Profian

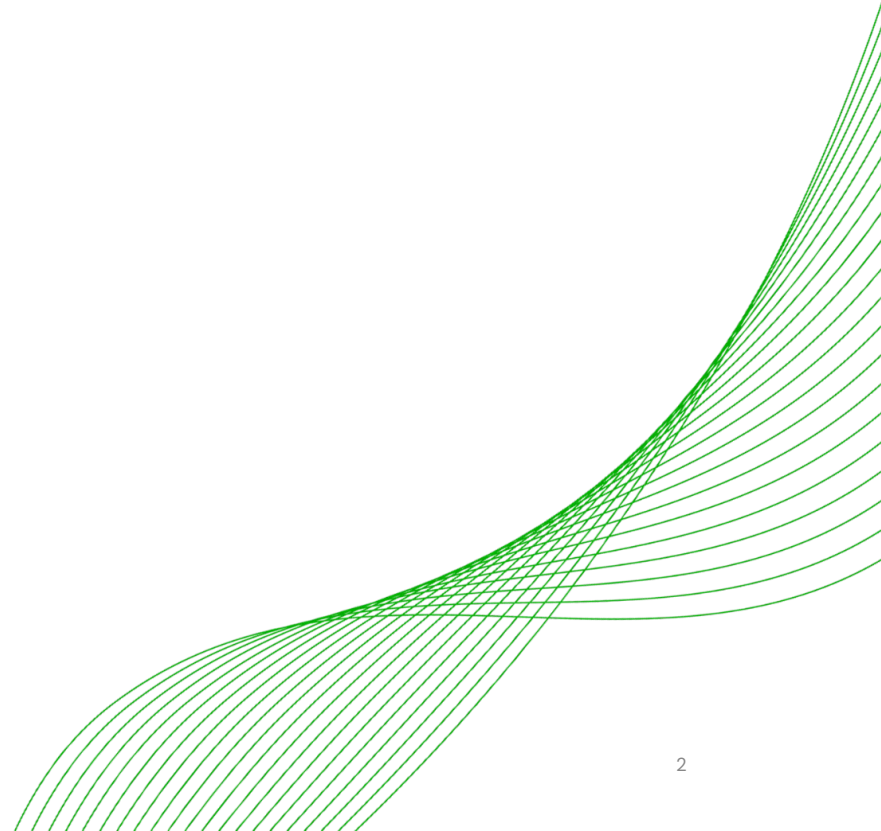
Attestation Flow

January 2023

Agenda

1. Disclaimer
2. High level flow
3. Details of each phases
4. Q&A

Diagrams and details are available online.



Disclaimer

- This is work in progress
- Not everything is implemented
- The design is being adjusted as we implement changes and uncover challenges

High Level Overview

Actors

Publisher (Developer)

- Does the development (maybe)
- Prepares a workload
  - Application(s)
  - Configuration
- Uploads into the registry

Administrator

- Does the deployment
- Chooses systems to run on
- Orchestrates the delivery of the runtime binaries that will run the application

Components

- Registry (Drawbridge)
- Host
- Guest (Enarx)
- Attestation server (Steward)
- Relying party

Registry (Drawbridge)

- A collection of applications and workload configurations
- Profian offers a service
- A private instance can be deployed
- Has access control
- Allows sharing repository with a group of people

Host

- A system where an application will run
- Multiple Linux distributions supported
- Needs to have application runtime for TEE - Enarx
- Needs to be configured to run applications in TEEs
  - CRLs and public keys cached - done by the systemd unit file
- Expect SGX or SEV for now

Guest

- Application runtime loaded into TEE
- Represented by the Enarx project
- Consists of:
  - Microkernels for different architectures (shims)
  - Wasmtime runtime
  - Enarx exec runtime layer – the logic
- Released and signed by Profian
- Known signatures are used in the attestation

Attestation Server (Steward)

- Acts as CA
- Receives requests from the guest
- Verifies the digests
- Issues a signed certificate with extensions
  - Attestation report
  - CRLs and TCB (Intel)
  - Signatures and digests of the application (deployment)

Relying party

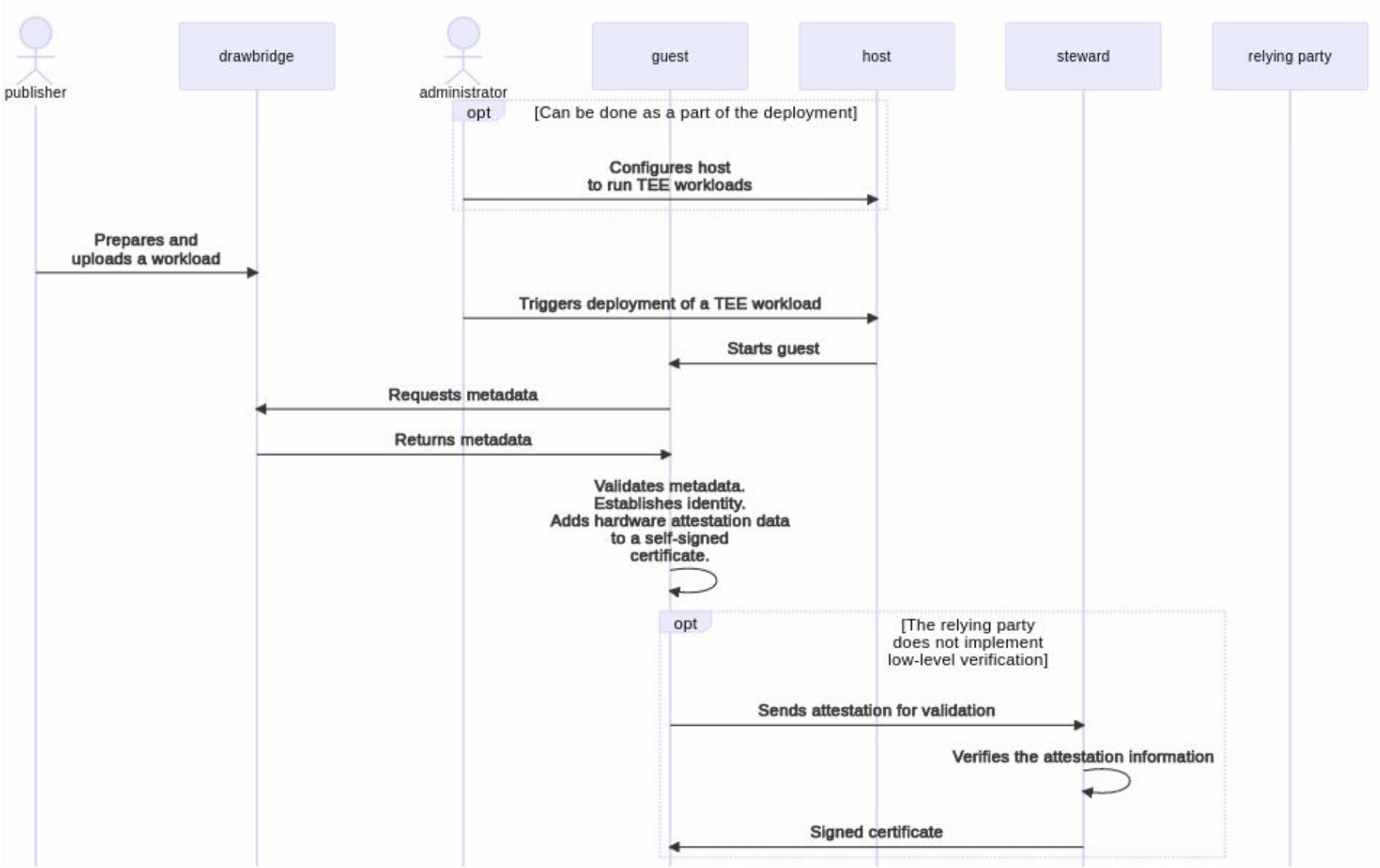
- A service on the network application connects to
- A part of the infrastructure that environment uses
- Expects TLS connection and a valid certificate
- Would want to make sure that certificate is valid
- Might want to inspect extensions to implement additional checks (implementation specific)

