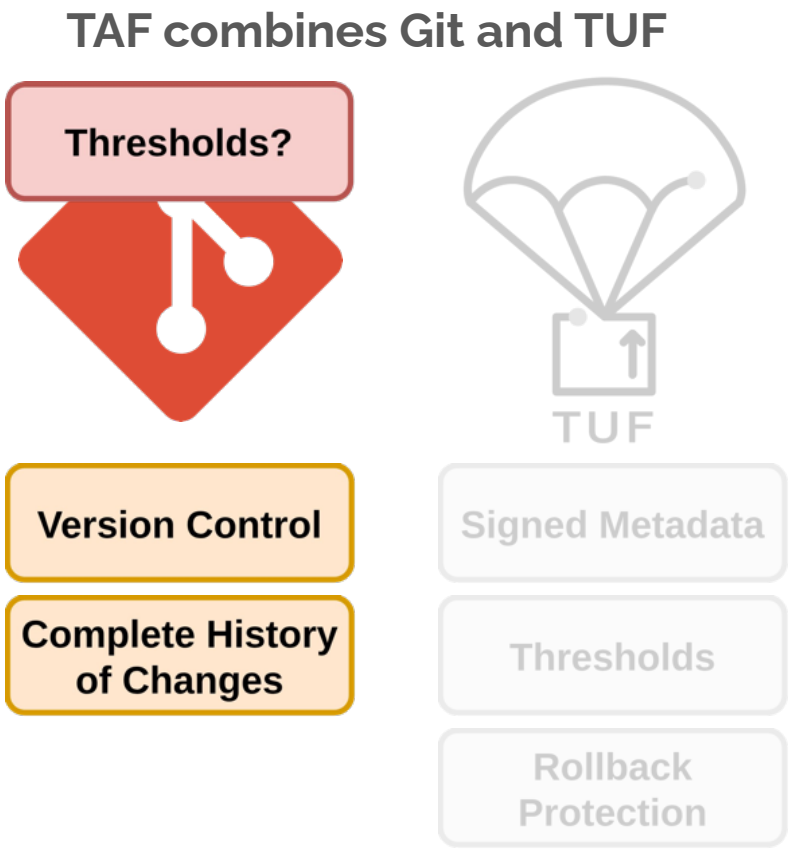
Complete History of Changes

Signed Metadata

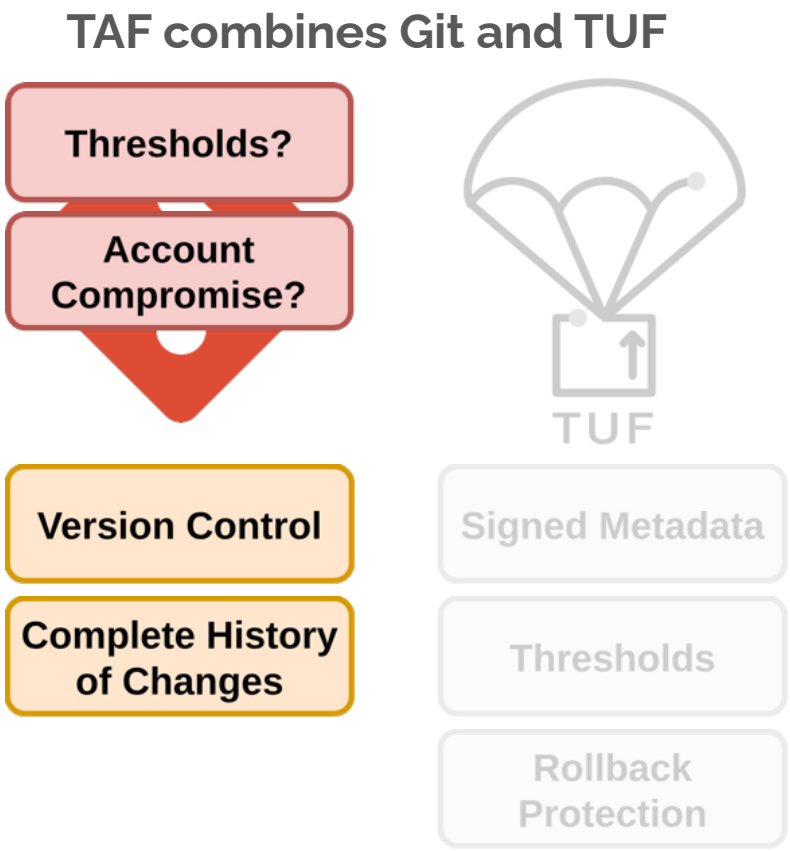
Thresholds

Rollback Protection

