Primitives for Confidential Group Communications

Question:

How can we represent and manage group membership in a way that is verifiable, tamper-proof, and practical in a decentralized topology?

A Group Membership Block Chain (GMBC) is…

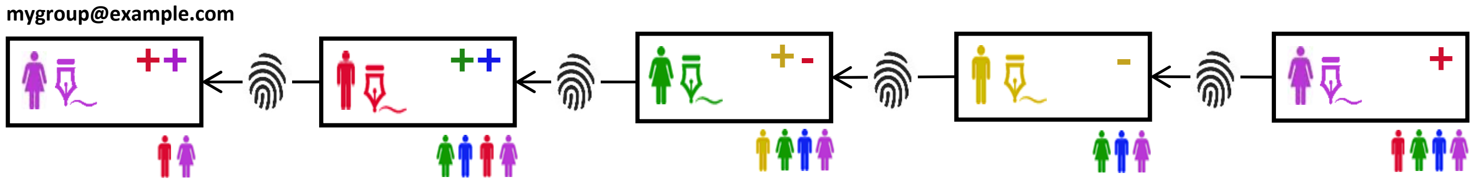
a ledger of group membership updates over time

a publicly verifiable record of membership and policy

tamper-proof based on public key authentication

supports zero-conflict centralized topologies

supports conflict-resolution in decentralized topologies



Drafts:

draft-abiggs-saag-primitives-for-conf-group-comms-01

draft-abiggs-saag-key-management-service-03

draft-thomson-xmpp-secure-00

A Group Key (GK) is…

a standard JOSE JSON representation that wraps a content key with the public keys of each other GMBC group members. GK objects can be shared openly without compromising confidentiality.