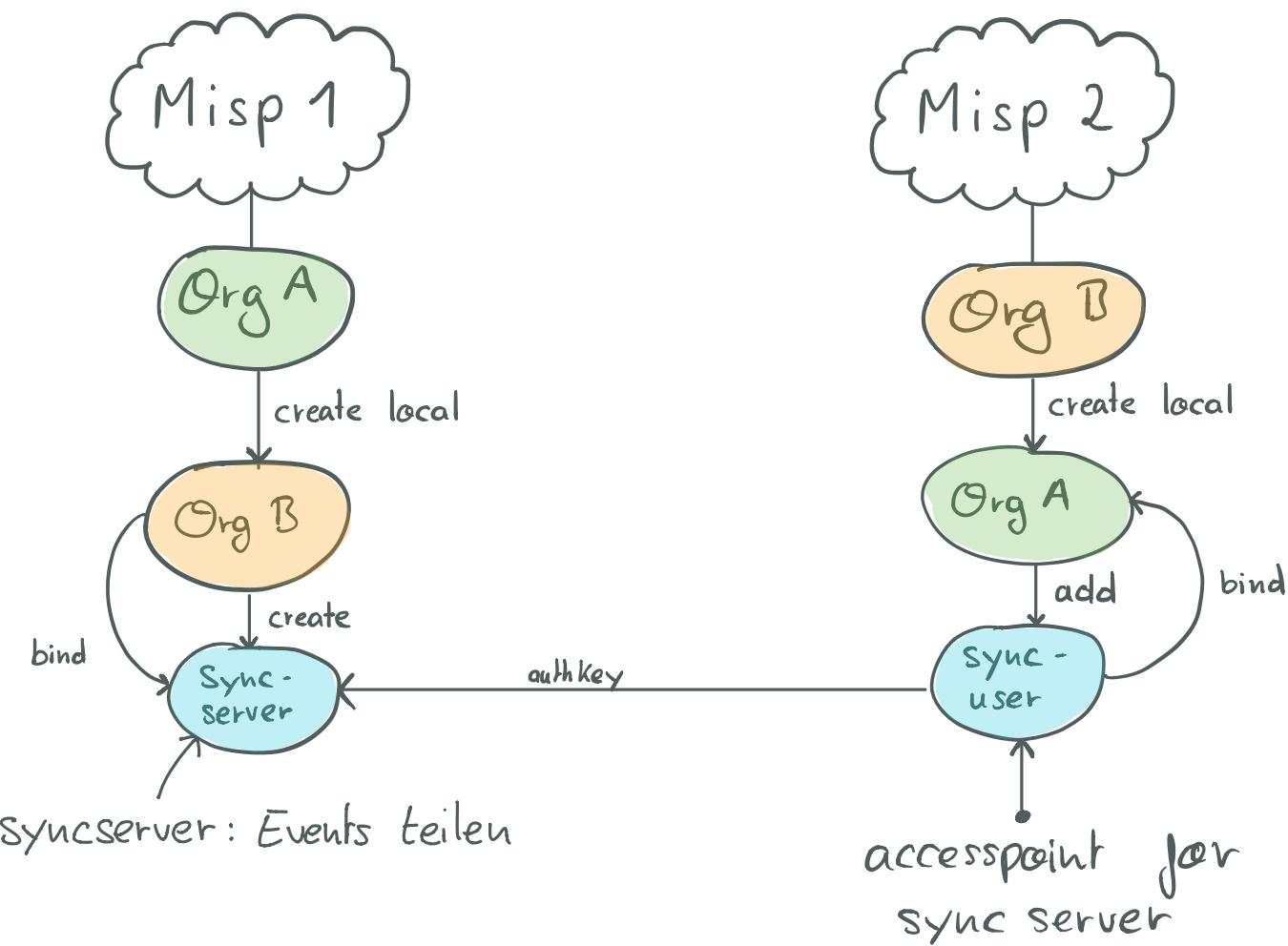