Terminology

- Application – a binary of the application
- Deployment (workload) – configuration of the application
- Right now we do not distinguish but we plan to
- Single signature is calculated for both
- Differentiation would allow to implement finer granular checks when two applications talk to each other:
  - Server – client
  - Web server – database

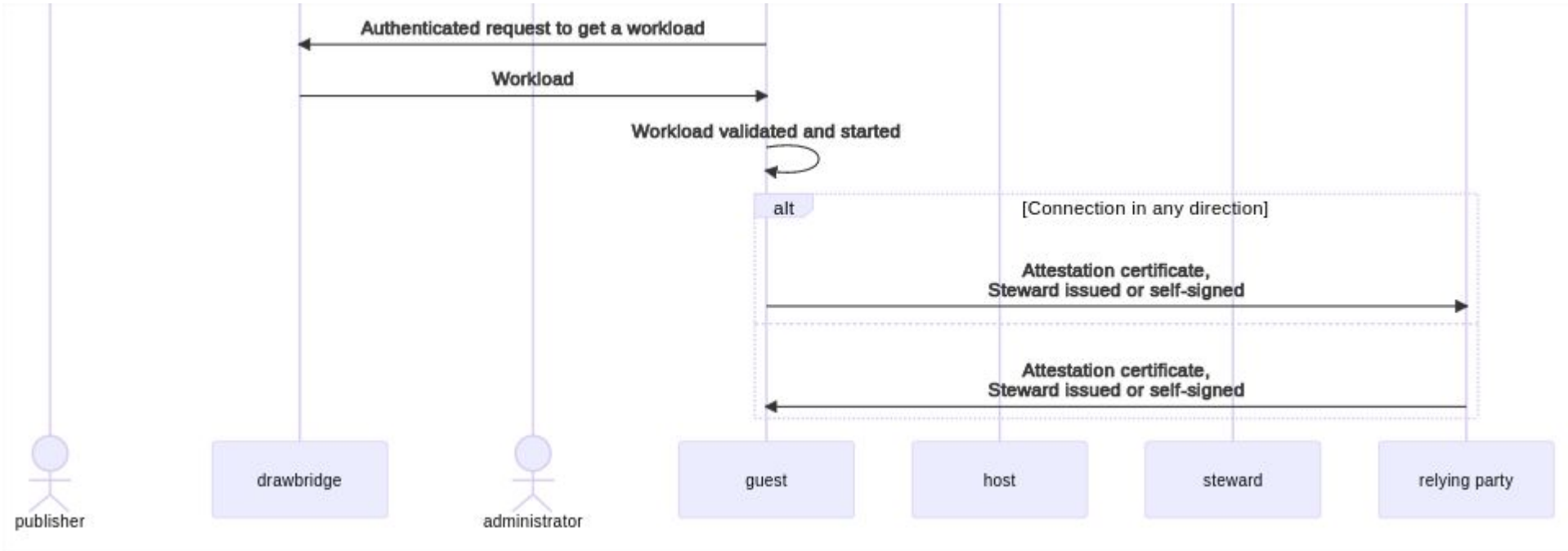
Phases of the flow

High level flow (part 1)



Profian

High level flow (part 2)

