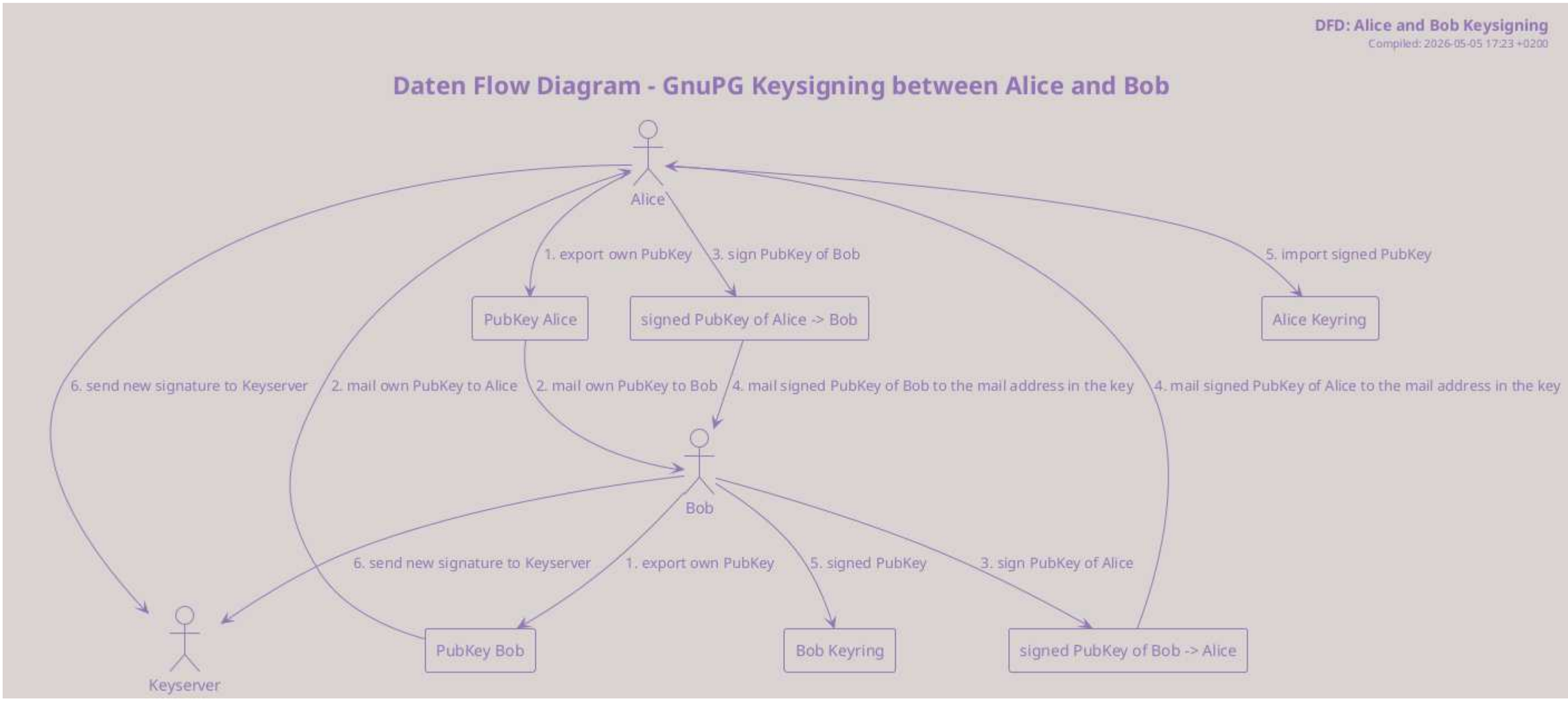
PLantUML Diagrams for GnuPG Key Signing and Reproducible Builds (SLSA4)

