Sigsum

Niels Möller
Glasklar Teknik AB

Problem statement

Do you depend on, or create, signed artifacts? How would you know if a signing key is compromised or misused?

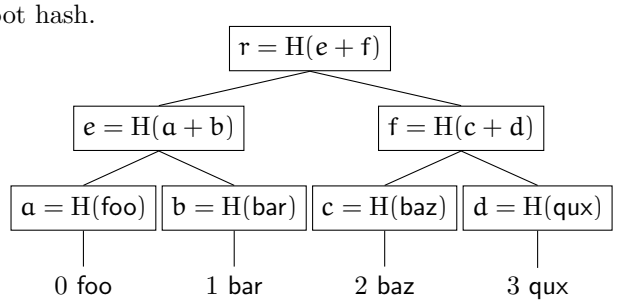
Objective

Sigsum brings transparency to the way signing keys are used. No signature that a verifier accepts as valid goes unnoticed because it is included in a public log.

The system does not prevent an attacker from using a compromised key to attack users. The aim is to detect such attacks, which may also deter potential attackers.

Preliminaries

A Sigsum log is a public append-only data structure, based on a Merkle tree. The state is represented by its size and root hash.



It is efficient to verify both that a certain entry is in the log (an Inclusion Proof), and that no previous entries were removed or modified as the log grows (a Consistency Proof).

A Sigsum leaf

Value	Size (bytes)	Purpose
Checksum	32	What?
Public key hash	32	By whom?
Signature	64	Binding

Threat model

The attacker is assumed to control all of:

- The signer's secret key and distribution infrastructure.
- The public log, including its hosting and secret key.
- A few (not too many) of the trusted cosigning witnesses.

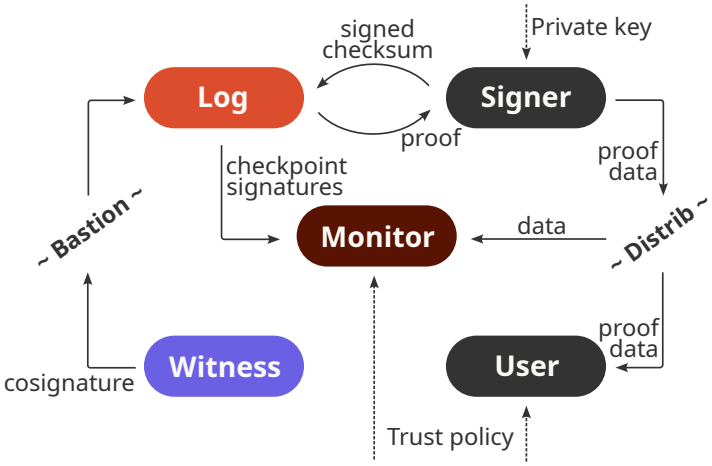
Example transparency applications

- Software updates
- Break-glass emergency access
- Delayed vulnerability publication
- Shell access

Tools

```
$ sigsum-submit -p POLICY -k SECRET < DATA
$ sigsum-verify -p POLICY -k PUB PROOF < DATA
$ sigsum-monitor -p POLICY PUB ...
```

System design



Parameters	Sigsum's choice
Anti-poison	No arbitrary leaf bytes
Anti-spam	Domain names, public keys
API & formats	HTTP, text
Cryptography	SHA256, Ed25519
Data structure	Chronological Merkle tree
SCTs	No
Sharding	No
Split-view	Witness cosigning
Submitter privacy	Mostly preserved
User privacy	Preserved

Sigsum proof of logging

```
version=2
log=44ad38f8...22a1
leaf=c0d8a714...0671 1c4ca8da...2400

size=5057
root_hash=aa82ce8a...d7f2
signature=0a334ae9...f301
cosignature=6bdf...04e3 1744717315 bc2c...280a
...

leaf_index=5056
node_hash=ee77a8fb...03ba
...
```

Trust policy

```
log 0ec7...1f25 https://seasalp.glasklar.is/

witness witness.glasklar.is b2106db9...8536
witness witness.mullvad.net 15d6d014...61ad
witness filippo-dev         68b0b4cd...67b8

group quorum-rule 2 w.gis ...  filippo-dev
quorum quorum-rule
```

https://www.sigsum.org/docs