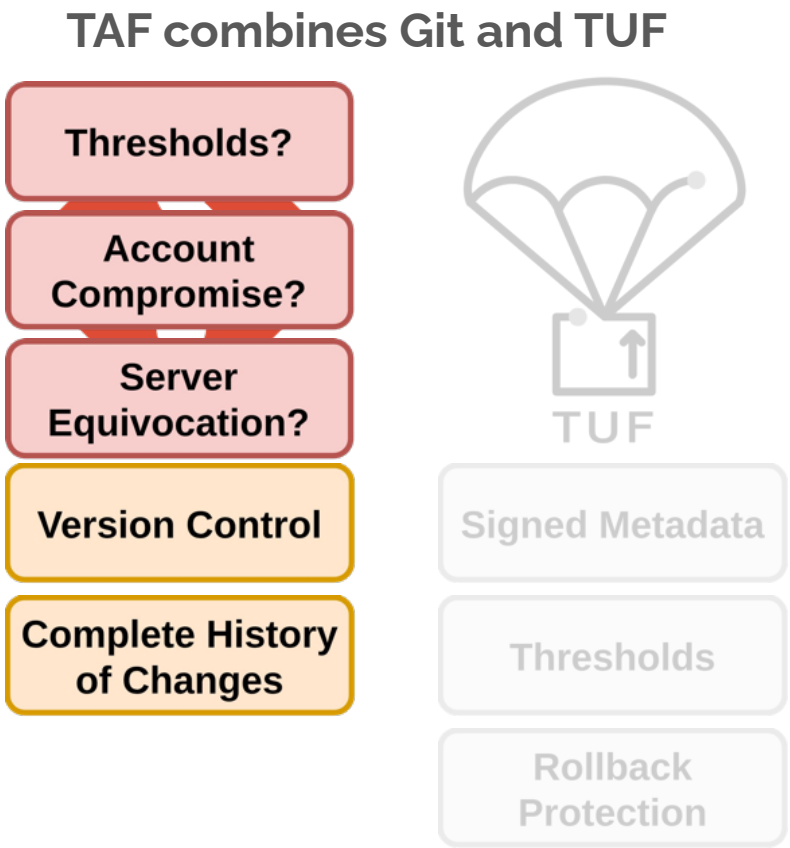
Our solution



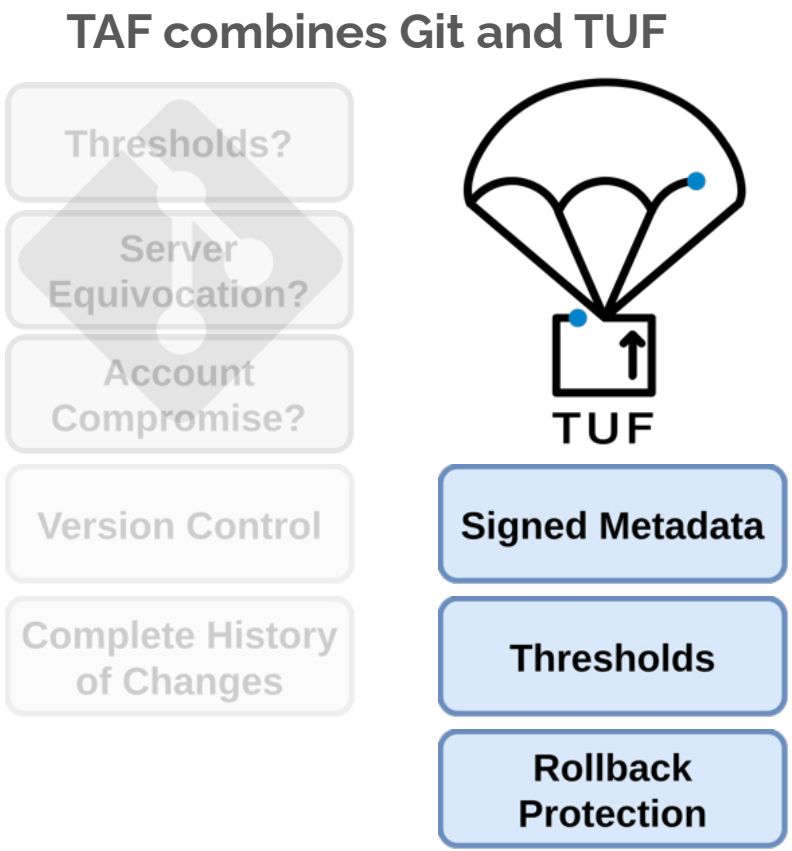
Our solution



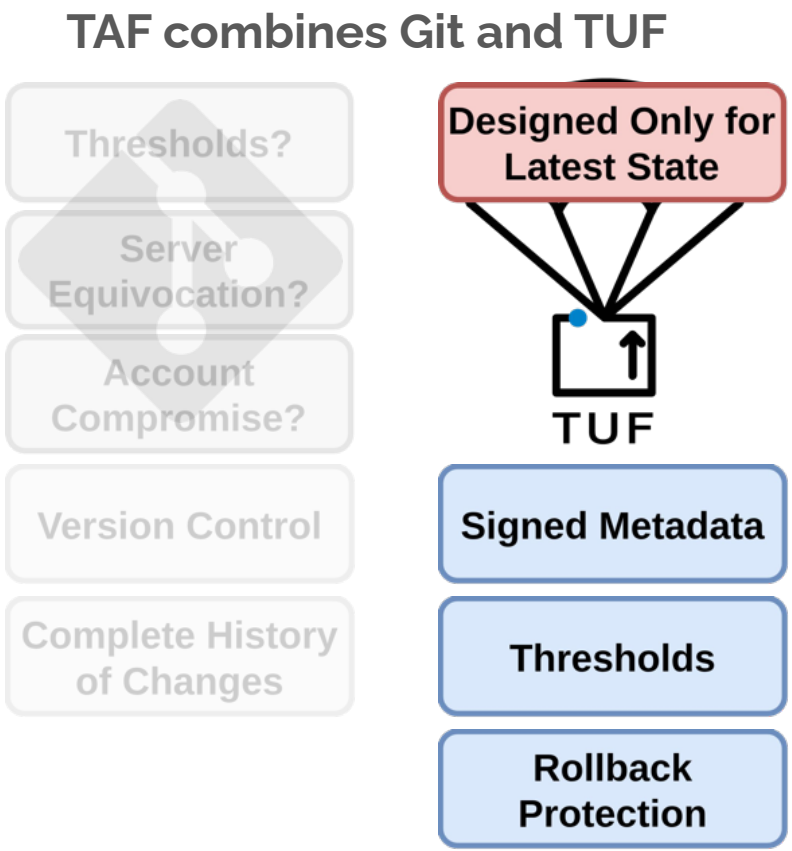
Our solution



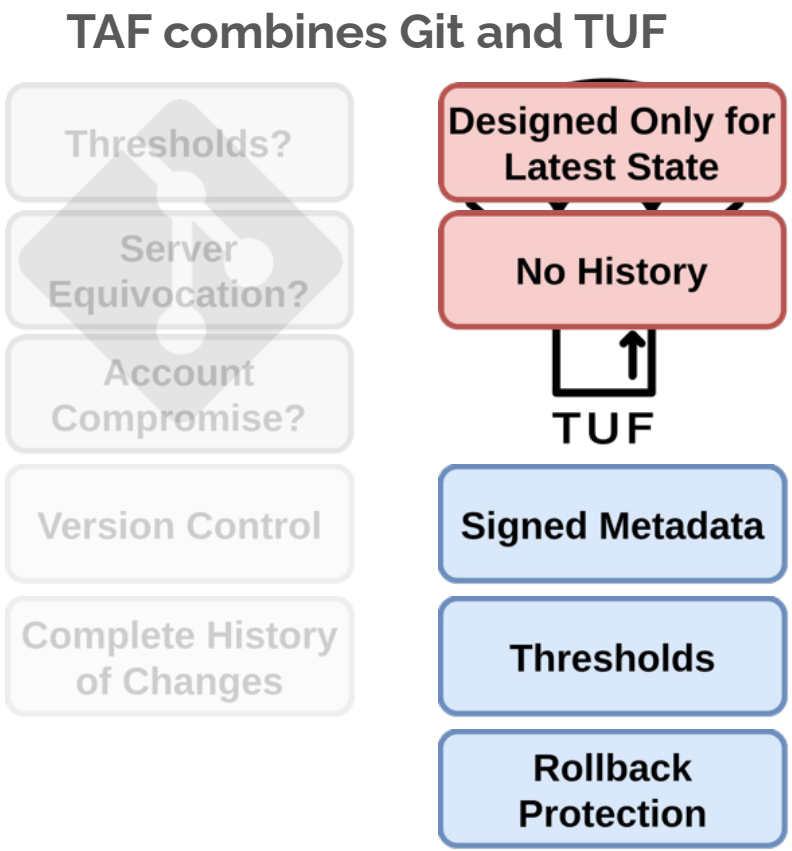
