

DAP taskprov: In-band Task Provision Extension

PPM - IETF 118 - Prague

Motivation

An automated mechanism for provisioning a DAP task among Clients and Aggregators.

Changes since IETF114:

- Updated to fit DAP-07 and VDAF-07.
- Use HTTP header to transport TaskConfig.

TaskConfig Struct ([The Taskprov Extension {#definition}](#))

```
struct {
    /* Info specific for a task. */
    opaque task_info<1..2^8-1>;

    /* Leader API endpoint as defined in I-D.draft-ietf-ppm-dap-07. */
    Url leader_aggregator_endpoint;

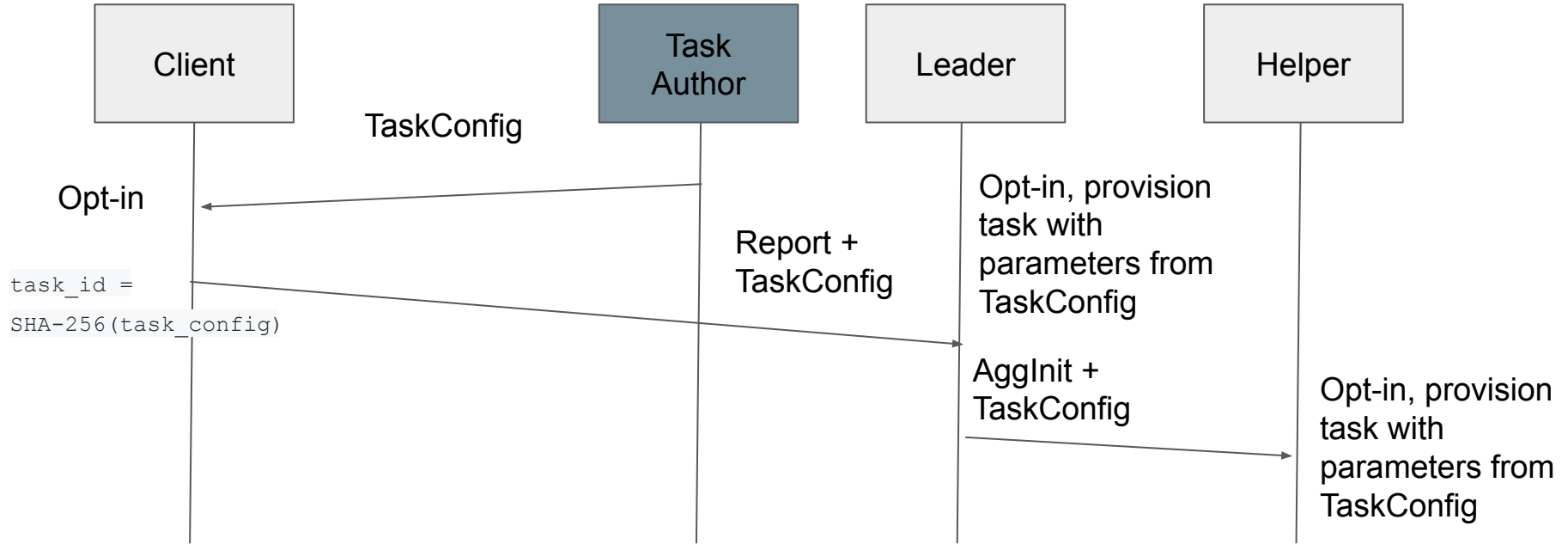
    /* Helper API endpoint as defined in I-D.draft-ietf-ppm-dap-07. */
    Url helper_aggregator_endpoint;

    /* This determines the query type for batch selection and the
       properties that all batches for this task must have. */
    QueryConfig query_config;

    /* Time up to which Clients are allowed to upload to this task.
       Defined in I-D.draft-ietf-ppm-dap-07. */
    Time task_expiration;

    /* Determines the VDAF type and its config parameters. */
    VdafConfig vdaf_config;
} TaskConfig;
```

Taskprov Flow

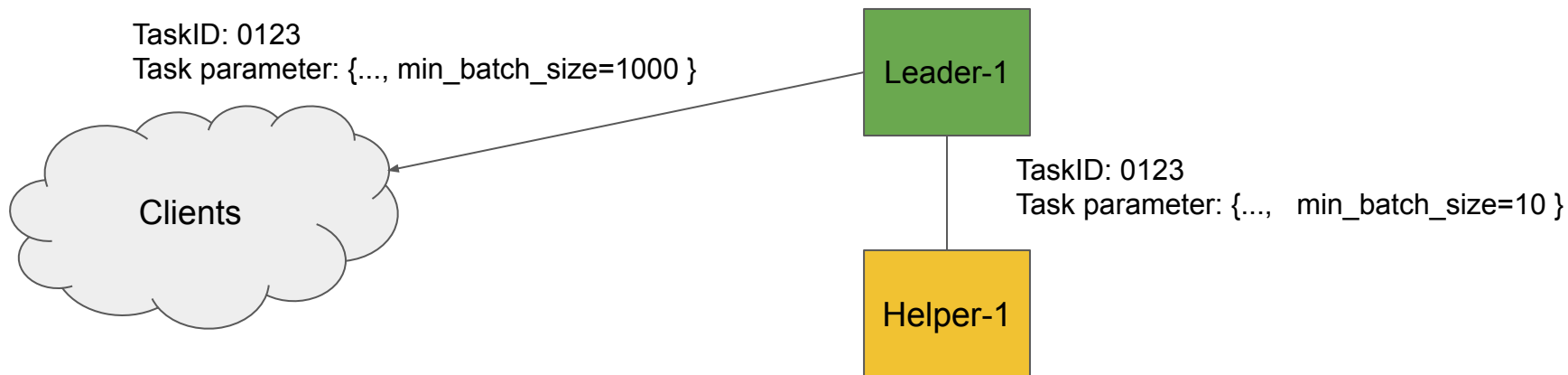


- *Leader and Helper exchange VDAF verify_key_init out of band, once in a while.*