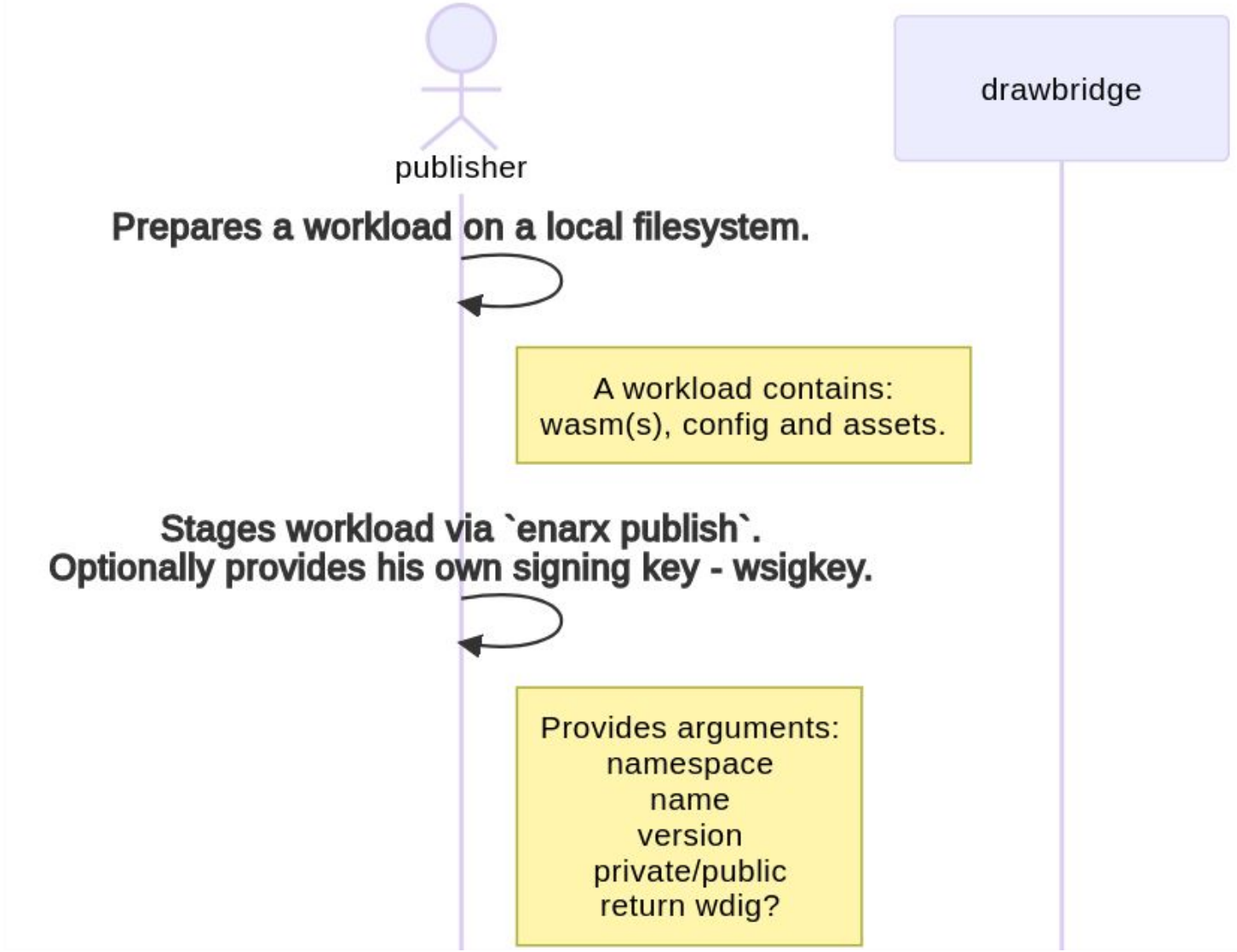


Phases

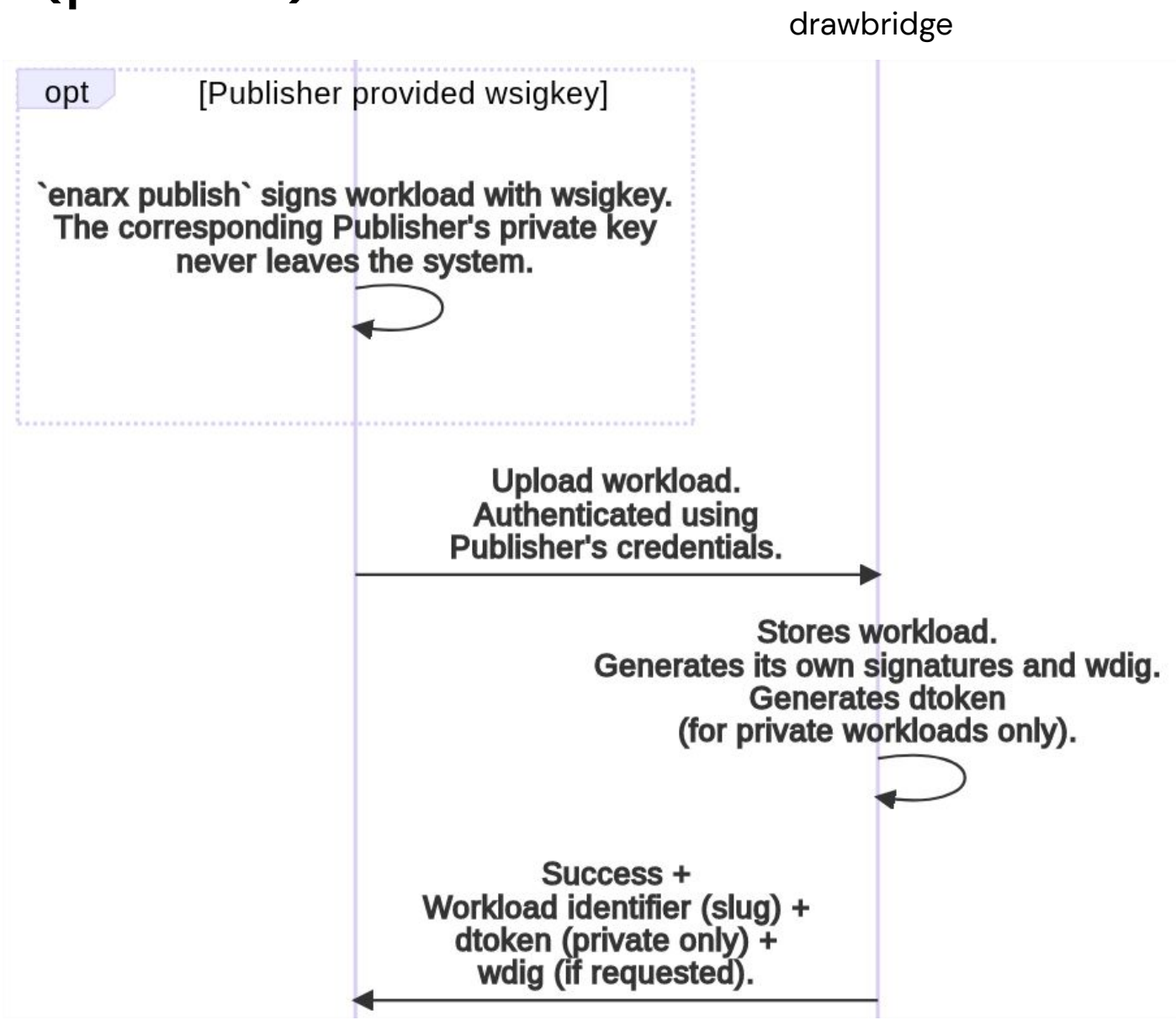
- Workload publisher stages a workload
- Prepare the host to run a Guest
- Deploy and run workload with the Attestation
    - Get and Validate Package Metadata
    - Establish Workload Identity
    - Download and Execute Workload
    - Attest to Relying Parties

Staging flow

Staging flow (part 1)



Staging flow (part 2)



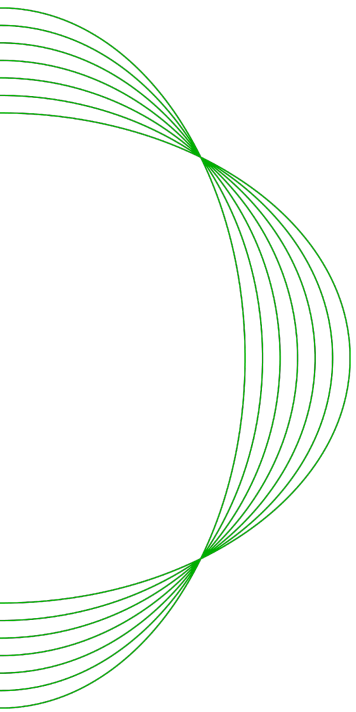
Prepare the host to run a Guest

- Deliver Enarx binary – how: standard deployment procedure
  - As an rpm/deb or a container
  - Includes: host side client, enarx runtime (shims, wasmtime, exec layer)
- Utility (same binary) to configure host and fetch certs
  - VCEK (AMD), TCB (Intel), CRLs
- Systemd unit file to refresh the cache
  - CRLs and certs cached on the system

Can be done anytime before the deployment of the workload

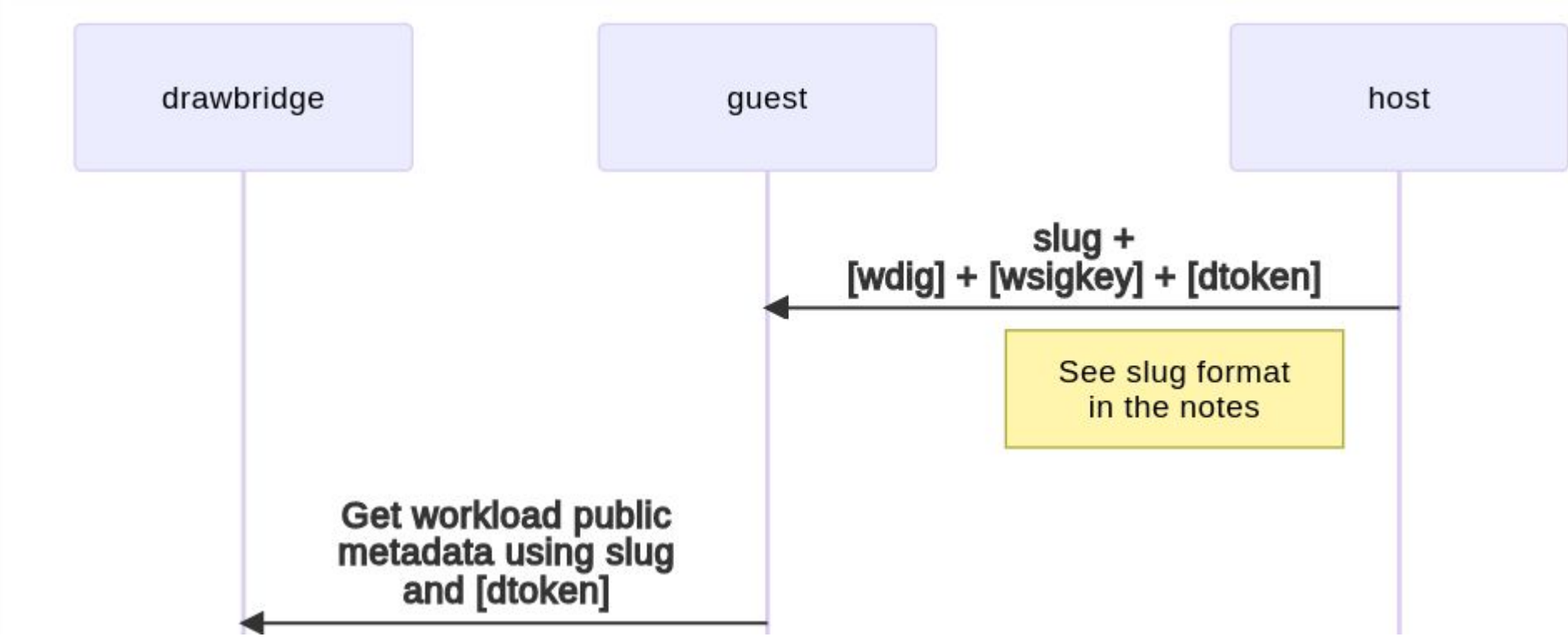
Trigger deployment

- Host calls `enarx deploy` (run) command
- Enarx binary is loaded into the TEE
- Binary starts running
    - “Guest” is instantiated