Our solution



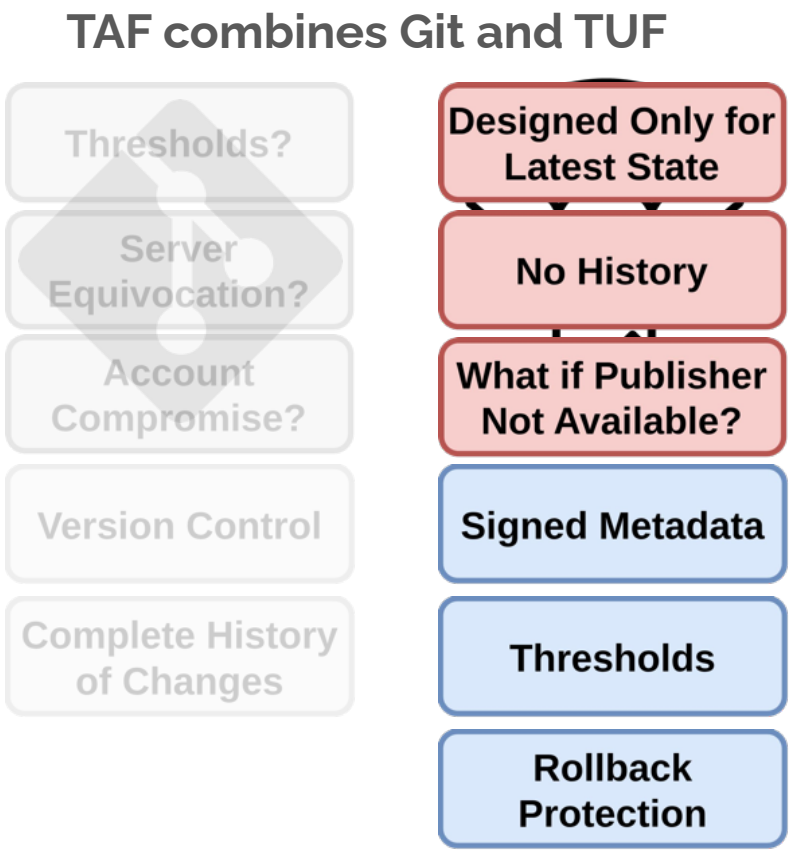
Our solution



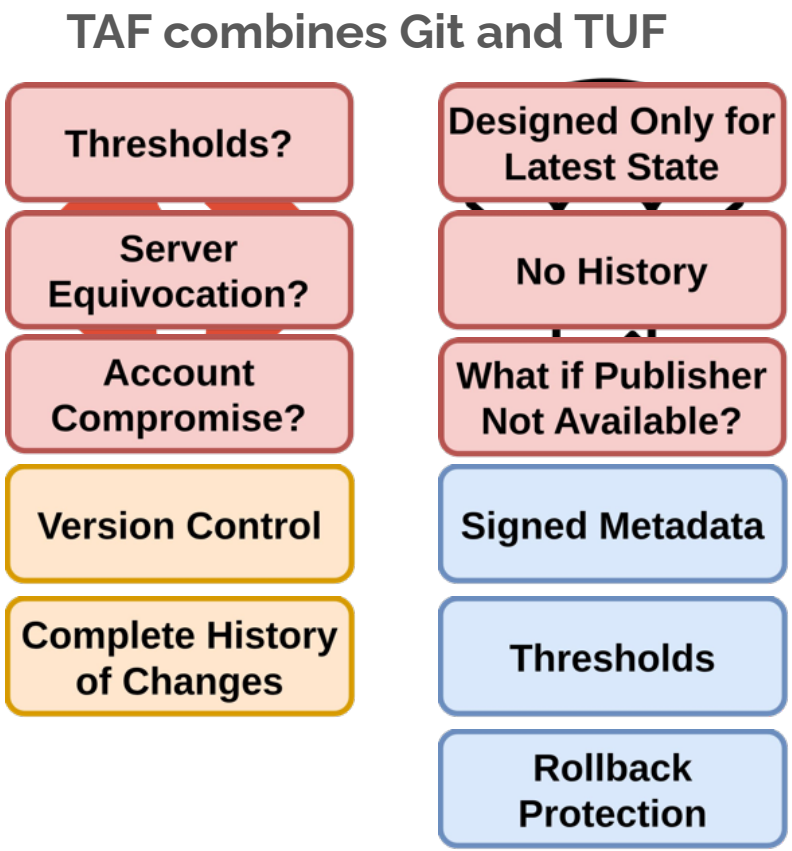
Our solution



Our solution



Our solution

