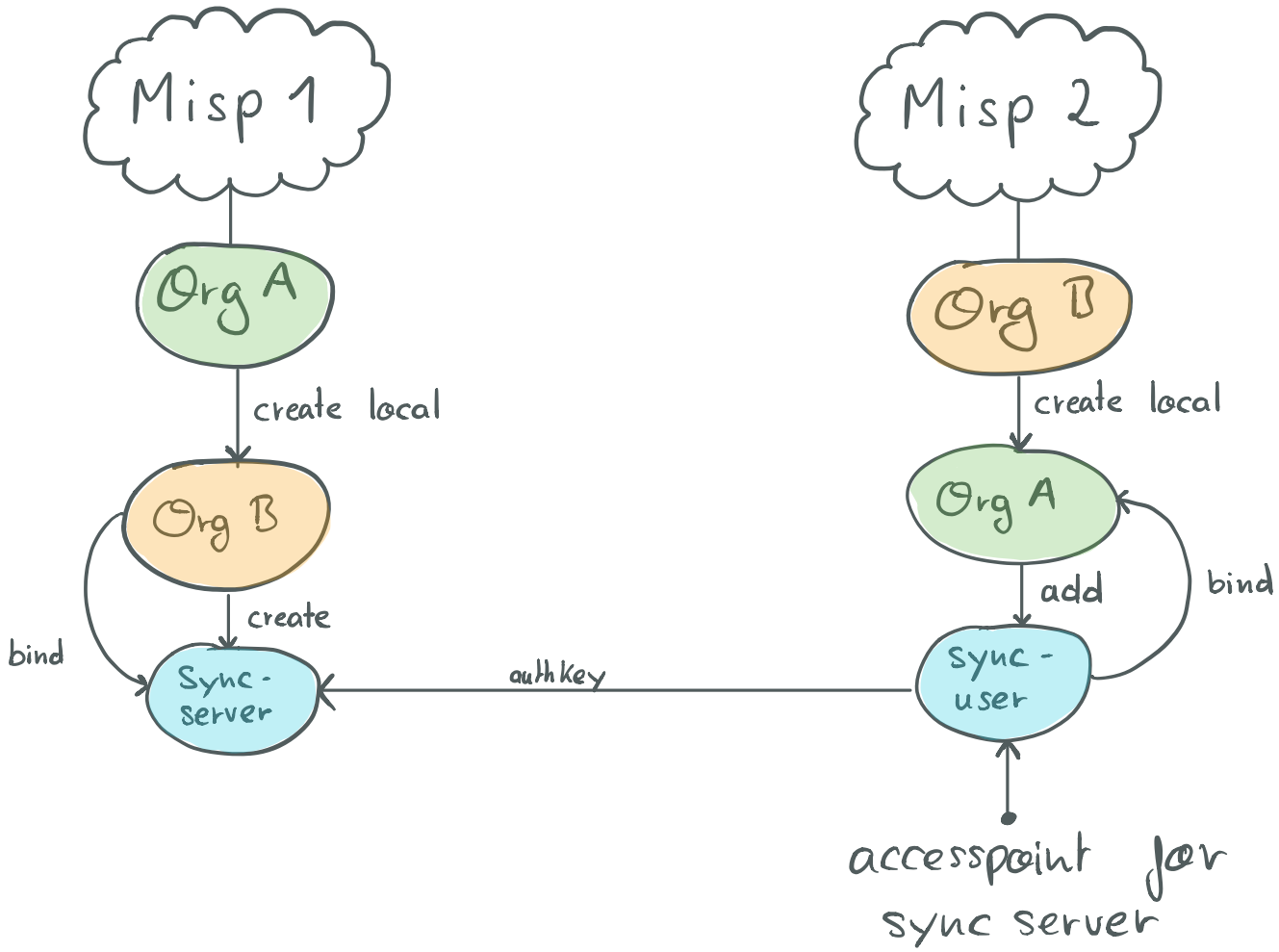
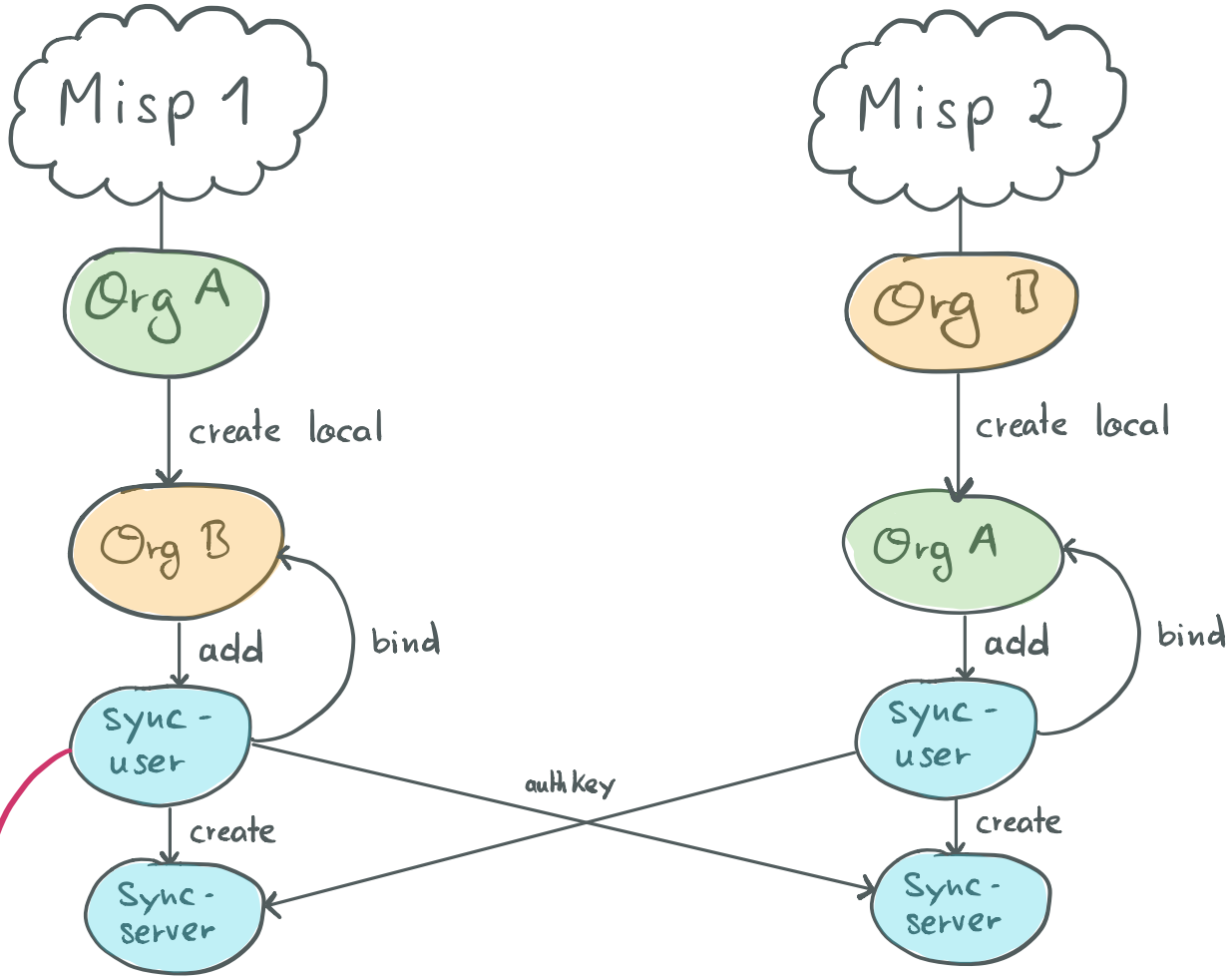