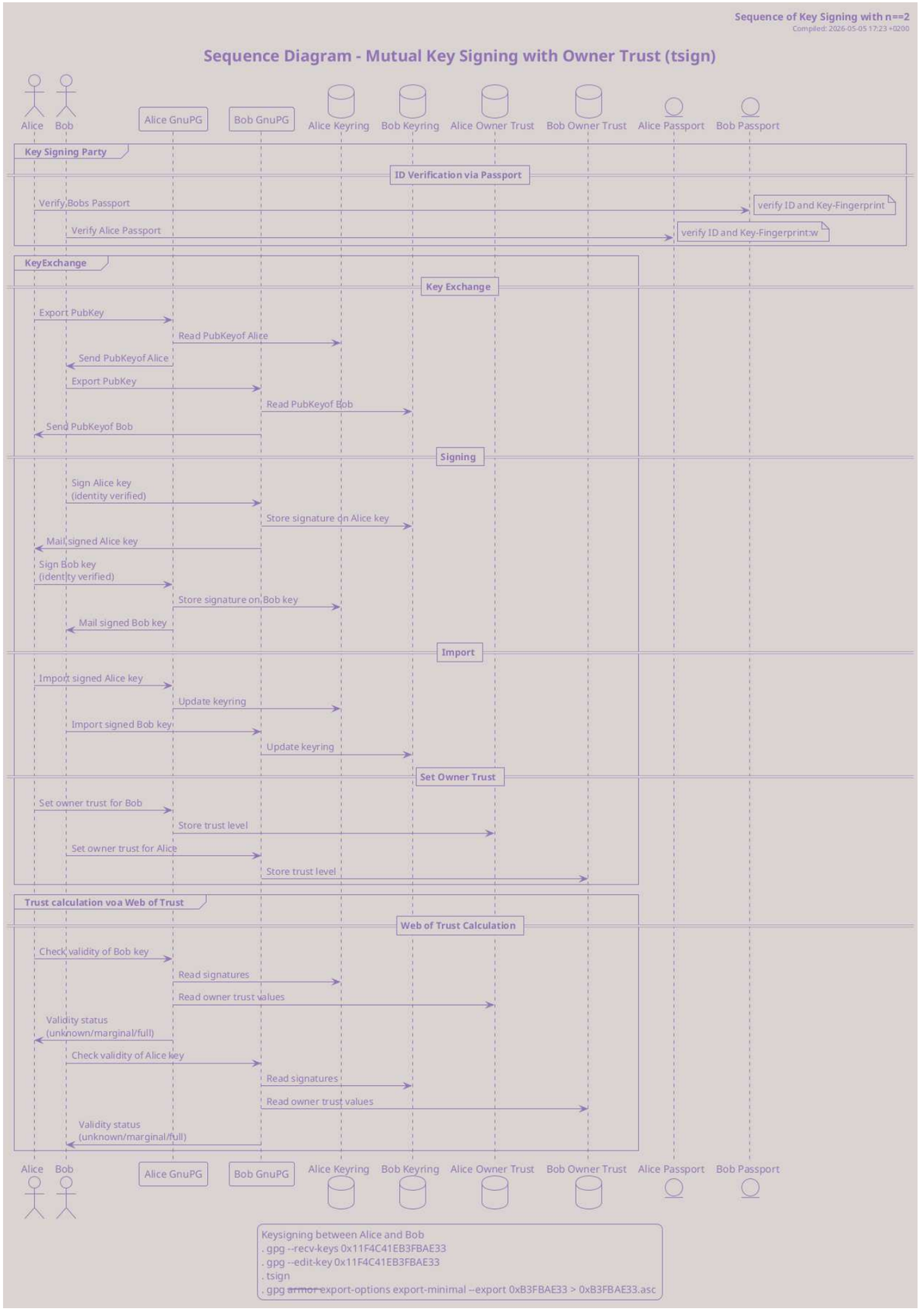
I am trying to model implicit and explicit trust in Zero Trust Architecture diagrams for Threat Modeling.