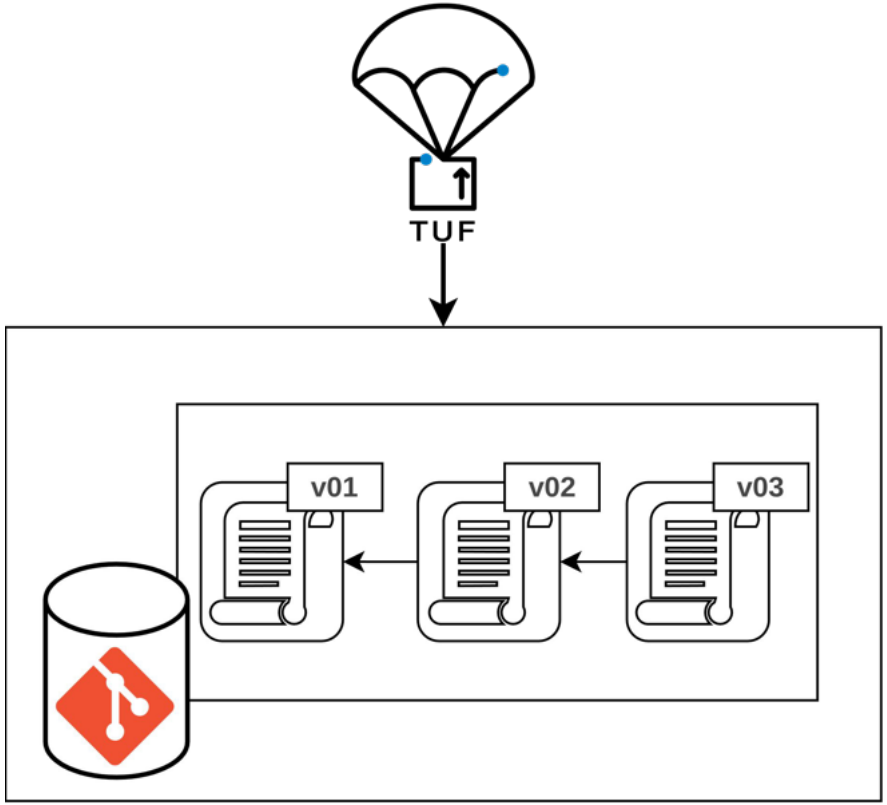


Why TAF is more than Git + TUF

Git + TUF ≠ verifiable legal history

- Combining these two tools does not automatically secure the timeline.

