Server initiated removal

MLS IETF 104 Prague

Context

- Strong interest from vendors
- External group management
- Requirement: roster is known to external party
- 2 proposals so far

Proposal 1: ExternalRemove

- External party can send HS messages to group
- HS messages are not encrypted under any group secret
- HS messages are signed by an external identity

Problems

- External identities are so far not linked to any group state
- Clients have agree on who to trust
- External identity management needs to be dynamic
- Worst-case: partition of a group

Proposal 2: RemoveRequest

- External party can send a request to remove to the group
- RemoveRequests are honoured by a member, who will issue a normal Remove
- Member can attach the RemoveRequest for context

UX/UI

Alice removed Bob -> Bob was removed [by some external party]

Proposal 2: RemoveRequest

Advantages

- No changes in MLS are needed
- Security properties should remain the same

Problems

- Pseudo-problem: the removal is not done in real-time, but MLS is asynchronous anyway

Version negotiation

MLS IETF 104 Prague

Addition to draft -04

- Mimic the ciphersuite approach
- Clients advertise their capabilities in UserInitKeys
- Group initiator decides on a version
- New members are informed in the Welcome handshake message

Addition to draft -04

```
uint8 ProtocolVersion;

struct {
      opaque user_init_key_id<0..255>;
      ProtocolVersion supported_versions<0..255>;
      CipherSuite cipher_suites<0..255>;
      HPKEPublicKey init_keys<1..2^16-1>;
      Credential credential;
      opaque signature<0..2^16-1>;
} UserInitKey;
```

```
struct {
  ProtocolVersion version;
  opaque group_id<0..255>;
  uint32 epoch;
  optional<Credential> roster<1..2^32-1>;
  optional<HPKEPublicKey> tree<1..2^32-1>;
  opaque transcript_hash<0..255>;
  opaque init_secret<0..255>;
} WelcomeInfo;
```

Open questions

- Should it be possible to upgrade existing groups to a newer version?
- If so, how?
- Should it happen on the application layer or within the protocol?
- What security properties would be conserved during an upgrade?