Privacy groups

Tessera supports operations related toHyperledger Besu privacy groups andresident groups for GoQuorum multiple private states (MPS) , such as managing privacy group data and handling transactions intended for a privacy group.

Behavior may differ depending on whichmode Tessera is running on.

The types of privacy group are:

- Legacy privacy group
- .
- Pantheon privacy group
- .
- Resident privacy group
- .

A uniqueprivacyGroupId is used to identify individual privacy groups. For private transactions sent to a privacy group, the correspondingprivacyGroupId is stored alongside the transaction.

note Once created, you can't change the members of a privacy group. To add or remove members, you must create a new privacy group. The following is an example of a privacy group and its related data:

{ "privacyGroupId": "jufzisK63xbXDciV0FW1uAi3vXFDNNJpf/M3lUhMiU0=", "name": "groupA", "description": "A description of this group", "type": "PANTHEON", "members": ["98FhPni7u6YspDGcOLl/LgQQwwGPGY4ddm3hmogsqF8=", "dzkrEhkHZ/IjHEaQ6teVTU/kMjiwXTI6Ooljcb56w1M="] }

Privacy group types

Legacy

Tessera automatically creates a legacy privacy group when a private transaction is sent to a list of recipient public keys usingprivateFor .

When returning private transaction data to a Besu client (as part of a/receive response), the legacyprivacyGroupId is also returned.

The legacyprivacyGroupId is generated by hashing the list of recipient keys. For a given set of recipients, there can be only one legacy privacy group.

note Besu and Tessera generate the same legacyprivacyGroupId from the same list of recipients.

Pantheon

Tessera supports API methods that enable the creation of pantheon privacy groups from a compatible blockchain client (for example, Besu).

Upon creation, the privacy group is distributed to all members ahead of transaction processing.

When a private transaction contains aprivacyGroupId , the transaction payload is distributed to all the members of the privacy group.

The pantheonprivacyGroupId is generated by hashing the list of recipient keysplus a random seed . This means that for a given set of recipients, there can be many pantheon privacy groups.

Resident

Resident privacy groups, or resident groups, are part of GoQuorumMPS and multi-tenancy . A resident group contains a list of member keys that are locally managed, and those members share the same private state.

Configure resident groups to use multi-tenancy.

Key differences between a resident group and other types of privacy group include:

- A resident group can only contain local keys, not remote keys.
- The name of the resident group is the group identifier.
- Resident groups can be configured in the Tessera configuration file.

API versioning

A node running a version of Tessera that doesn't support privacy groups can't understand requests containingprivacyGroupId . This can cause inconsistent persisting of data on different nodes.

In API version 3.0, Tessera includes the privacy group in the encoded payload in/push to only those recipients supporting a correct version, otherwise the transaction fails withPrivacyGroupNotSupportedException .

Privacy group APIs

Privacy group compatible blockchain clients (for example, Besu) can be used to create, delete, find, and retrieve privacy groups. Tessera'sQ2T API adds support for these operations. Edit this page Last updatedonOct 9, 2023 bydependabot[bot] Previous Peer discovery Next Multi-tenancy