What a naive combination gives you

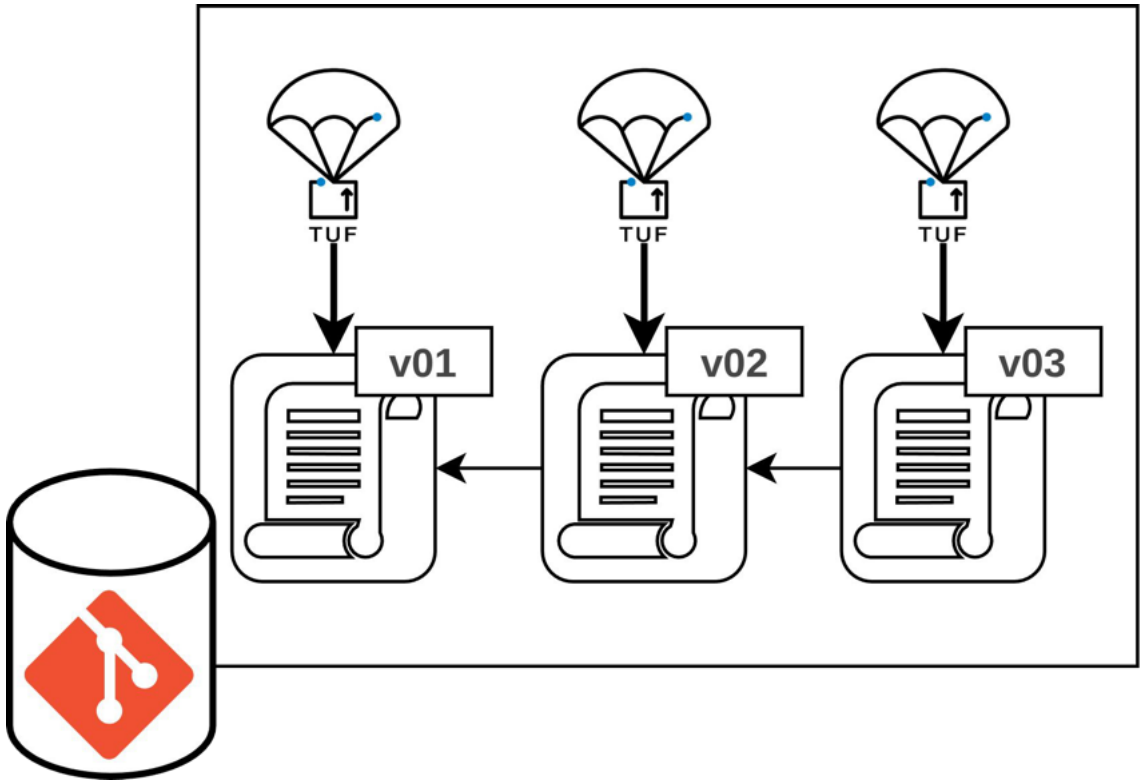


- Git records versions
- TUF authenticates a repository state
- Clients can verify the current version

But...

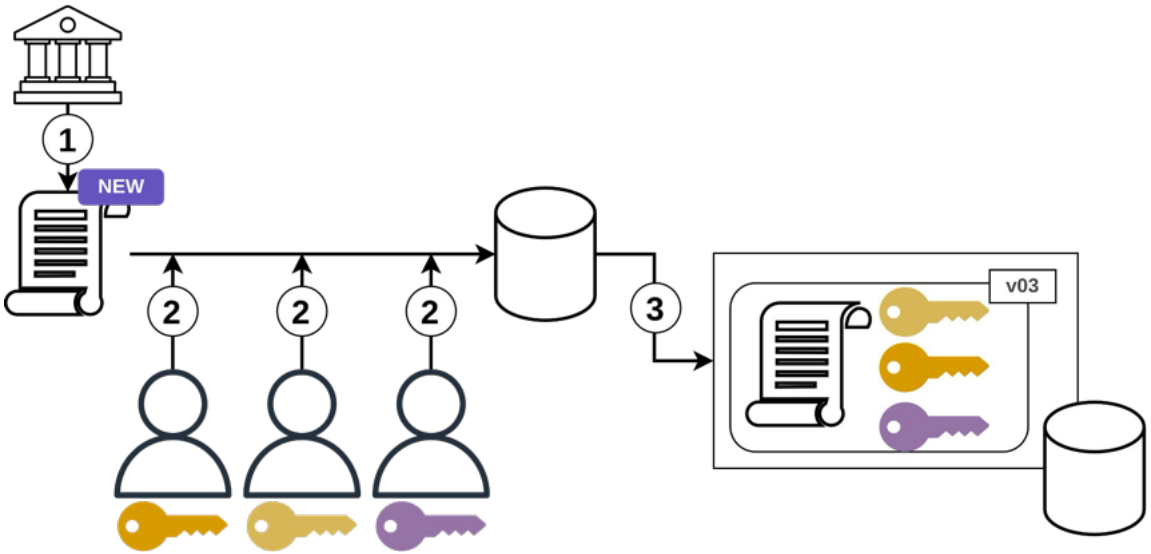
- No guarantee that every past version was authenticated
- No verifiable notion of time

