Part of the Standard vs Choices by Vendor

Standard Parameters:

1. *Unit of Privacy:* The set of parties used to manage the privacy budget.
2. *Epoch:* The amount of time over which the differential privacy budget is managed.

Vendor Parameters:

1. ε: The differential privacy parameter which measures the amount of individual differential information leakage allowed in each epoch.
2. *Aggregation minimum threshold*: the number of clients/users that need to be included in a given aggregation.
3. *Private Computation Instantiation*: When servers are used, do we leverage MPC or TEEs?

Current State of MPC and TEE

	Privacy	Scale
MPC	Likely Consensus	Open Question
TEE	Likely No Consensus	Likely Can Support

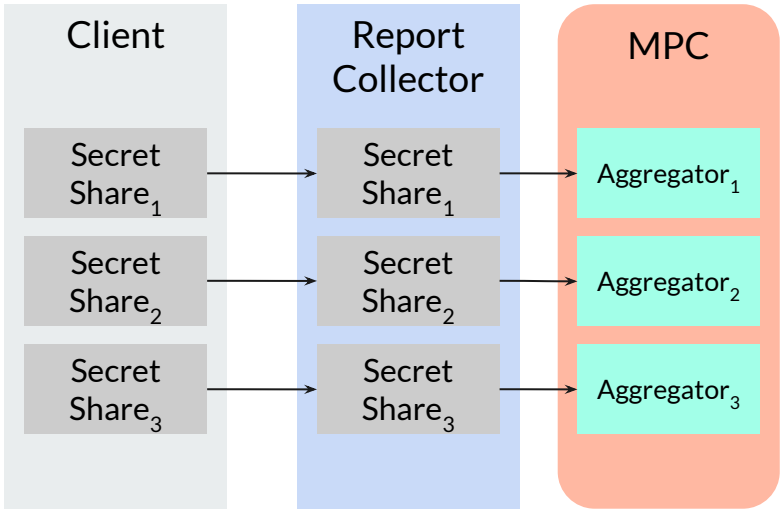
Goal for *PATCG/WG* Specs

Standardized Methodology
to allow for uniform service to all sites/apps

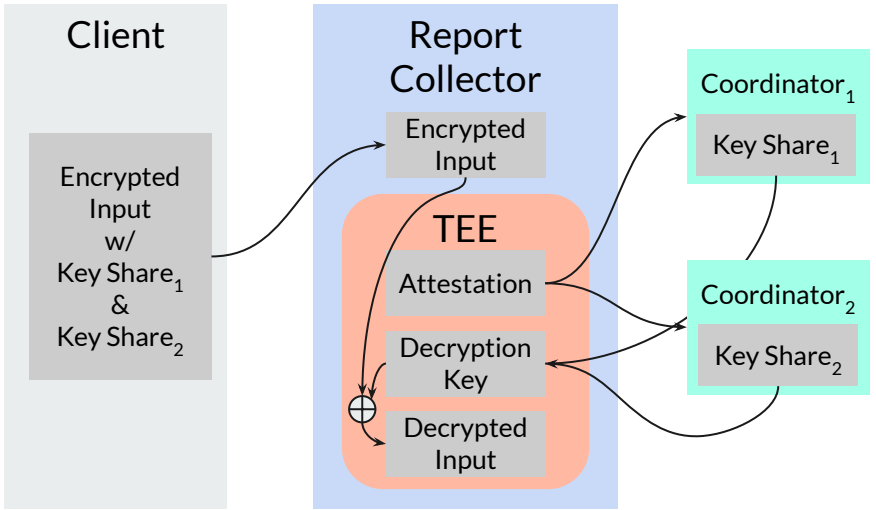
Incremental Extensions
provided by a subset of web platform vendors

Helper Party Networks

Aggregators (MPC)



Coordinators (TEE)



Helper Party Network Responsibilities

- **Privacy:** Limit the usage of encrypted reports provided by a specified API to the predefined function, without revealing any new information beyond the output of that predefined function.
  - This includes limiting the number of times a report can be used, for example by:
    - Preventing replay attacks, e.g., reports can only be used once (client side privacy budgeting)
    - Tracking a differential privacy budget (server side privacy budgeting)
- **Correctness:** Parties recieving the intended output can trust that the predefined function is computed correctly.

Spliting Privacy Budgets

Suppose that Browser_A allows for:

- 5 units of privacy (typically measured by ε)
- Helper Party Networks (HPN): HPN_1, HPN_2, HPN_3

With the same privacy guarantee, you could split your privacy budget across any subset of those HPNs. For example, the following would all have the same privacy guarantee:

- 5 units assigned to HPN_1
- 2 units assigned to HPN_1 and 3 units assigned to HPN_2
- 2 units assigned to HPN_1, 2 units assigned to HPN_2, and 1 unit assigned to HPN_1

Layering Private Computation Instantiations

	Privacy Budget	Supported Instantiations
$Browser_A$	5 Units	MPC
$Browser_B$	10 Units	MPC, TEE
$MobileOS_C$	3 Units	MPC
$MobileOS_D$	10 Units	MPC, TEE

	Platforms Supported	Assigned Budget	Events From
$HPN_{1\text{-}MPC}$	All	3 Units	All Platforms
$HPN_{2\text{-}MPC}$	All	2 Units	$Browser_A$, $MobileOS_C$, $MobileOS_D$
$HPN_{3\text{-}TEE}$	$Browser_B$, $MobileOS_D$	5 Units	$Browser_A$, $MobileOS_D$

Open Issues - github.com/patcg/docs-and-reports

- #16 Expand on privacy budgeting
- #19 Who is assumed to have access to first and delegated party assets?
- #20 Collusion within and across helper party networks
- #21 Should we include a mitigation for running coordinators across multiple clouse providers?
- #22 Abstract MPC beyond secret sharing based MPC
- #23 Helper Party networks with single coordinator vs multiple cooridators (likely resolved)
- #24 Include FHE as an instantiation of private computation
- #25 Complete section “1.9 Operators of TEEs” (looking for TEE experts)