So I need to bring together the Blue Team/White Hat perspective and the Red Team/Black Hat stuff.

DFD: Keysigning Simple



SEQ: Keysigning with ID check and WoT


Sequence Diagram - Mutual Key Signing with Owner Trust (tsign)
Alice
Bob
Alice GnuPG
Bob GnuPG
Alice Keyring
Bob Keyring
Alice Owner Trust
Bob Owner Trust
Alice Passport
Bob Passport
Key Signing Party
ID Verification via Passport
Verify Bobs Passport
verify ID and Key-Fingerprint
Verify Alice Passport
verify ID and Key-Fingerprint:w
KeyExchange
Key Exchange
Export PubKey
Read PubKeyof Alice
Send PubKeyof Alice
Export PubKey
Read PubKeyof Bob
Send PubKeyof Bob
Signing
Sign Alice key
(identity verified)
Store signature on Alice key
Mail signed Alice key
Sign Bob key
(identity verified)
Store signature on Bob key
Mail signed Bob key
Import
Import signed Alice key
Update keyring
Import signed Bob key
Update keyring
Set Owner Trust
Set owner trust for Bob
Store trust level
Set owner trust for Alice
Store trust level
Trust calculation voa Web of Trust
Web of Trust Calculation
Check validity of Bob key
Read signatures
Read owner trust values
Validity status
(unknown/marginal/full)
Check validity of Alice key
Read signatures
Read owner trust values
Validity status
(unknown/marginal/full)
Alice
Bob
Alice GnuPG
Bob GnuPG
Alice Keyring
Bob Keyring
Alice Owner Trust
Bob Owner Trust
Alice Passport
Bob Passport
Keysigning between Alice and Bob
. gpg --recv-keys 0x11F4C41EB3FBAE33
. gpg --edit-key 0x11F4C41EB3FBAE33
. tsign
. gpg armor export-options export-minimal --export 0xB3FBAE33 > 0xB3FBAE33.asc