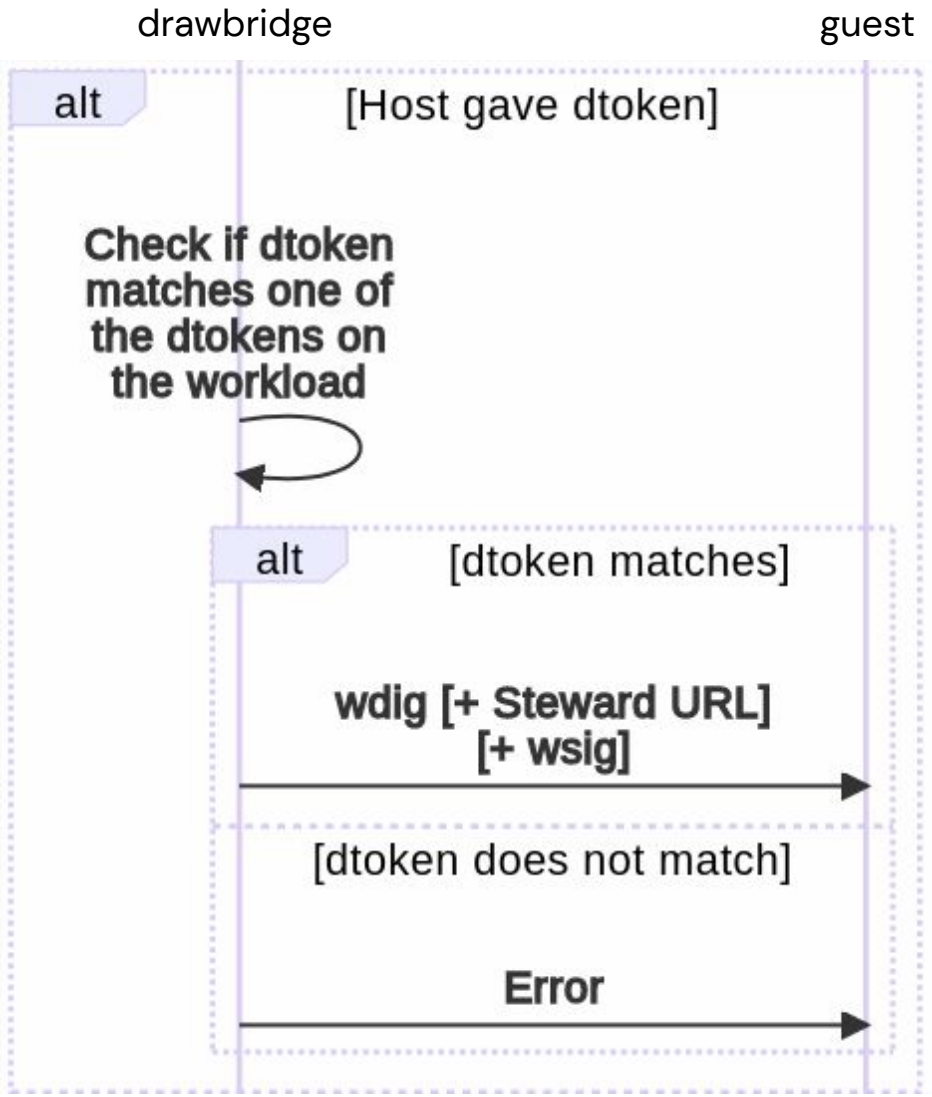


Get and validate package metadata

Get and validate package metadata (part 1)

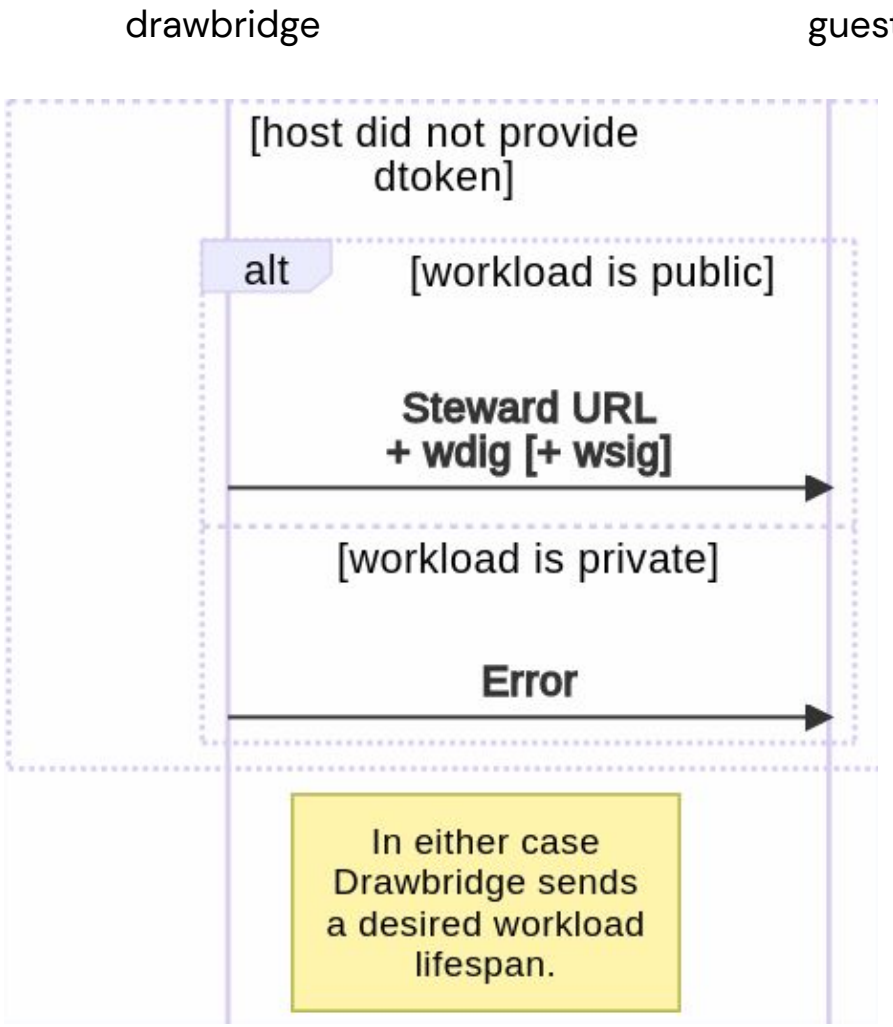


Get and validate package metadata (part 2)

