



OpenCloud Groupware

A new JMAP Client



OpenCloud

Who am I ?

Pascal Bleser



Senior software developer

~15 years for Atos Worldline

~10 years for Open-Xchange

~1 year for OpenCloud

Pascal Bleser



- openSUSE contributor
- Twice on the openSUSE Board
- Organized FOSDEM for 10 years
(merci Raphaël <3)



OpenCloud

What is OpenCloud even?

OpenCloud



- Efficient file management and sharing
- Open Source (ASL2, AGPL3, GPL2)
- Great Web UI
- Desktop Clients (including for Linux)
- Mobile Apps

OpenCloud



- Backend in Go
- Frontend in Vue/TS
- Desktop in Qt/C++

OpenCloud



- Easy to install and use
- No database, everything in xattrs
- All-in-one or microservices for scaling
- Runs on Pi, runs on K8s

OpenCloud APIs



- WebDAV
- OCS (Open Collaboration Services)
- OCM (Open Cloud Mesh)
(draft-ietf-ocm-open-cloud-mesh-02)
- LibreGraph (MS Graph)



OpenTalk



- Video conferencing
- Open Source (EUPL)
- Backend in Rust
- Frontend in TypeScript

Mailbox



- Provider
- Email
- Drive
- Video conferencing
- Office

Adding Groupware

OpenCloud Groupware



- We are a JMAP Client
- Our own Go JMAP client library

OpenCloud Groupware



- Might split the client library off
- First need to stabilize
- Get some real-world usage

OpenCloud Groupware



JMAP because...

- Time frame
- Avoiding IMAP
- Developer friendly



JMAP because...

Stalwart

OpenCloud Groupware API



- Higher level APIs for our clients
- Still uses JMAP data model
- Avoid “reverse engineering”
- Inject additional data
- Caching, etc...

OpenCloud Groupware



Integrate information from our products

- OpenCloud Drive
- OpenCloud Groupware (+ Stalwart)
- OpenTalk



OpenCloud

Targets ?



Target Audiences

- Single user (“hosting” scenario)
- SMBs
- Education
- Education Networks, Government
- Private Sector
- ...

What they have in common



Groups of people, expected to be
able to share objects easily

Sharing easily



- Email account representatives
- Automatic shared address books
- Easily share mailboxes
- Automatic shared accounts and mailboxes

Sharing Automation

Sharing Automation



- Larger organizations: departments
- Different groups and perspectives
- Tenants
- Groups

Sharing Automation



- 1 Tenant = 1 Address Book
- 1 Group = 1 Address Book
- Whom I shared with
- Who shared with me
- Tenant or department quotas

Sharding

Sharding



- “Collaboration Units”
- ... are also “Sharding Units”

Sharding



- Hot caches and data locality
- Access data of users in the same unit

Sharding



Optimize performance

- Avoid cross-database queries
(e.g. Galera cluster)
- Avoid cross-datacenter queries
(e.g. Cassandra cluster)



OpenCloud

Yes please, Mauro.

JMAP Metadata (Proposal)



JMAP Metadata

draft-ietf-jmap-metadata-01

Attach deep key-value to JMAP Objects

JMAP Metadata



- Avoid additional storage services
- Avoids denormalization
- Additional data
without going through RFCs

User Preferences Storage (Proposal)

User Preferences Storage & API



A simple protocol
to easily manage
account settings

User Preferences Storage & API



Passwords,
App Passwords,
MFA settings

Basic email
forwarding

Blocking email
addresses

A simple protocol
to easily manage
account settings

Locale
preferences

Timezone
configuration

Encryption-at-rest
settings

JMAP Mailbox Sharing (Proposal)

JMAP Mailbox Sharing

draft-ietf-jmap-mail-sharing-00



- Same RFC9670 JMAP sharing model, but for Mailbox objects
- Useful for obvious reasons, especially in “enterprise” scenarios



OpenCloud

Integration Challenges

Authentication

Authentication



Larger customers require
custom authentication

Authentication



They already have

- IDM,
- provisioning,
- administration

Authentication



OIDC is great, but not enough,
e.g. group membership
(LDAP “member”)

Authentication



LDAP is still around

- Fast
- Very well supported, great client SDKs
- Hierarchies
- OpenLDAP: replication, indexes