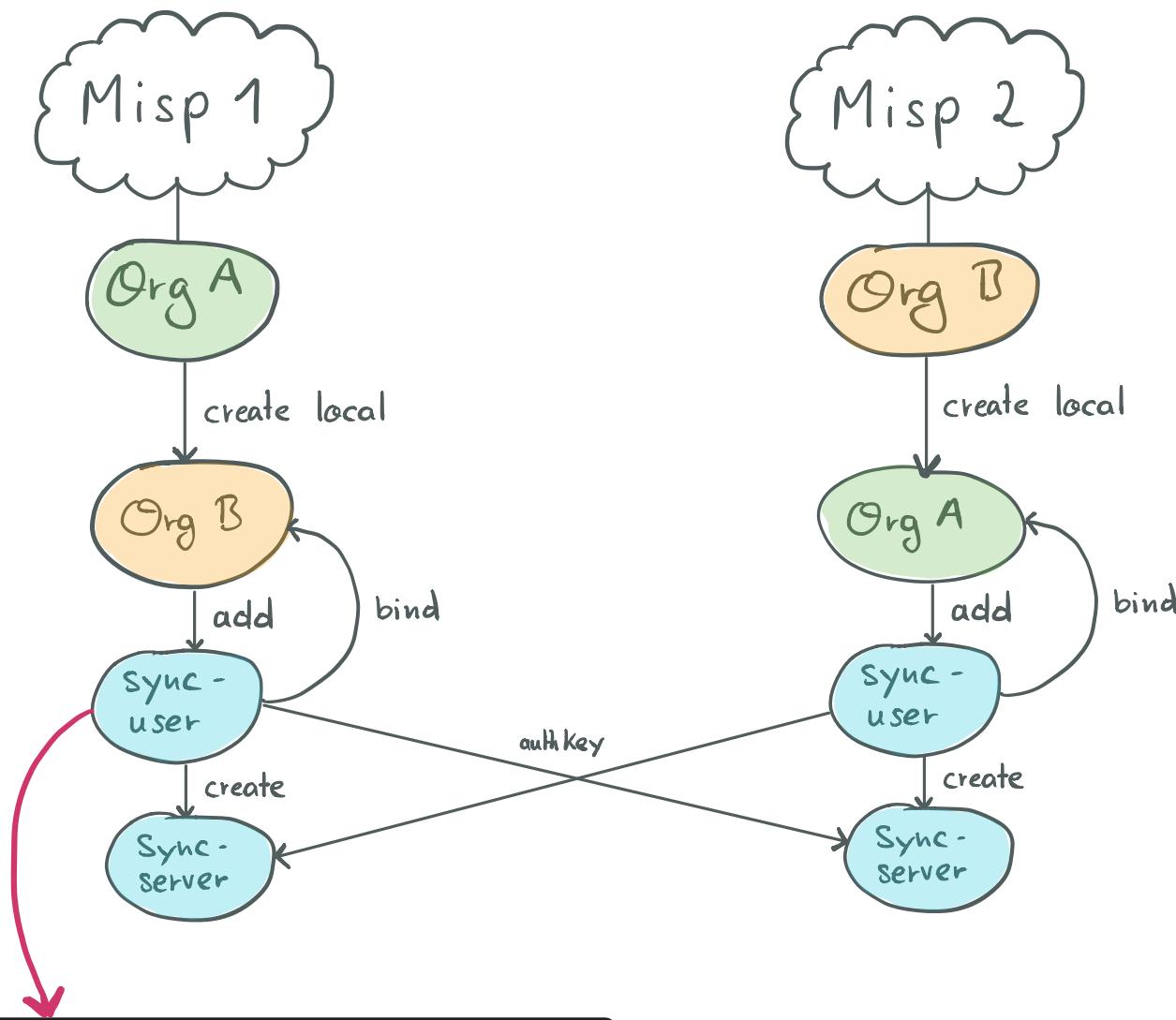