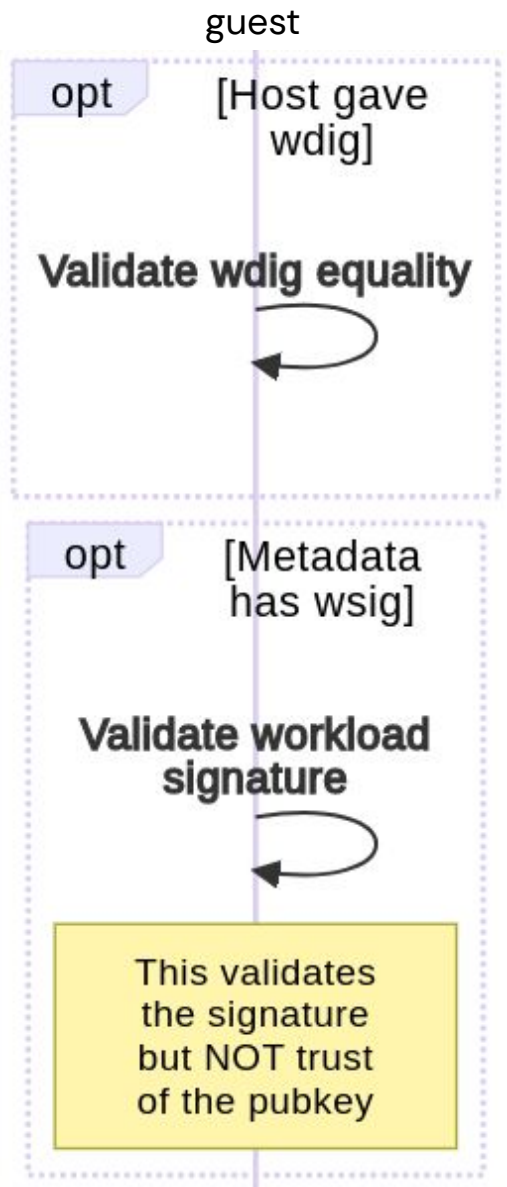


Profian

Get and validate package metadata (part 3)

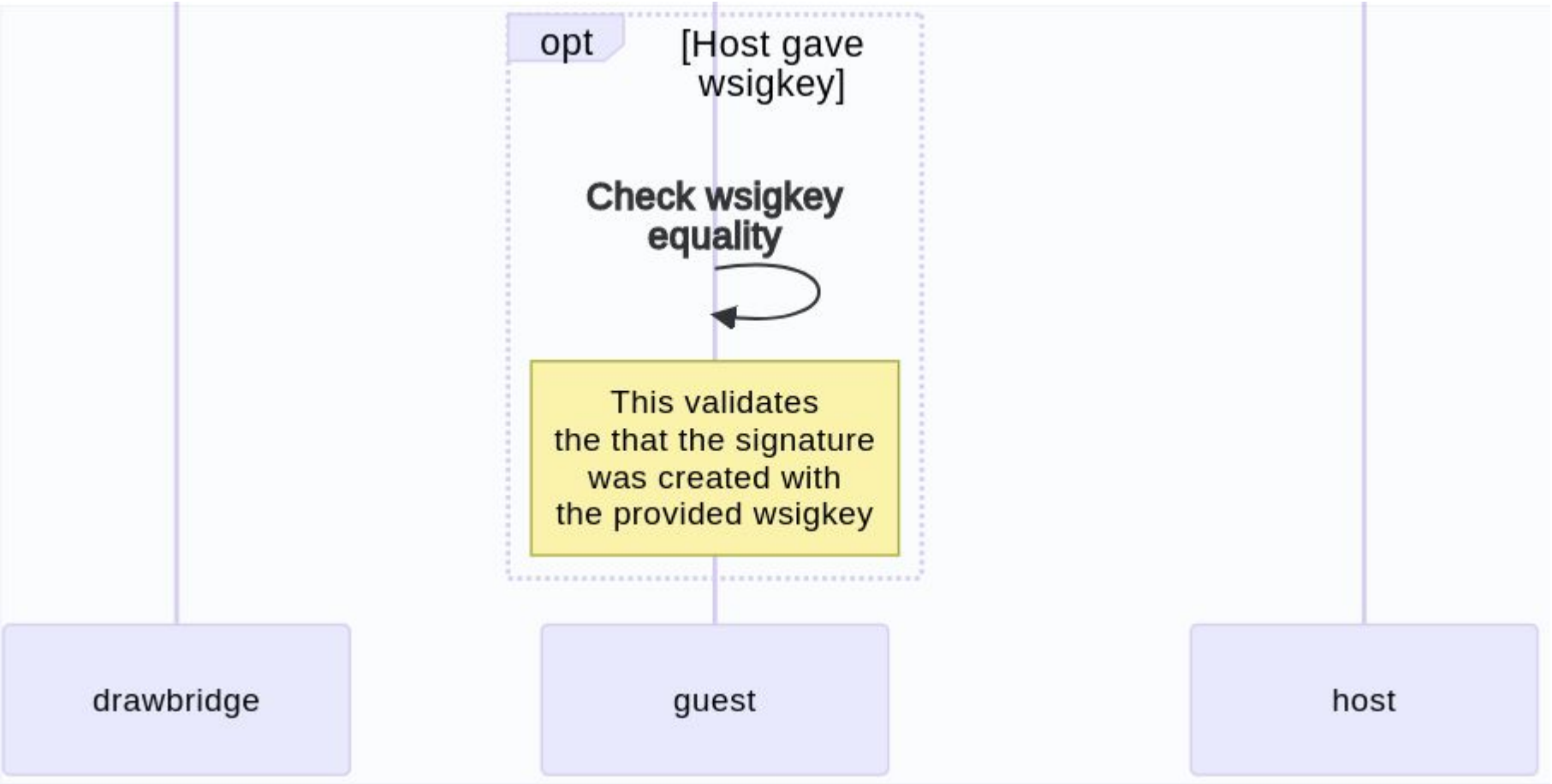


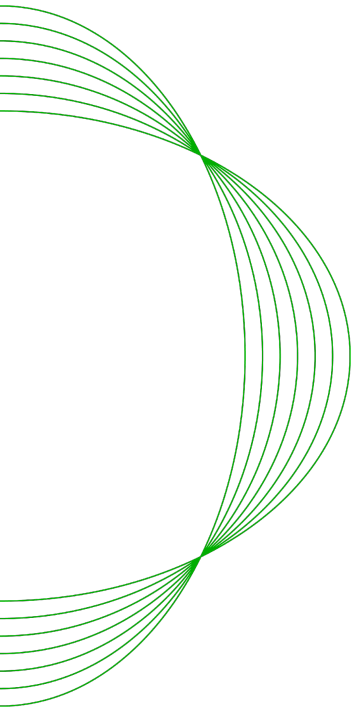
Get and validate package metadata (part 4)