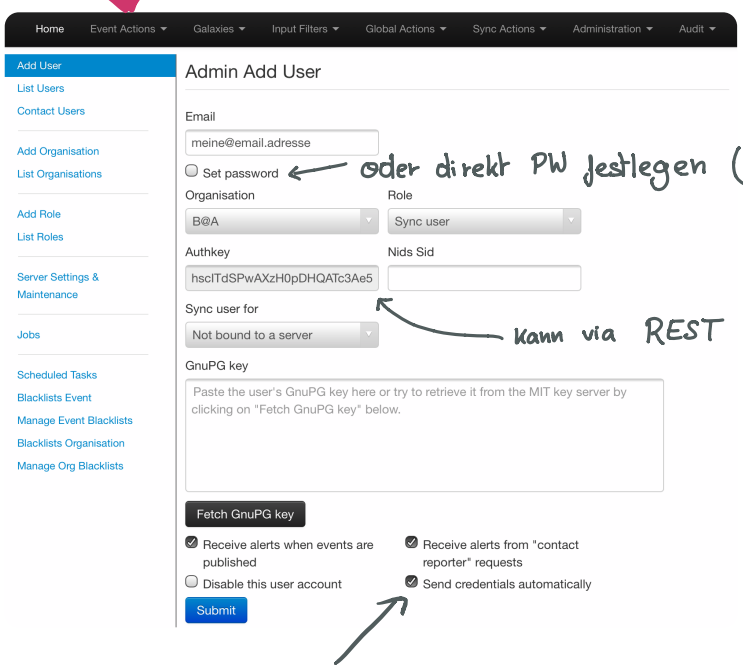
Szenario 1: Einseitiger share (1 → 2)