Authentication



Master Authentication

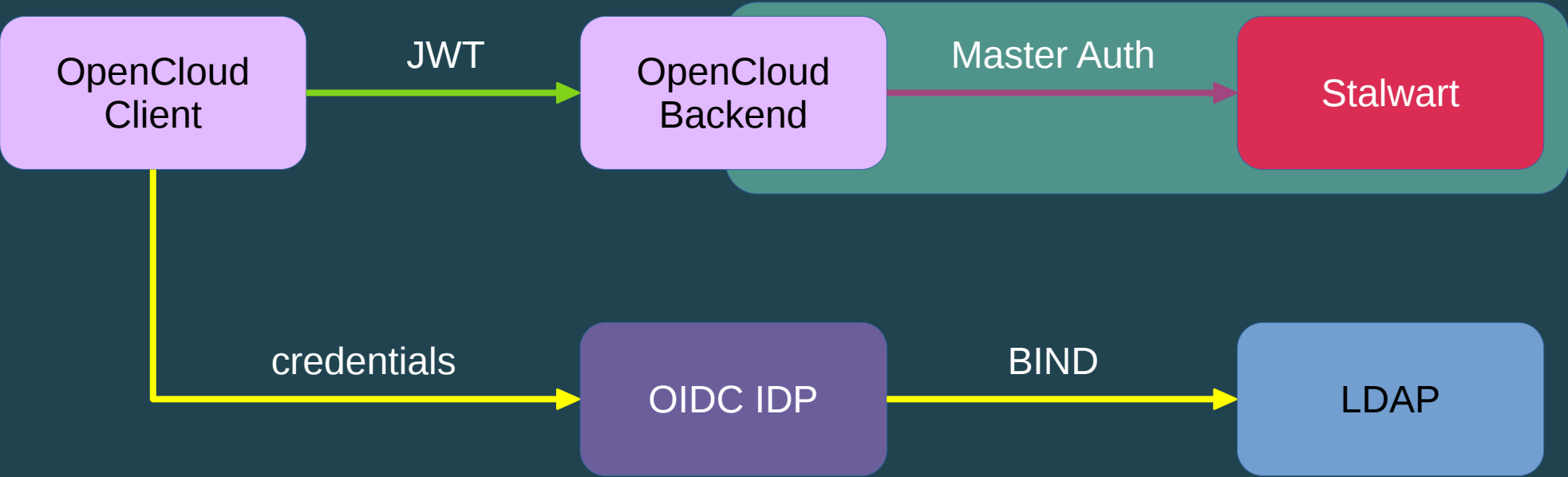
- Shared secret (password)
- Not ideal
- Often necessary
- Inside a “trusted zone”
- IP address ranges, additional shared secret