Profian

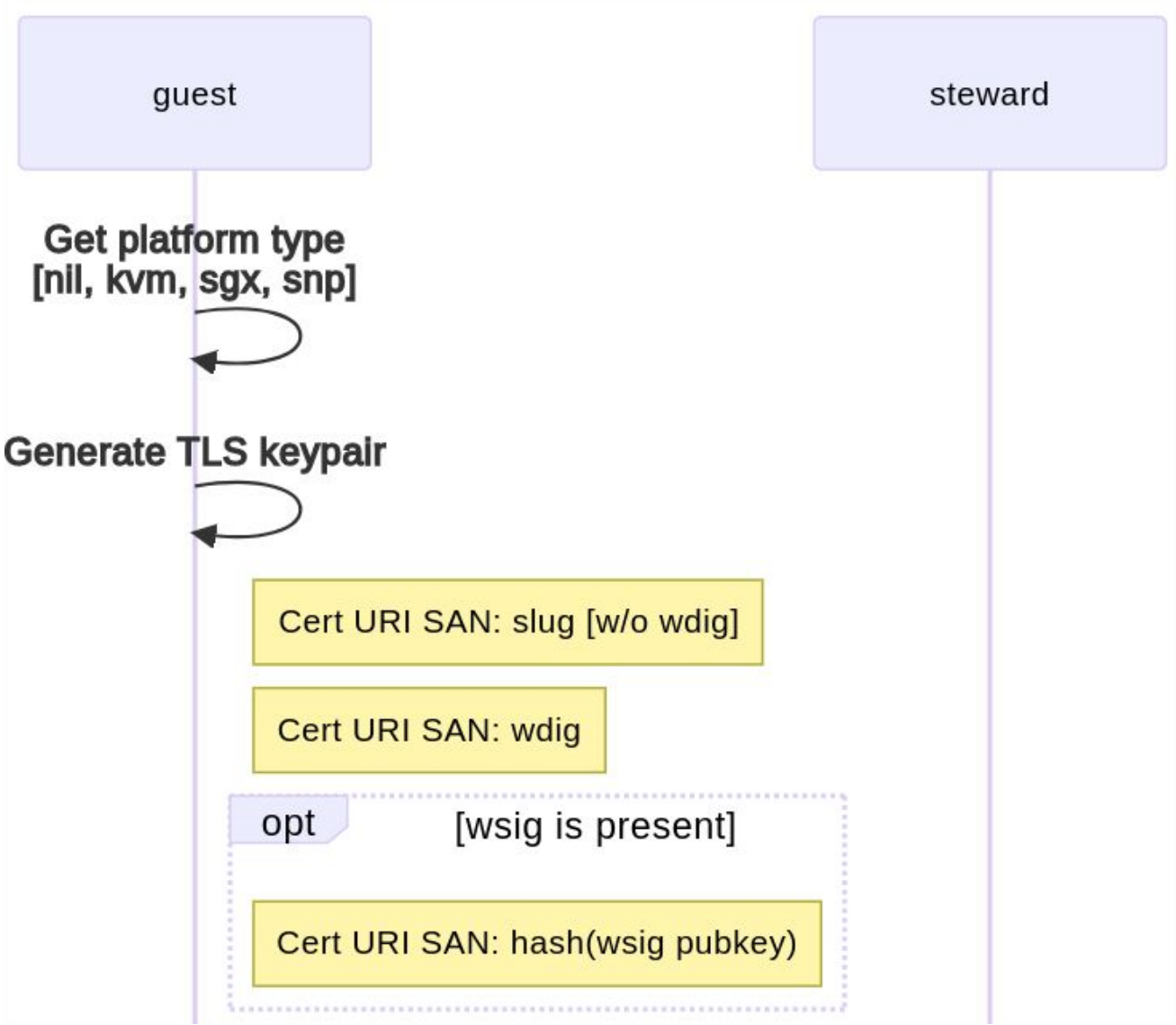
Get and validate package metadata (part 5)



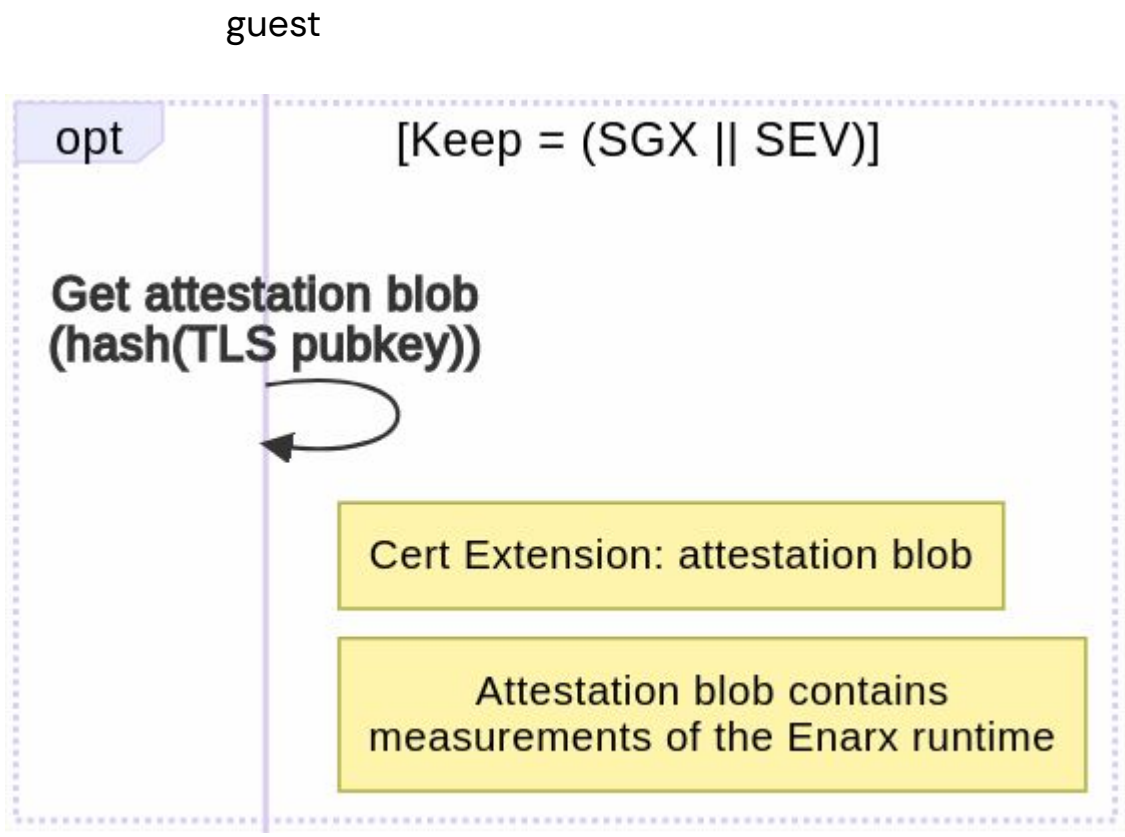


Establish workload identity

Establish workload identity (part 1)