Szenario 2: bidirectional share





oder direkt PW festlegen (PW's müssen immer GENAU 12 Zeichen lang sein :/)

kann via REST selbst bestimmt werden

erst nach einloggen mit Zugangsdaten aus Email + anschließendem PW-Change ist authkey aktiv.

Szenario 3: Authkey wird "geklaut"

- Authkey ist erst nach PW-change aktiv
- Nur Syncuser - Authkey wird per QR übermittelt

Role

Id	5
Name	Sync user
Permission level	Manage and Publish Organisation Events
Delegate	Yes
Sync	Yes
Admin	No
Audit	No
Auth	Yes
Site Admin	No
Regexp Access	No
Tagger	No
Template	No
Sharing Group	Yes
Tag Editor	No
Sighting	Yes
Object Template	No

!

- Permissions können für jede Rolle angepasst werden
- Im schlimmsten Fall können Events ausgelesen werden, oder falsche Events geschrieben werden

MISP - Plugin (Modules)

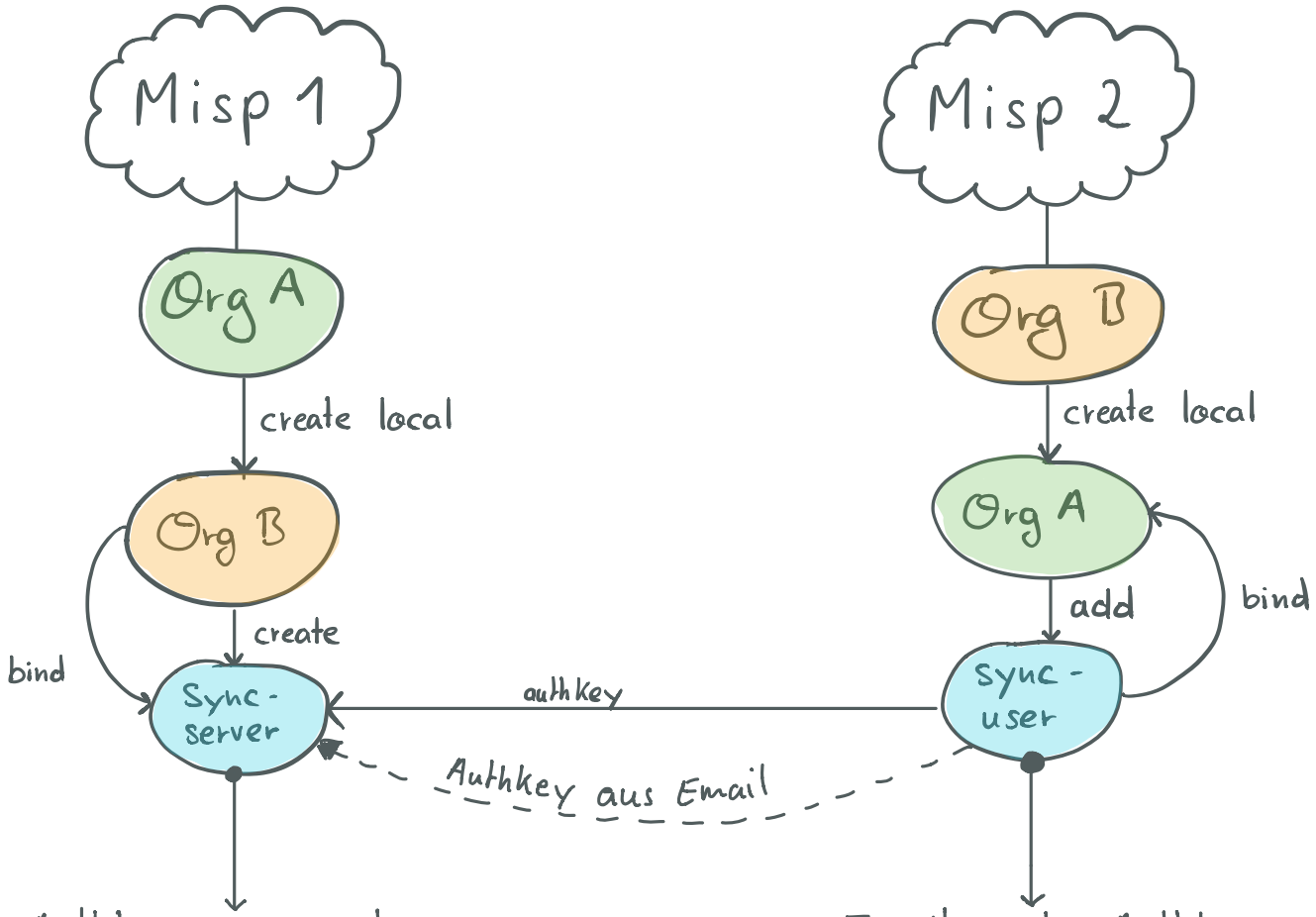
- Es gibt nur 4 Typen von Modulen
  1. expansion: z.B. domain zu IP od. andersrum
  2. hover: nähere Infos zu Attributen, ohne Event updaten zu müssen
  3. import: jegliche Art von Objekt um Event zu erweitern.
  4. export: Objekte, Events, Daten ...

- Für alles Andere:
  - Kern von MISP muss verändert werden
  - Tiefes Verständnis der MISP Architektur notwendig

  (Quelle: MISP Trainingsmaterialien)

Auth per Email (Authkey & Passwort in Email)

- nur möglich wenn MISP-Core verändert wird.
- Text der automatisch generierten Email (mit temporären Passwort) kann in MISP (statisch) verändert werden (MISP.newUserText)



- Authkey muss dann manuell in Syncserver eingetragen werden
- Email mit Authkey an syncuser Email

- oder "schwierig" zu implementierende Schnittstelle