Szenario 1 : Share from MISP1 to MISP2



Szenario 2: bidirectional share



Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration Audit

Add User List Users Contact Users

Add Organisation List Organisations

Add Role List Roles

Server Settings & Maintenance

Jobs

Scheduled Tasks

Blacklists Event Manage Event Blacklists

Blacklists Organisation Manage Org Blacklists

Admin Add User

Email: meine@email.adresse

Set password oder direkt PW festlegen (PW's müssen immer GENAU 12 Zeichen lang sein)

Organisation: B@A Role: Sync user

Authkey: hscITdSPwAXzH0pDHQATc3Ae5

Sync user for: Not bound to a server Kann via REST selbst bestimmt werden

GnuPG key: Paste the user's GnuPG key here or try to retrieve it from the MIT key server by clicking on "Fetch GnuPG key" below.

Fetch GnuPG key

Receive alerts when events are published Receive alerts from "contact reporter" requests

Disable this user account Send credentials automatically

Submit

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

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 gelesen, geschrieben,

gelöscht und verändert werden

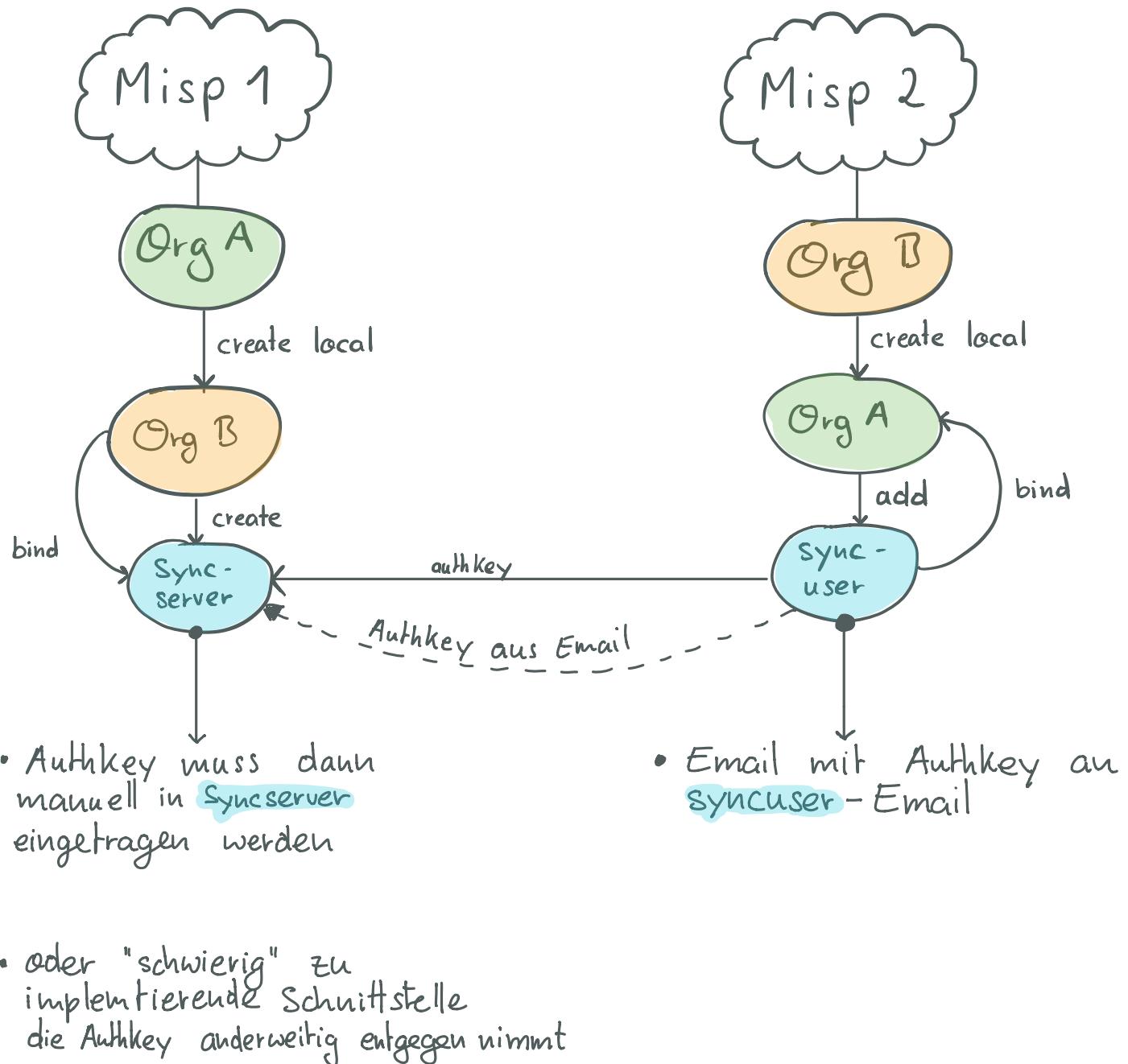
(Bezieht sich nur auf eigene Org)