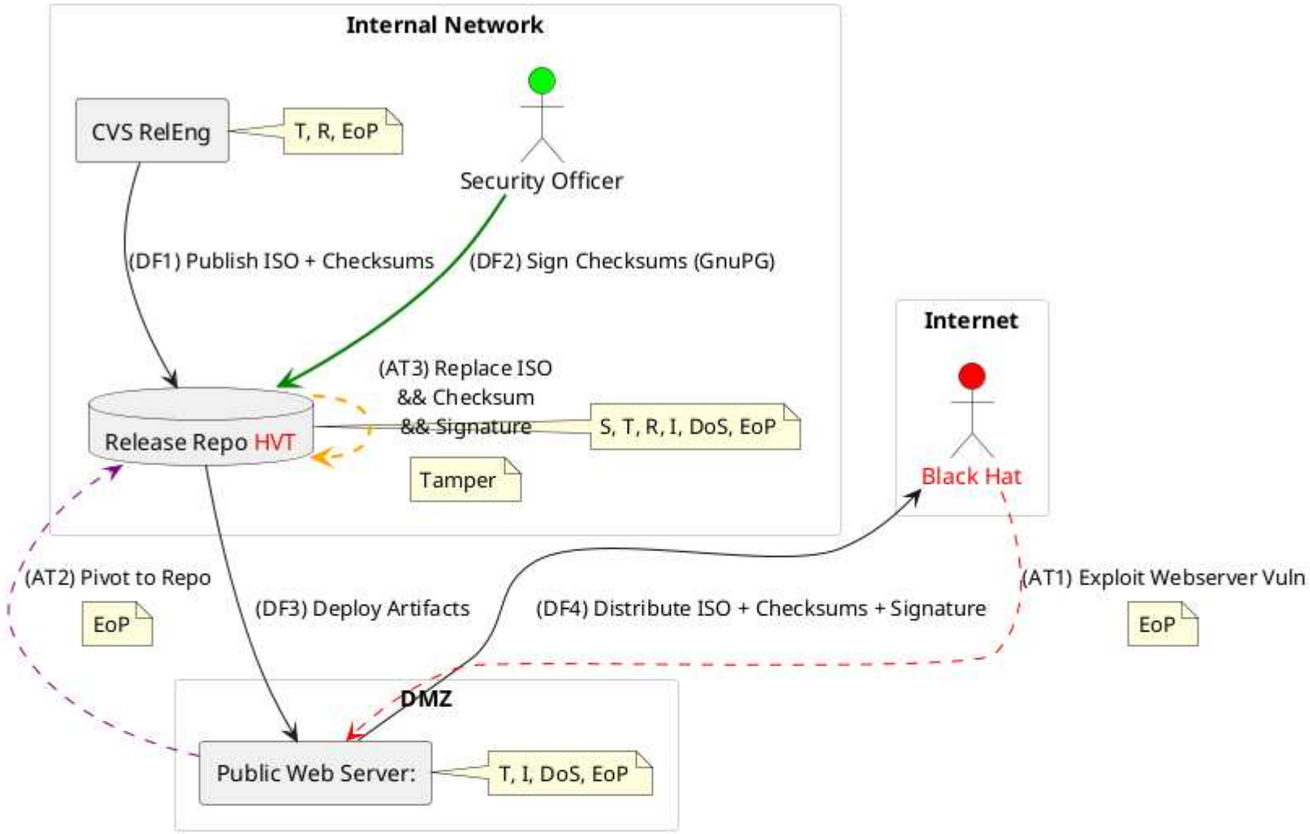
NetBSD RelEng Attack STRIDE

The ISO Image is built, signed and uploaded to the WWW server, as well as the Signature file and checksums.

Evil Black Hat hacks the webserver, and swaps the ISO image for a manipulated one with a valid Signature.

The manipulated Signature verifies the fake-integrity of the manipulated ISO image, but not the authenticity.

Attack Flow and Trust Boundaries: manipulated ISO image AND manipulated checksums/signatures (SLSA1)



STRIDE	Abbreviation
S	Spoofing
T	Tampering
R	Repudiation
I	Information Disclosure
DoS	Denial of Service
EoP	Elevation of Privilege