What TAF does



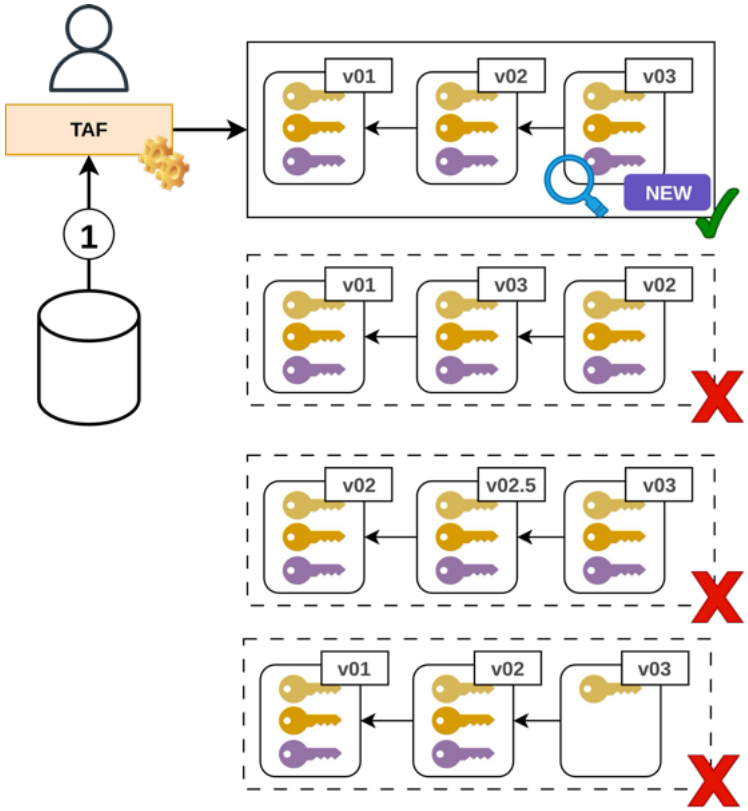
- TAF applies TUF-style authenticity to every version in Git's history — not just the latest one
- Versions form a single, ordered chain of authorized legal states.

How TAF handles legal updates



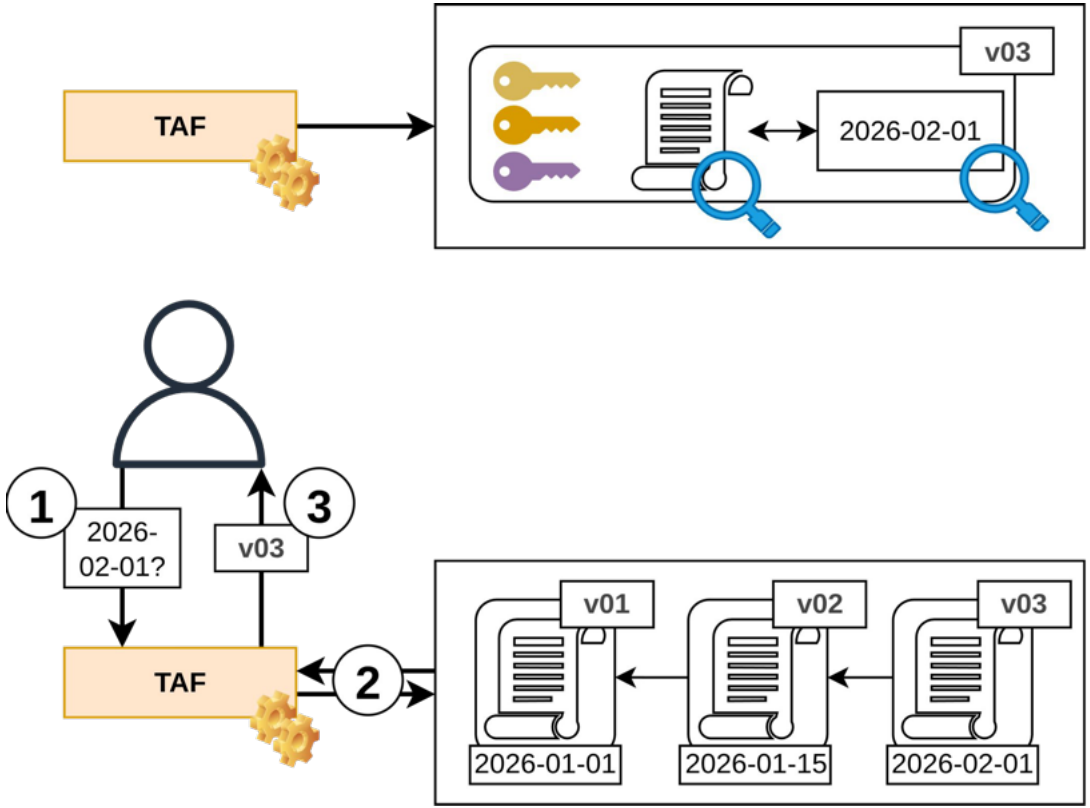
- Publishers prepare updates to the law using their existing workflows
- Publishing the updates requires explicit authorization
  - Formal approval of a specific state of the law as valid and official.
- May require approval by a threshold of keys
- Each authorization, coupled with a corresponding state of the law, becomes part of an ordered history of valid versions