MISP - Modules

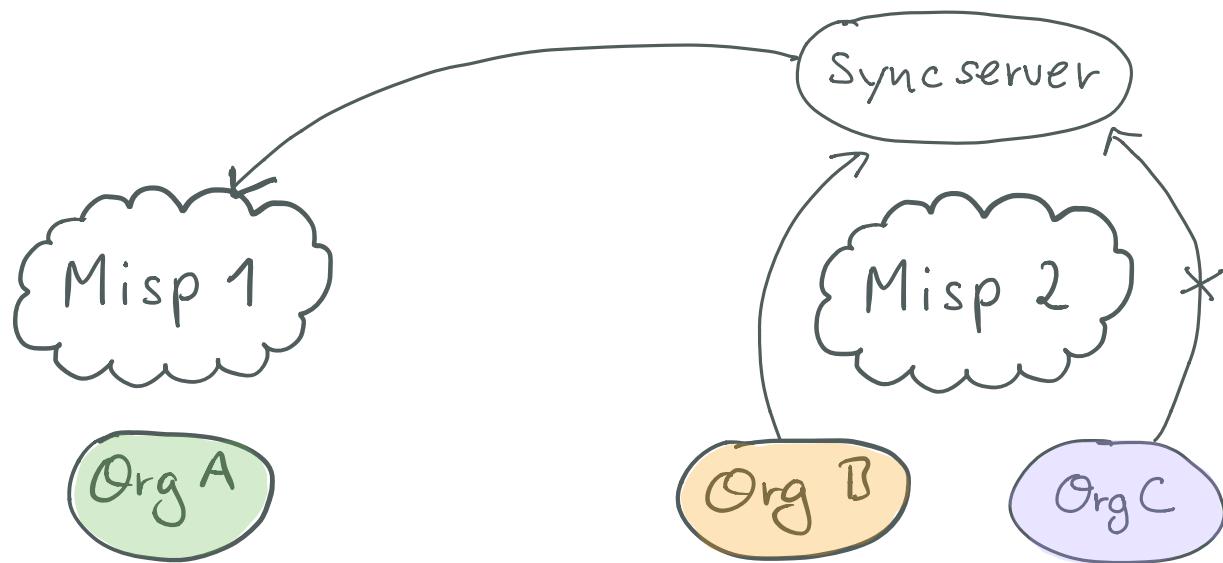
- Es gibt nur 4 Typen von Modulen
 1. expansion: z.B. domain zu IP od. andersrum
 2. hover: nähere Infos zu Attributen, ohne Event updateen zu müssen
 3. import: jegliche Art von Objekt um Event zu erweitern.
 4. export: Objekte, Events, Daten ...
- Für alles Andere:
 - Kern von MISP muss verändert werden
 - Tiefes Verständnis der MISP Architektur notwendig
(Quelle: MISP Trainingsmaterialien)

Auth per Email

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



Sharing Optionen



- Syncserver push rules:
Für alle lokalen Orgs kann ausgewählt werden ob sie ihre Events über einen bestimmten Sync-Server teilen.