Key Properties

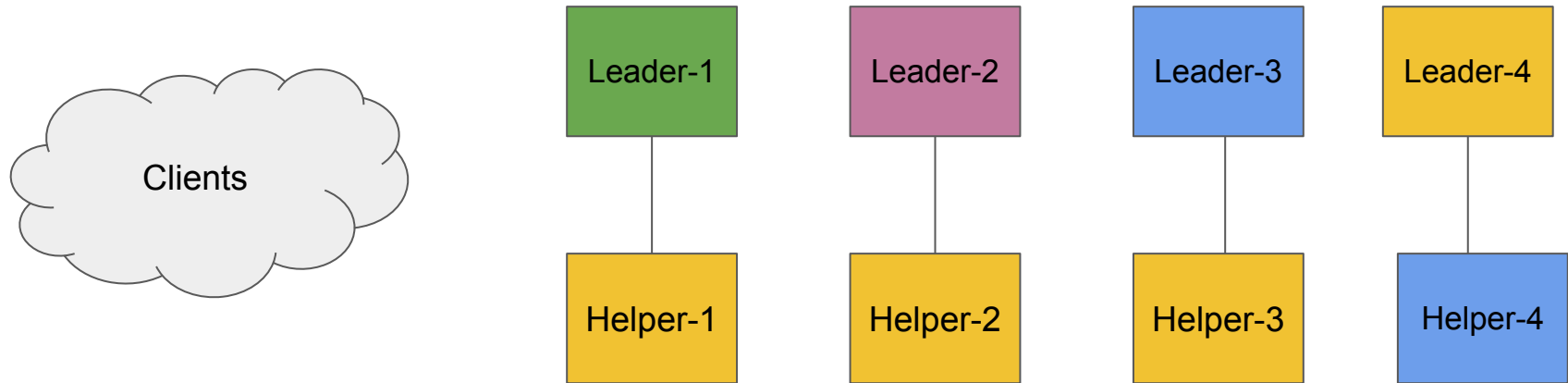
Binding TaskID with TaskConfig: allows each party to know task is configured using the parameters it has opt-in to.

- For Client: better transparency and auditing.
- For Aggregators: mitigate cross-protocol attack.



Key Properties

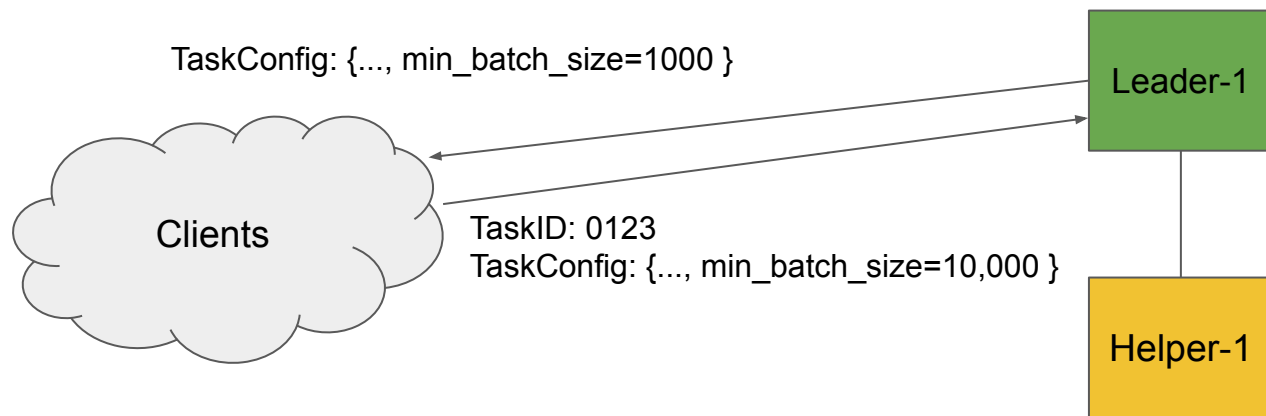
Deployment Agnostic: Task provision happens in-band, no out-of-band mechanism required.



May require 3 different OOB task provision methods

Key Properties

Allow Client to update task parameters: Client can hardcode privacy parameters, or update them without informing Aggregators.



Operational Considerations

Suitable Deployment:

- Payload size \gg TaskConfig size.
- High cardinality of tasks, > 1000 s.
- > 1 Aggregator pairs.
- Client can update TaskConfig.

Bandwidth waste: TaskConfig is uploaded with every Report.

Malicious client polluting Aggregator storage by uploading many distinct TaskConfigs.

- One mitigation: TaskAuthor to include TaskConfig signature

Call for adoption as DAP extension

It's not suitable for every DAP deployment, but we feel it's useful to many. Therefore we want call for adoption as extension.

Latest draft: <https://datatracker.ietf.org/doc/draft-wang-ppm-dap-taskprov/05>.