How clients verify legal history



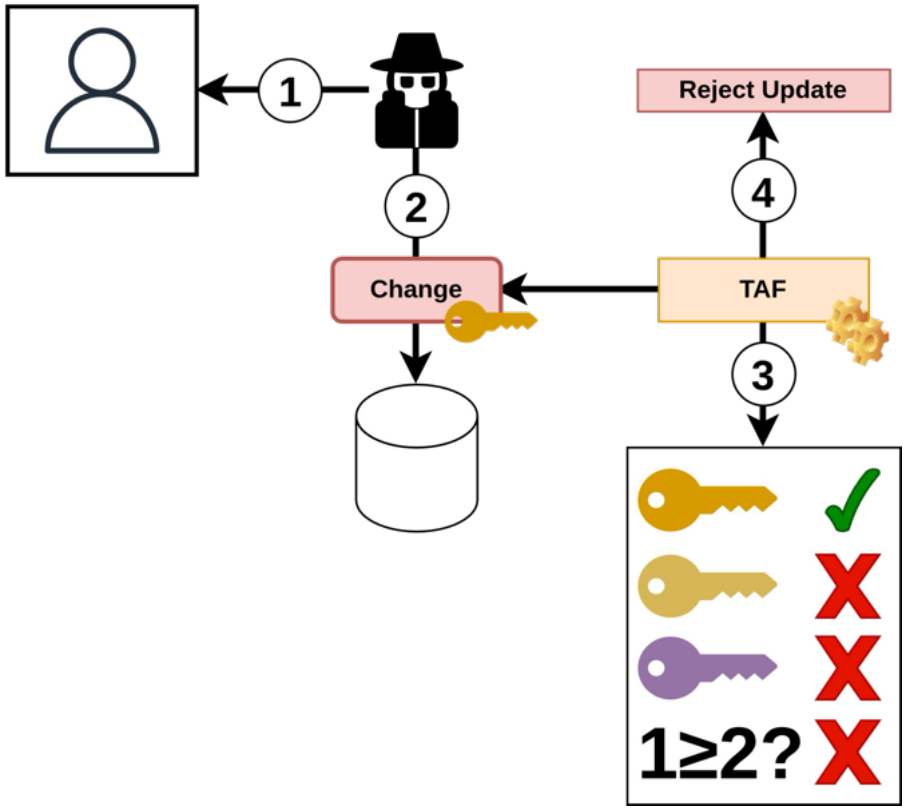
- Clients download and update their local copy of a digital legal archive
- They cryptographically verify states of the legal corpus sequentially, according to the ordered authorization history.
- Updates without a corresponding signed authorization are rejected
- Reordering, deletion, or insertion of versions breaks verification

Time as part of verification



- Each version of the law is authorized together with its effective date
- Clients cryptographically verify content and effective dates as a unit
- Enables temporal queries
  - (e.g., what did the law look like on a given date?)

Scenario 1 Attacker wants to update the law

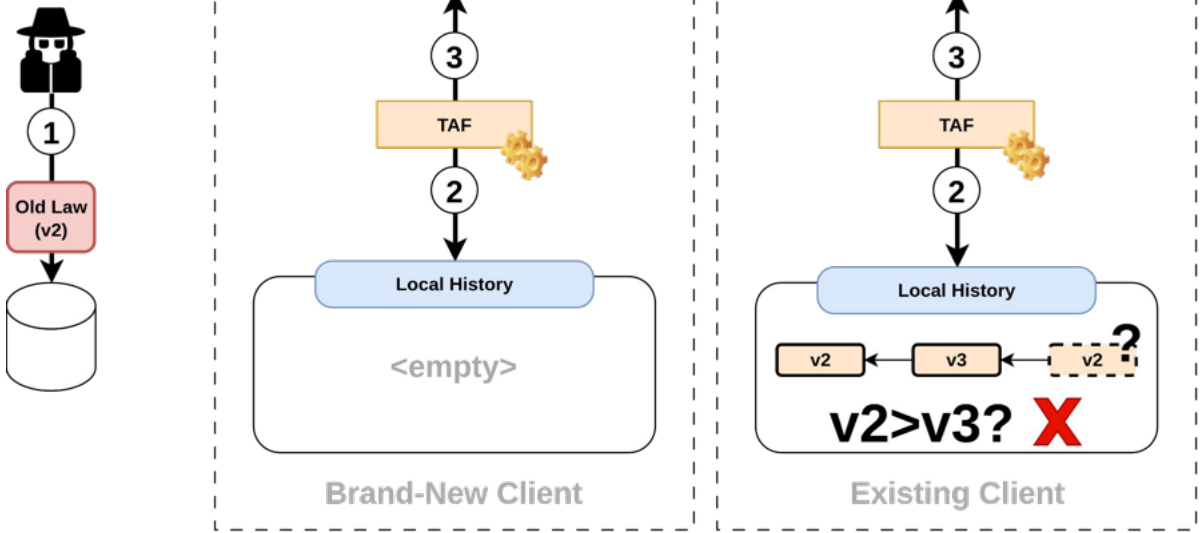


- Attacker can modify the law's contents
- Publishing requires authorization by a threshold of signing keys
- Signing keys are protected (e.g., stored on YubiKeys)

➡ Attacker cannot obtain the required threshold of keys

➡ Result: the update cannot be authorized and published

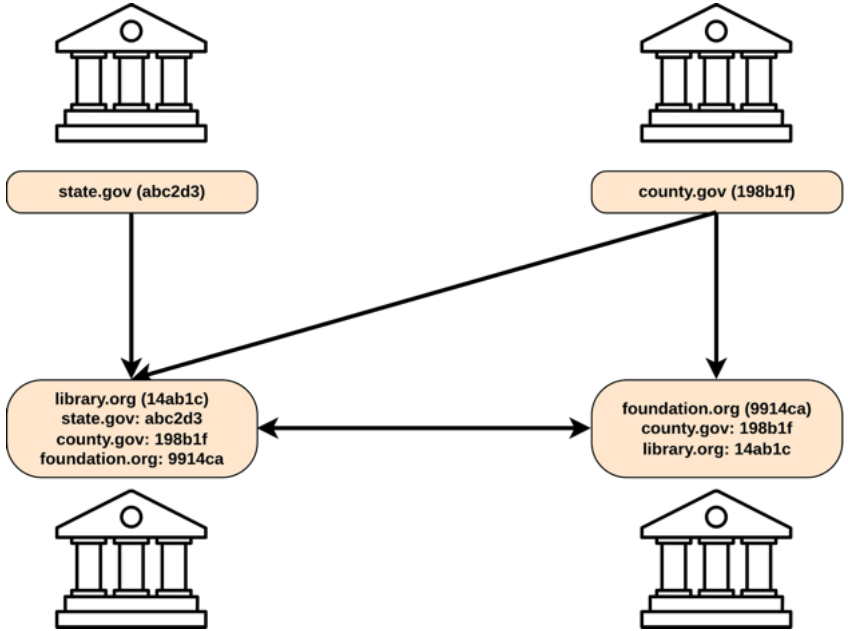
Scenario 2 Presenting outdated law as current