Authentication

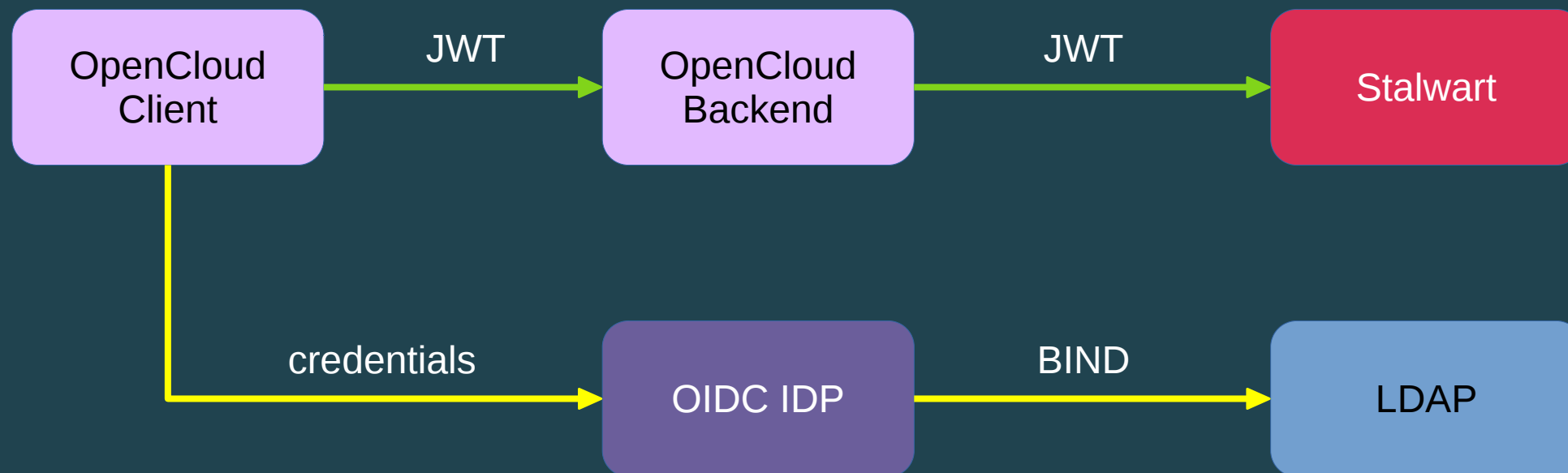


Better: mTLS or JWT

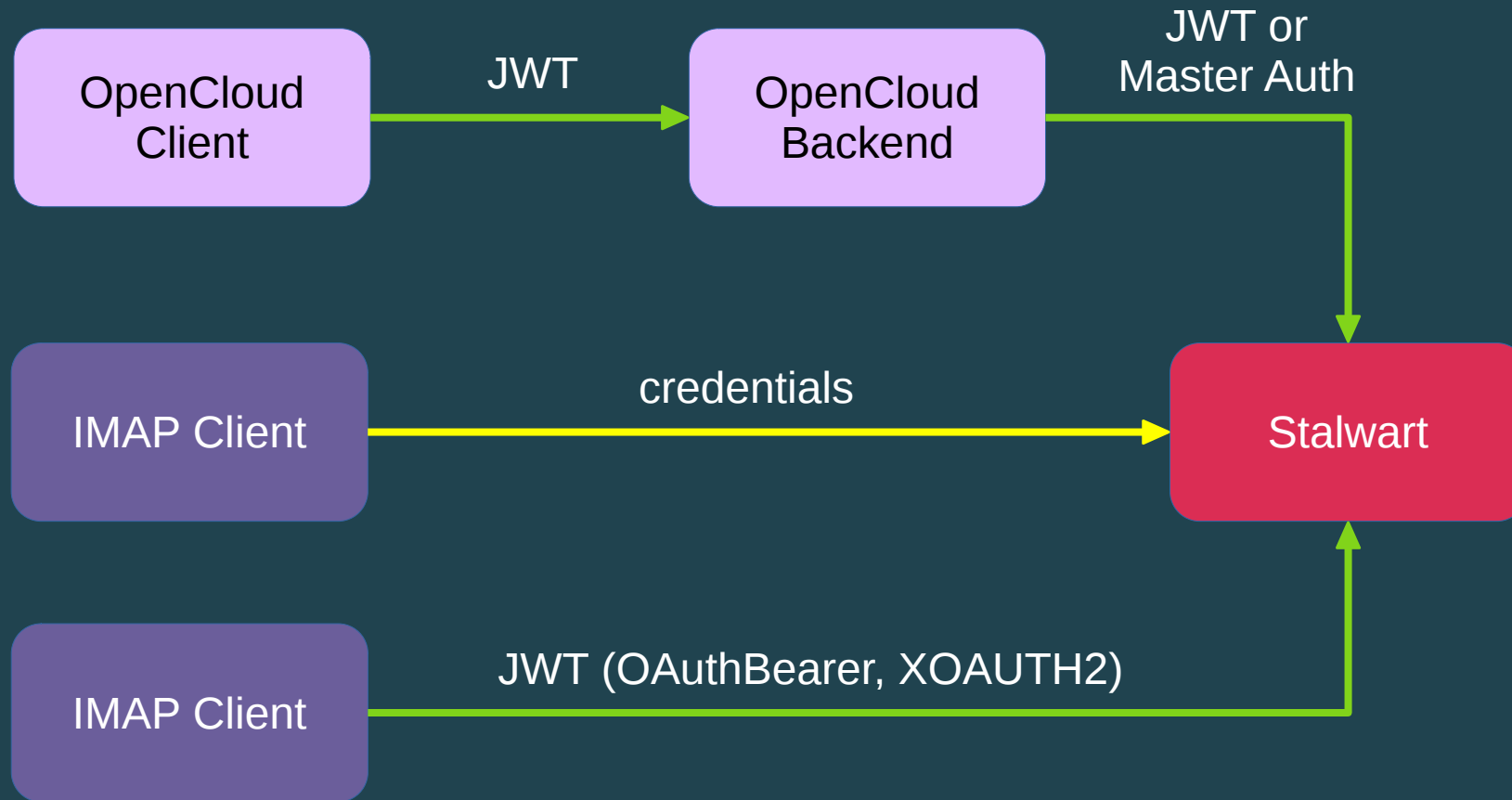
Master Authentication



JWT Forwarding



Different Authentication Channels



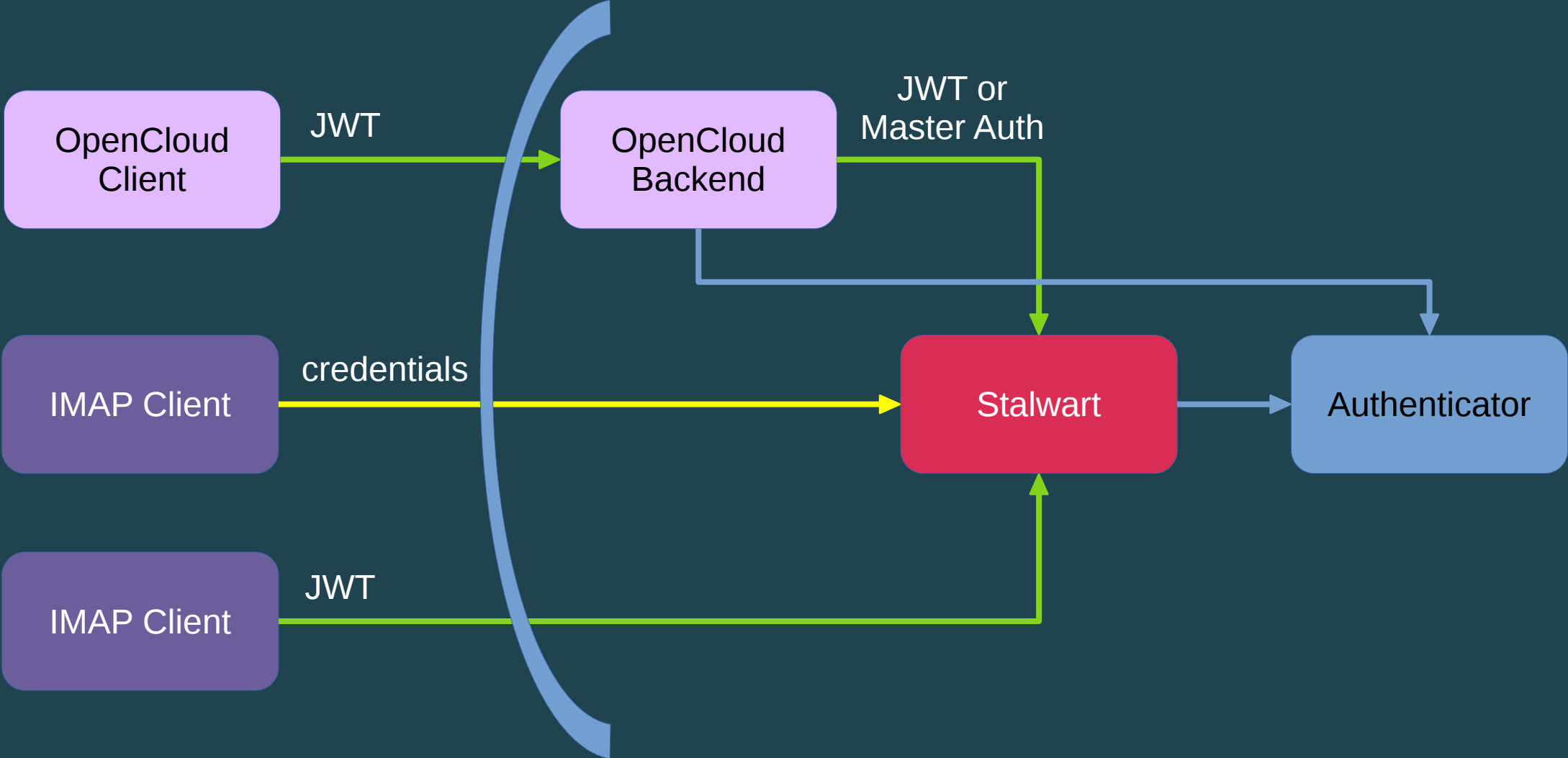
Authentication



Need an Authentication API ?

- Basic, JWT, ...
- Track brute force attempts
- Implement customizations once

Multichannel Authentication Monitoring (for brute force detection)



Provisioning

Provisioning



Provisioning users into multiple systems

- No one wants to do that
- De-provisioning, too
- Error-prone, retries, keeping track/state
- Auto-provisioning ability helps

Provisioning



Commercial customers want upselling

- Intertwined with their admin solution
- Customers, contracts, features, quotas, billing, ...

Provisioning



Keep track of user state in a workflow

- Tryouts, offers
- Missed a payment
- Soft deletion
- Keep data around for renewal

Q & A



Thank you !