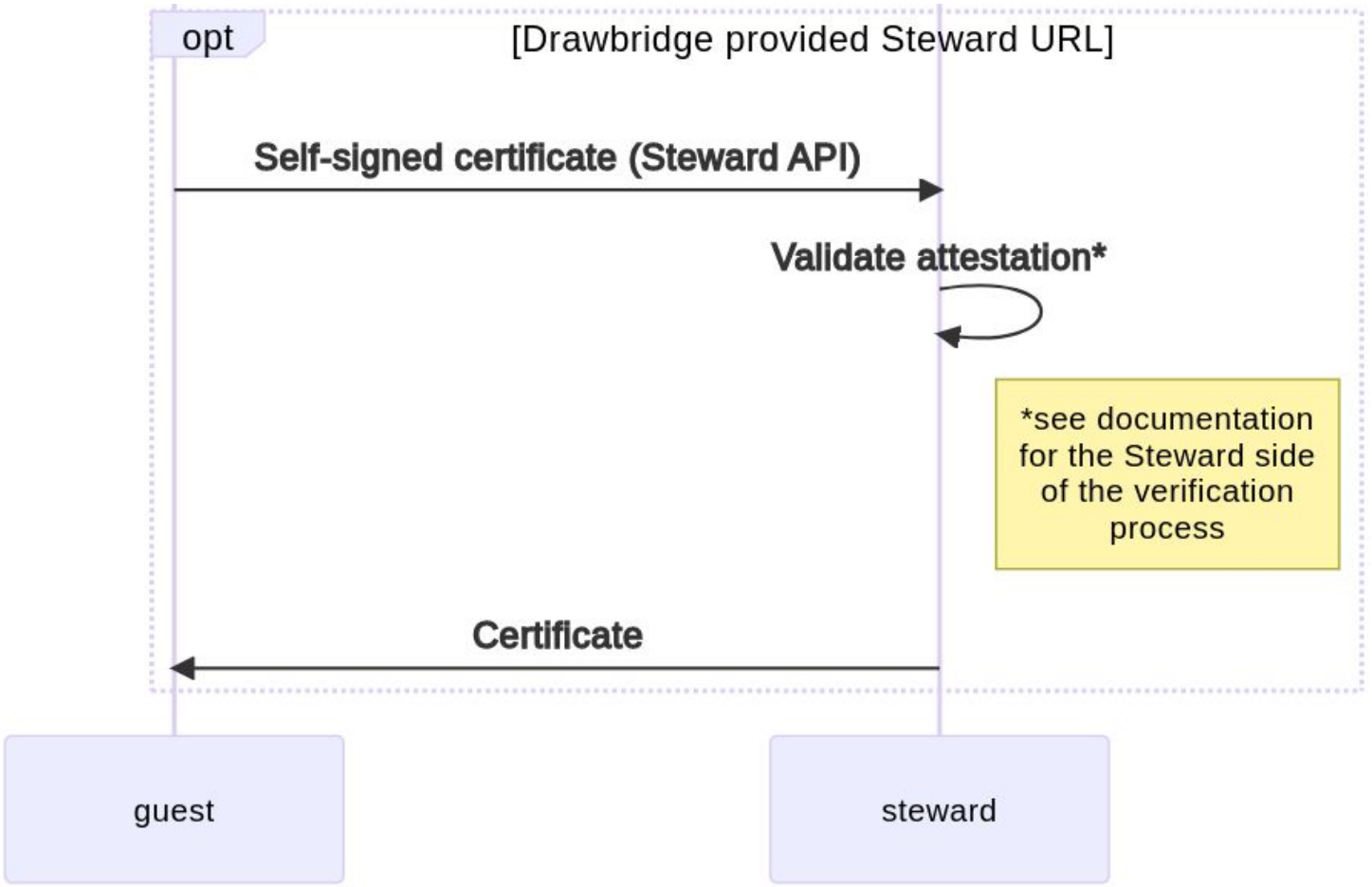


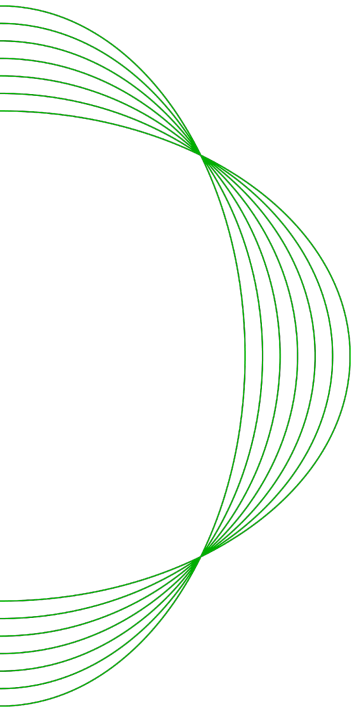
Establish workload identity (part 2)



Establish workload identity (part 3)

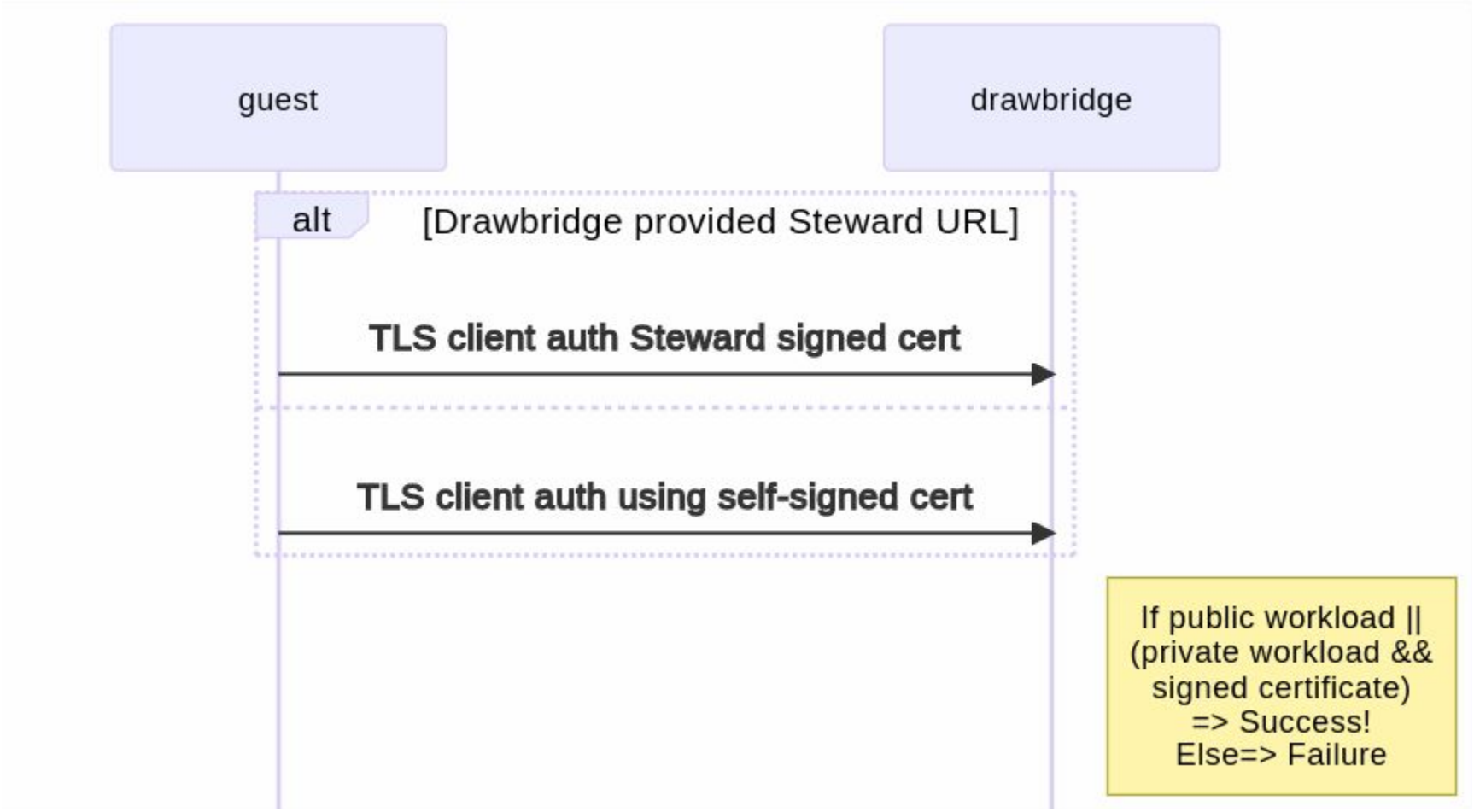
Establish workload identity (part 4)