- An attacker deletes the newest versions of the law
- The corresponding authorizations are deleted as well
- A brand-new client has no prior state to compare against
- The attack is only detectable if a trusted mirror or prior copy exists

A network of trustworthy institutions

- Multiple independent institutions mirror
- Each mirror verifies updates as they appear and keeps a record of all verified versions
- Clients can compare views across institutions
- History truncation becomes detectable through disagreement



Implementation details

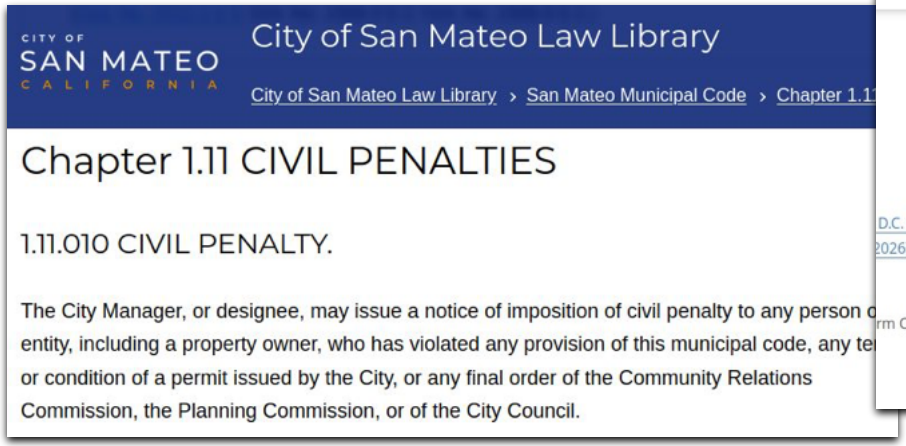
- This talk focused on the high-level model and guarantees.
- For a detailed description of the system, including how concepts from Git and TUF are combined, please see the paper

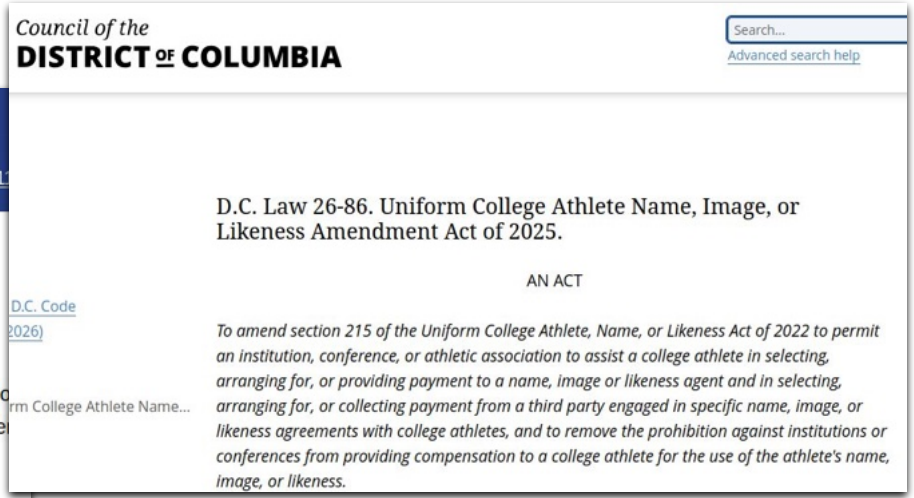
Design details

- Poster: “Building Networks of Trust for Legal Preservation with TAF”
- Accepted at NDSS 2026 — public release forthcoming

Real-world deployment

- Deployed in 14 U.S. jurisdictions, including the District of Columbia, the State of Maryland and several tribal governments
- Also in use by the National Indian Law Library (NILL), which independently mirrors tribal law repositories





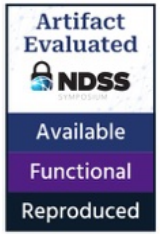
Evaluation

TAF Repository

https://github.com/openlawlibrary/taf

Simulation / Demo

https://github.com/renatav/taf-ndss-eval



Limitations & future work

- Inherited assumptions and vulnerabilities from underlying versioning systems
- Further work on networks of independent institutions (e.g., divergence detection and resolution)
- Defining explicit time semantics and integrating trusted time sources
- Long-term cryptographic agility

Conclusion

- Digital law requires long-term verifiability and provenance
- TAF combines version control with threshold-based authenticated publication
- Published revisions remain cryptographically verifiable over time
- Already deployed across 14 jurisdictions

Thank You!
Questions?

vrenata8@gmail.com
Open to new opportunities

nikolic.dusan@uns.ac.rs

patrick.z@nyu.edu