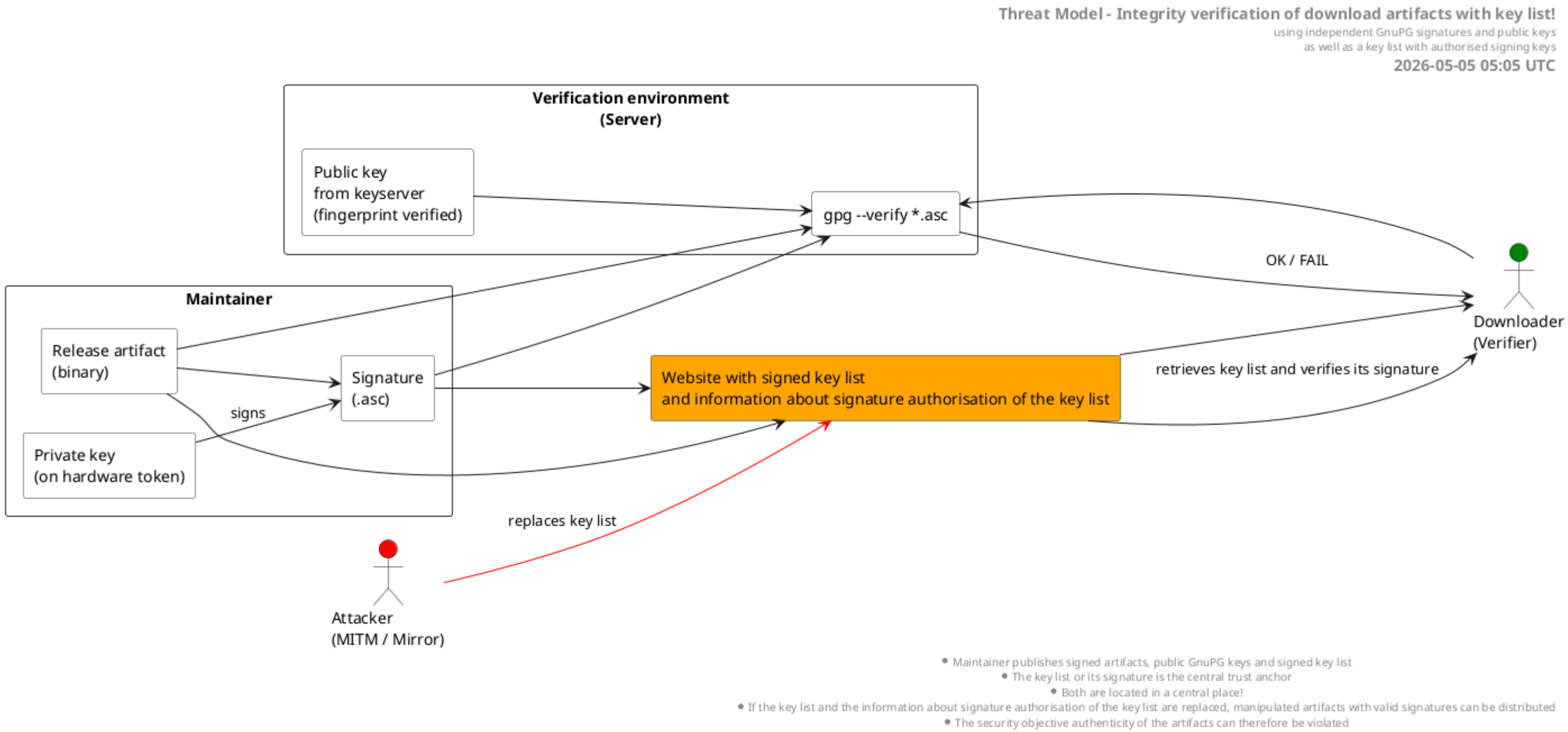
Relationship Colour

Colour	Attack Phase
Red	Initial Exploit
Deep Purple	Lateral Movement
Orange	Integrity Violation
Green	Legitimate Signing

LightGray box: Trust Boundary
Notes on Relation: STRIDE category
DF: Data Flow
AT: Attack Path

Supply-chain Levels for Software Artifacts

A simple threat model for SLSA Level 1 and Leve 4 build and distribution pipelines.



Reproducible Builds SLSA L4

Modeling Trust, Trust Anchors and Boundaries and Attack Vectors for SLSA4:

The whole process draws heavy inspiration from those implemented by NetBSD, Debian, NixOS and the Tor Browser!

