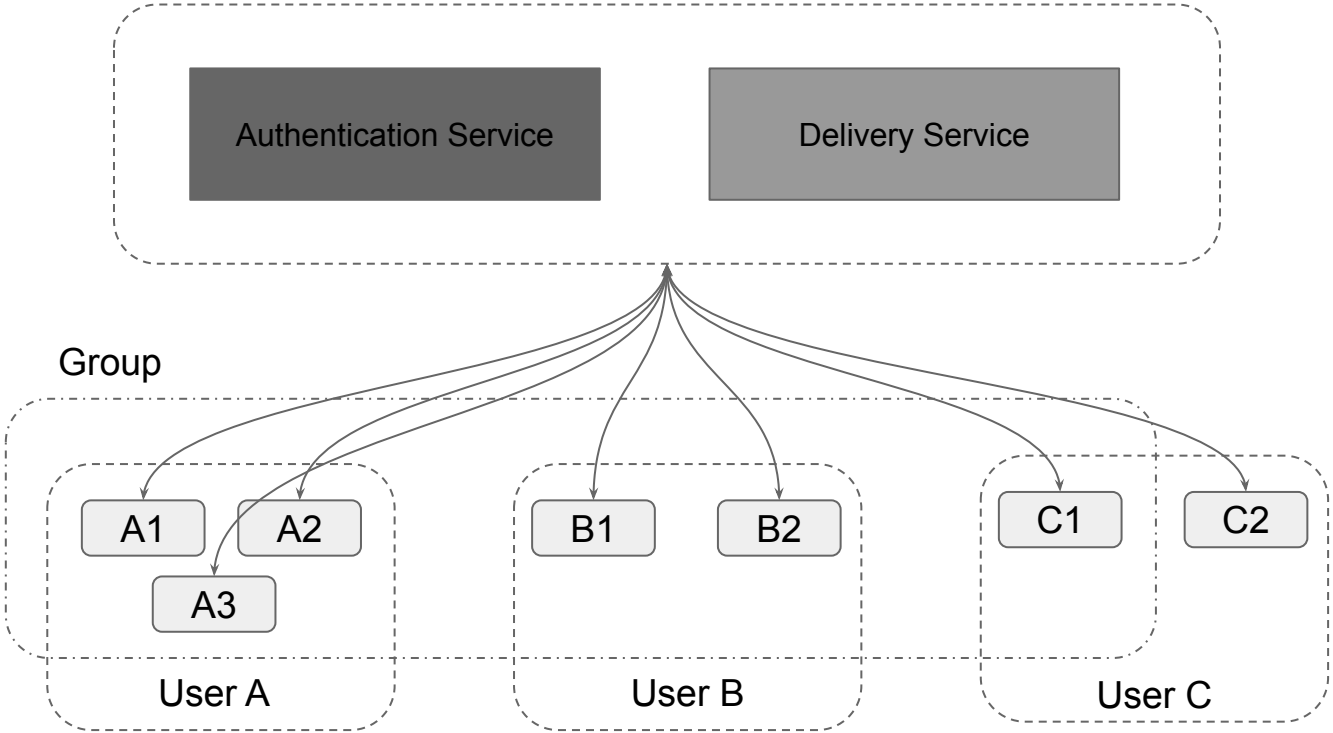
Architecture

IETF 104

benjamin.beurdouche@inria.fr

System Overview



Security Requirements

- Message secrecy, integrity and authentication
  - Only current group member can read messages
  - Messages are only accepted if it was sent by a current group member
  - *Message padding to protect against traffic analysis
  - Forward secrecy and post compromise security
  - Data origin authentication and *deniability

- Group membership security
  - Consistent view of group members
  - Added clients can’t read messages sent before joining
  - Removed clients can’t read messages sent after leaving

Functional Requirements

- Scalable
  - Support group size up to 50,000 clients
- Asynchronous
  - All client operations can be performed without waiting for the other clients to be online
- Multiple devices
  - Devices are considered separate clients
  - Restoring history after joining is not allowed by the protocol, but Application can provide that.
- State recovery
  - Lost/Corrupted state must be recovered without affecting the group state.
- Metadata collection
  - AS/DS must only store data required for message delivery
- Federation
  - Multiple implementation should be able to interoperate
- Versioning
  - Support version negotiation

Previous open questions...

- Should the draft define the frequency of key update or keep it open to the application?
- Should the protocol hide the user devices to protect their privacy?
- Is the server trusted to store group membership?

New questions ?

- Concurrency of the Group Operations
- Metadata retention
- Ephemeral signatures
- Deniability

Editorial

- Describe security guarantees and expectations with much more precision
- Recommendations for privacy related Application metadata
- Changes due to the existence of a federation document