



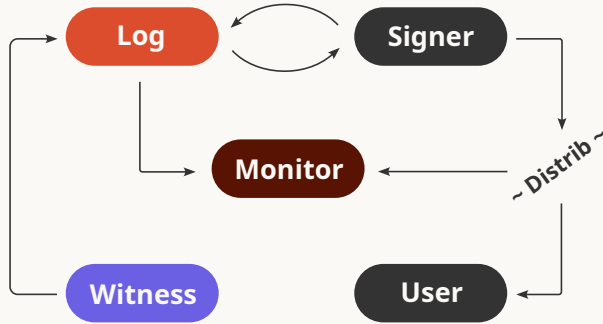
The diff between sigsum/v1 and sigsum/v2?

October 1, 2026

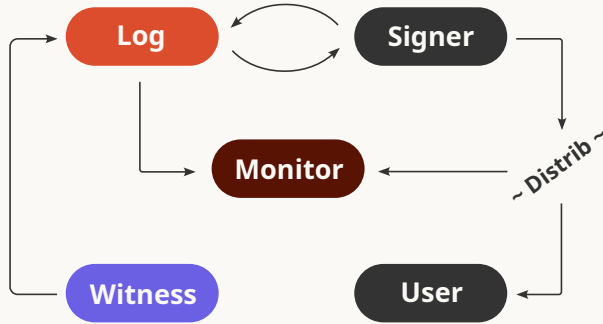
Rasmus Dahlberg

rgdd@glasklarteknik.se

Overview



Overview



Overall system remains the same

What we're planning to change

- Use the shared C2SP.org specs
- Decide what should be in the leaf
- (Decide how a leaf gets submitted)
- (Specify a bit of policy and glue)



The Community Cryptography Specification Project



The Community Cryptography Specification Project (C2SP) is a project that facilitates the maintenance of cryptography specifications using software development methodologies, applying the successful processes of open source to specification documents.

What we're planning to change

- Use the shared C2SP.org specs
- Decide what should be in the leaf
- (Decide how a leaf gets submitted)
- (Specify a bit of policy and glue)



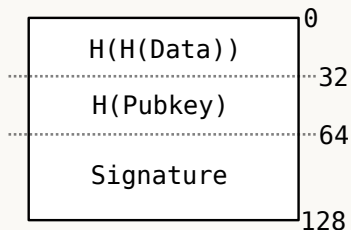
The Community Cryptography Specification Project



The Community Cryptography Specification Project (C2SP) is a project that facilitates the maintenance of cryptography specifications using software development methodologies, applying the successful processes of open source to specification documents.