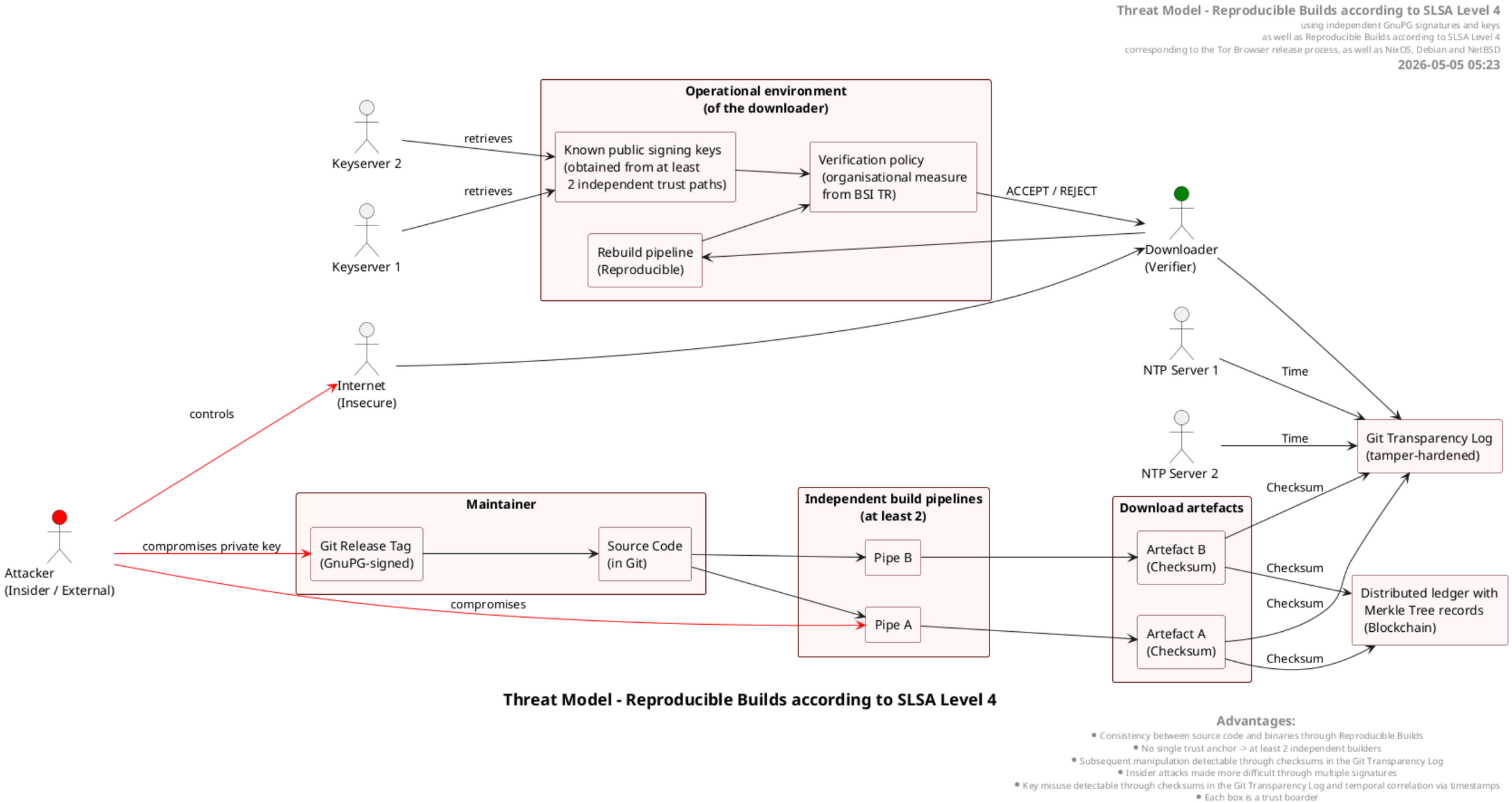
Goals:

a. Build process produces identical artefacts (bit-for-bit) from the same source and inputs
b. independent parties can rebuild and verify outputs match the original → verify freedom from insider threat!
c. require a deterministic build environments