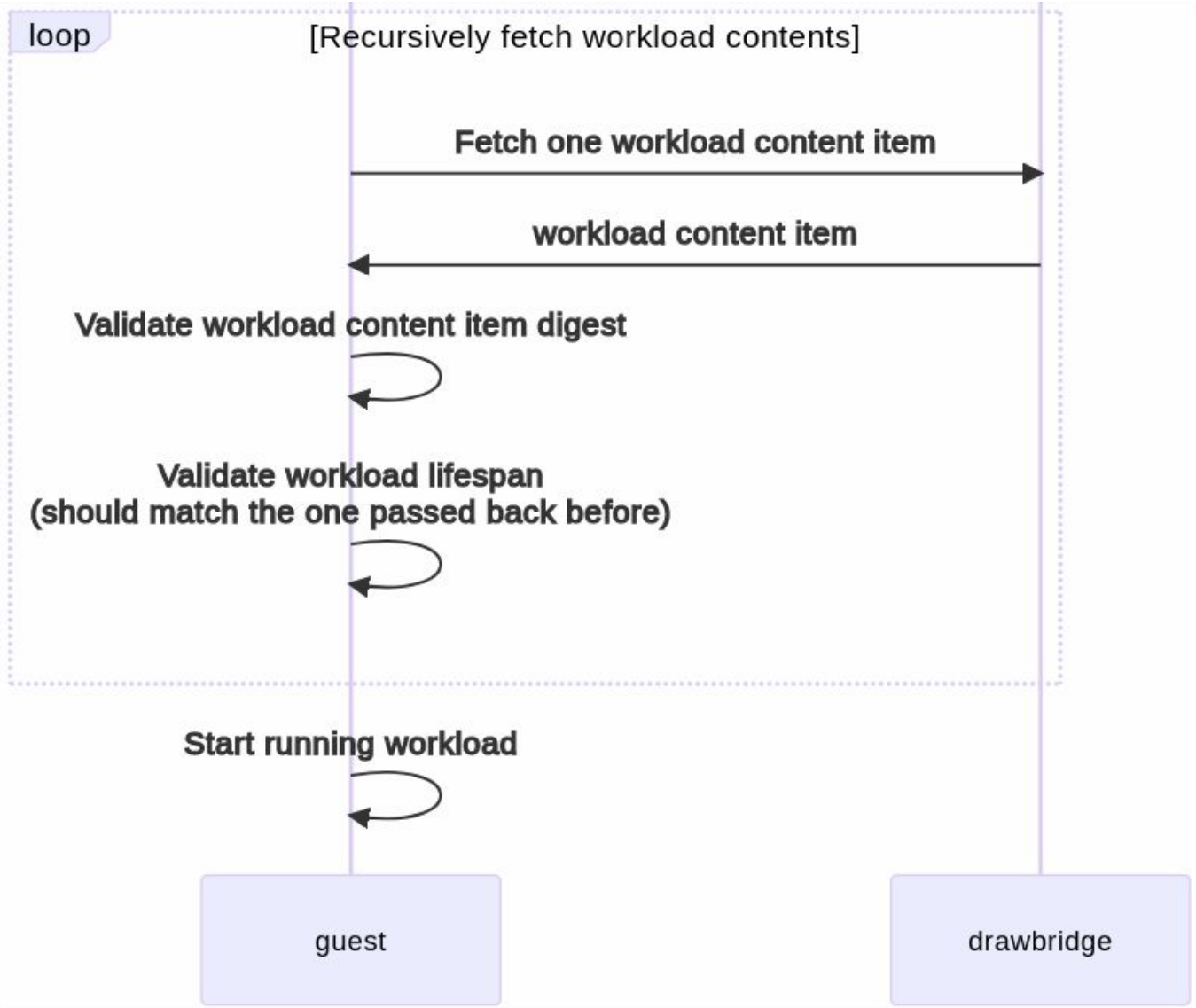


Download and execute workload

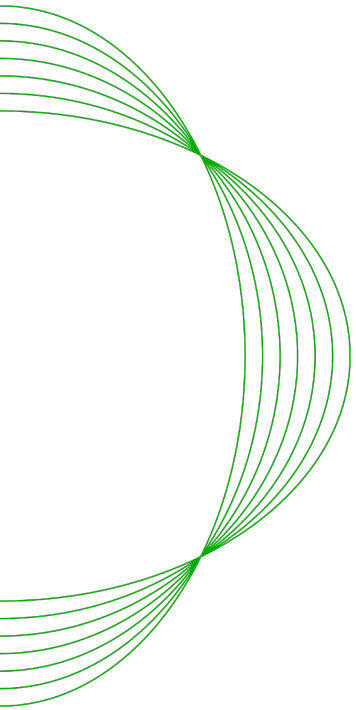
Download and execute workload (part 1)



Download and execute workload (part 2)

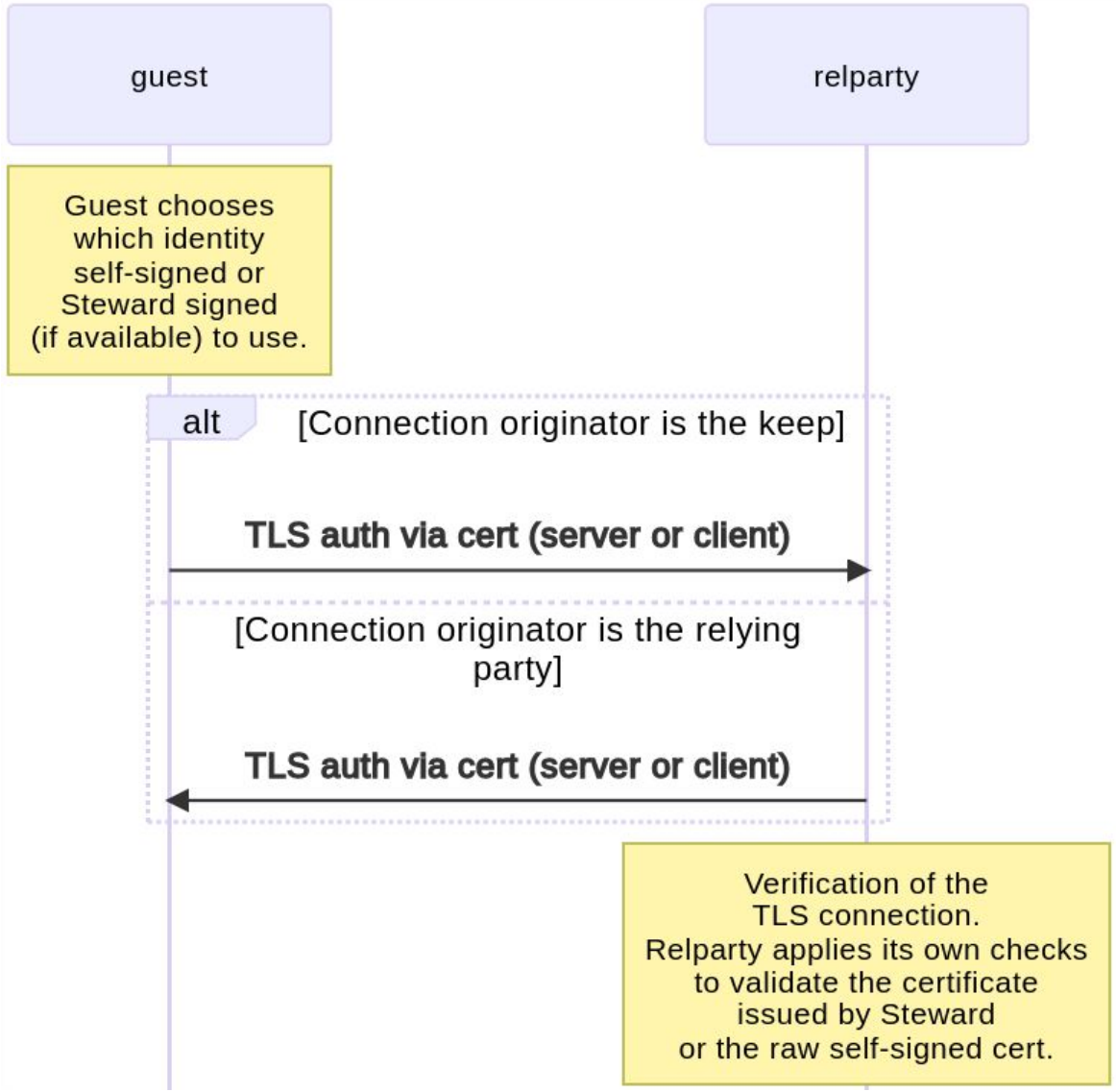


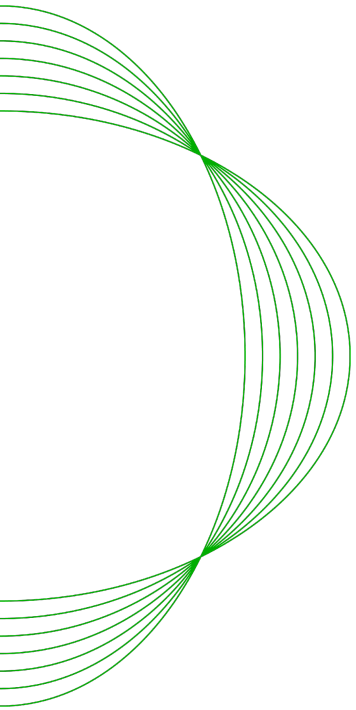
Profian



Attest to relying parties

Attest to relying parties





Questions?

Profian

Thank you.

Dmitri Pal

Profian.com

dmitri@profian.com