Focus of this talk: the upcoming leaf

What we have today



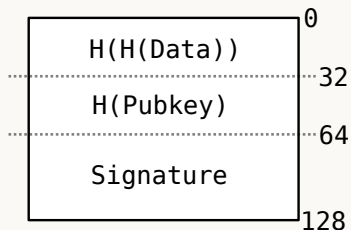
`Namespace = "sigsum/v1/tree\0"`

`Checksum = H(H(Data))`

`Message = Namespace + Checksum`

`Verify(Pubkey, Message, Signature)`

What we have today



`Namespace = "sigsum/v1/tree\0"`

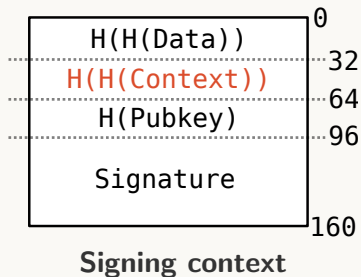
`Checksum = H(H(Data))`

`Message = Namespace + Checksum`

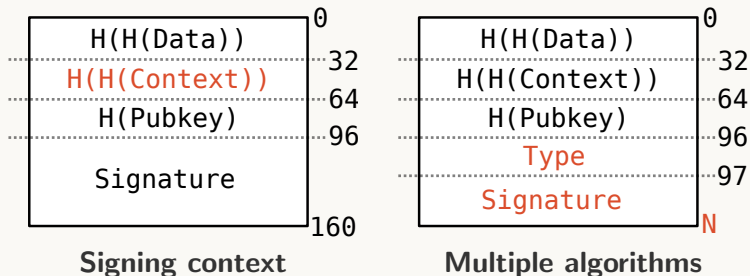
`Verify(Pubkey, Message, Signature)`

Double hash to protect both the submitter and the log

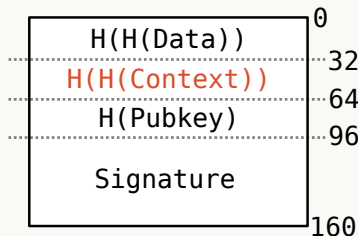
Building the upcoming leaf step-by-step



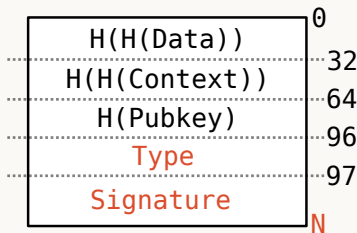
Building the upcoming leaf step-by-step



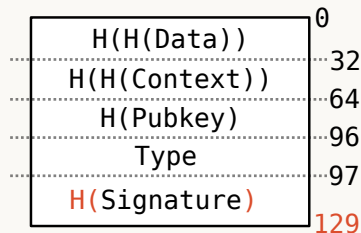
Building the upcoming leaf step-by-step



Signing context

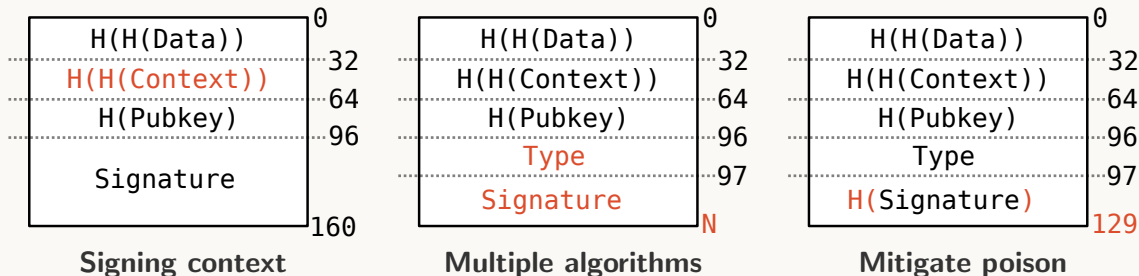


Multiple algorithms



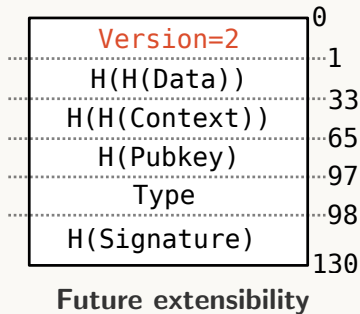
Mitigate poison

Building the upcoming leaf step-by-step



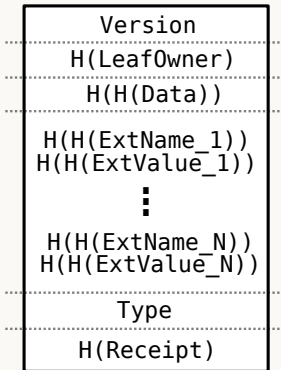
Signature as 'extra data' also makes it possible to not store large signatures forever

Building the upcoming leaf step by step (continued)



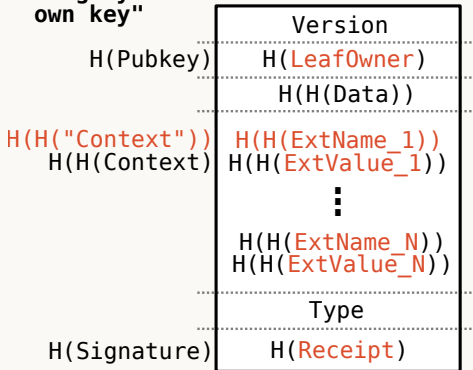
Interoperability?

The so-called identity-based leaf

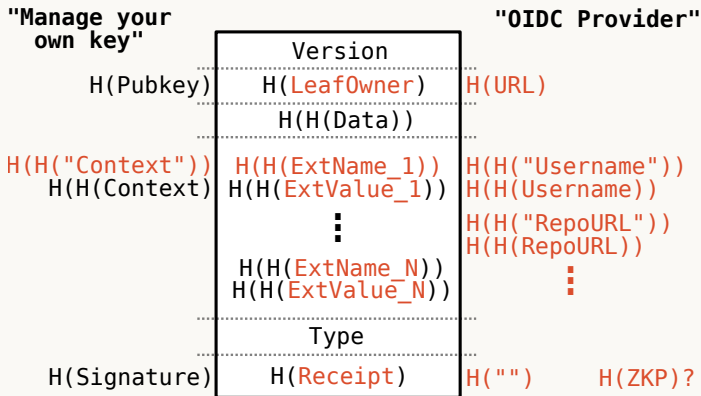


The so-called identity-based leaf

"Manage your
own key"

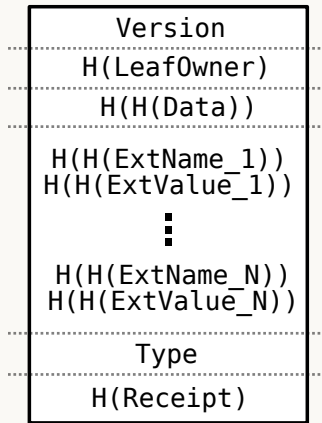


The so-called identity-based leaf



sigsum/v2 likely boils down to:

- Same parties, flows, and semantics
- Core C2SP.org specifications
- Flavor of identity-based leaf
- One or more submit endpoints
- A bit of policy and glue...



Context extension + receipt based on Ed25519, MLDSA-44, or hybrid signature

Thank you

Project <https://www.sigsum.org/>

Speaker <https://www.rgdd.se/>

Slides <https://git.glasklar.is/rgdd/tds-26/>

Leaf <https://github.com/C2SP/C2SP/pull/244>

This is a work in progress together with several community members, notably including Hayden Blauzvern, Filippo Valsorda, Niels Möller, and many of the regulars at Sigsum weekly meets.