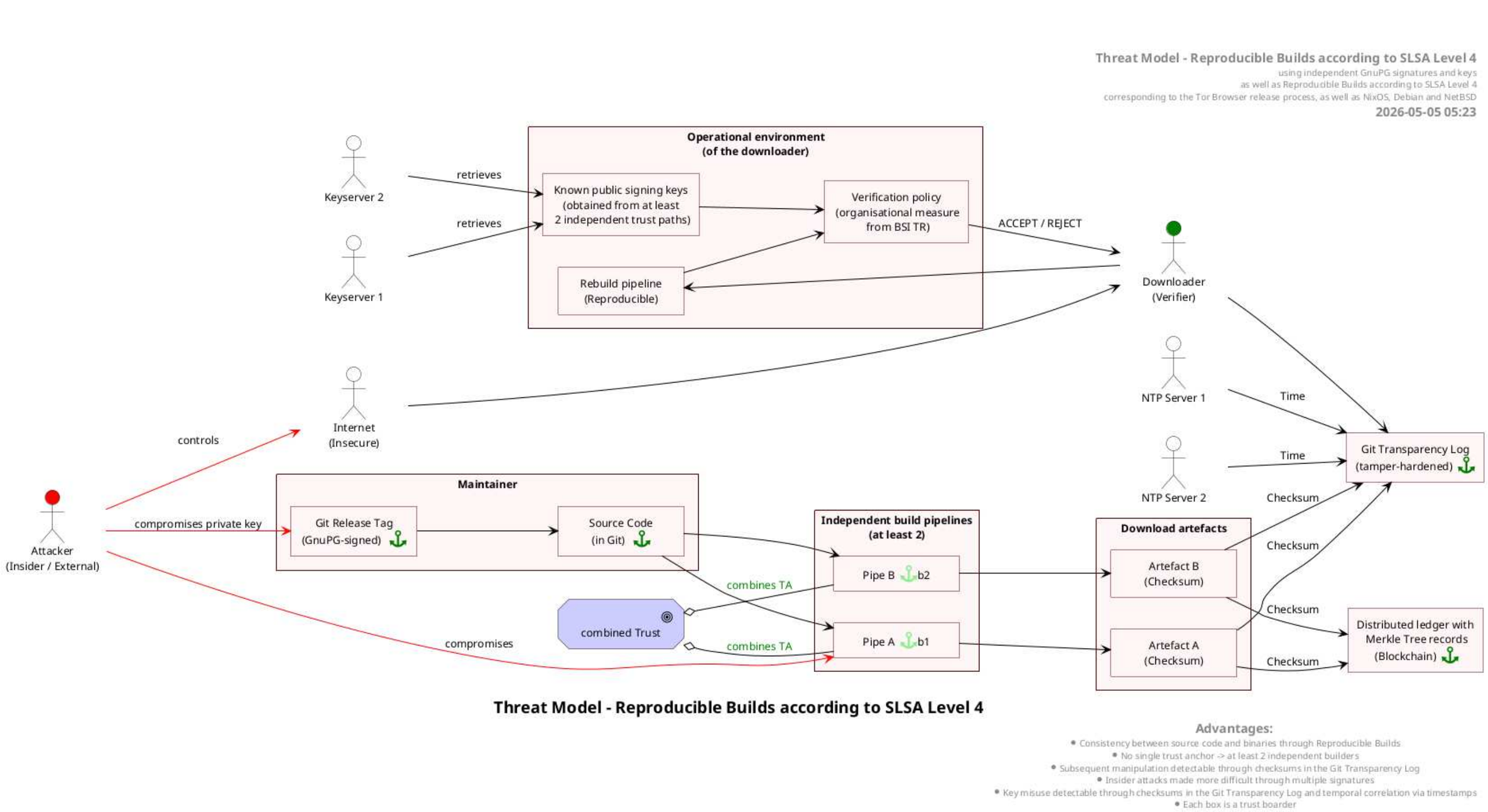
d. all build steps, dependencies, and tooling are tightly controlled and audited
    1. security goals:
e. detect tampering in build pipelines or artefacts
f. prevents hidden backdoors introduced during compilation or packaging by a malicious insider
g. ensure integrity of supply chain, dependencies and build tools
h. enables independent verification without trusting the original builder
i. drastically reduce insider and supply chain attack surface
    1. Zero Trust:
j. never trust, always verify!
k. verifiable evidence (rebuild && compare)
l. eliminates implicit trust in build pipeline
m. build system considered untrustworthy
n. combine with signed artefacts and attestation frameworks for full supply chain integrity

The whole implementation

- Trust Boundaries: Rectangles
- Attack Vectors: Red Arrows



- Trust Anchor: Green Anchor



Motivation/Business Layer: Risk/Security Overlay

SLSA4 - Risk and Security Overlay