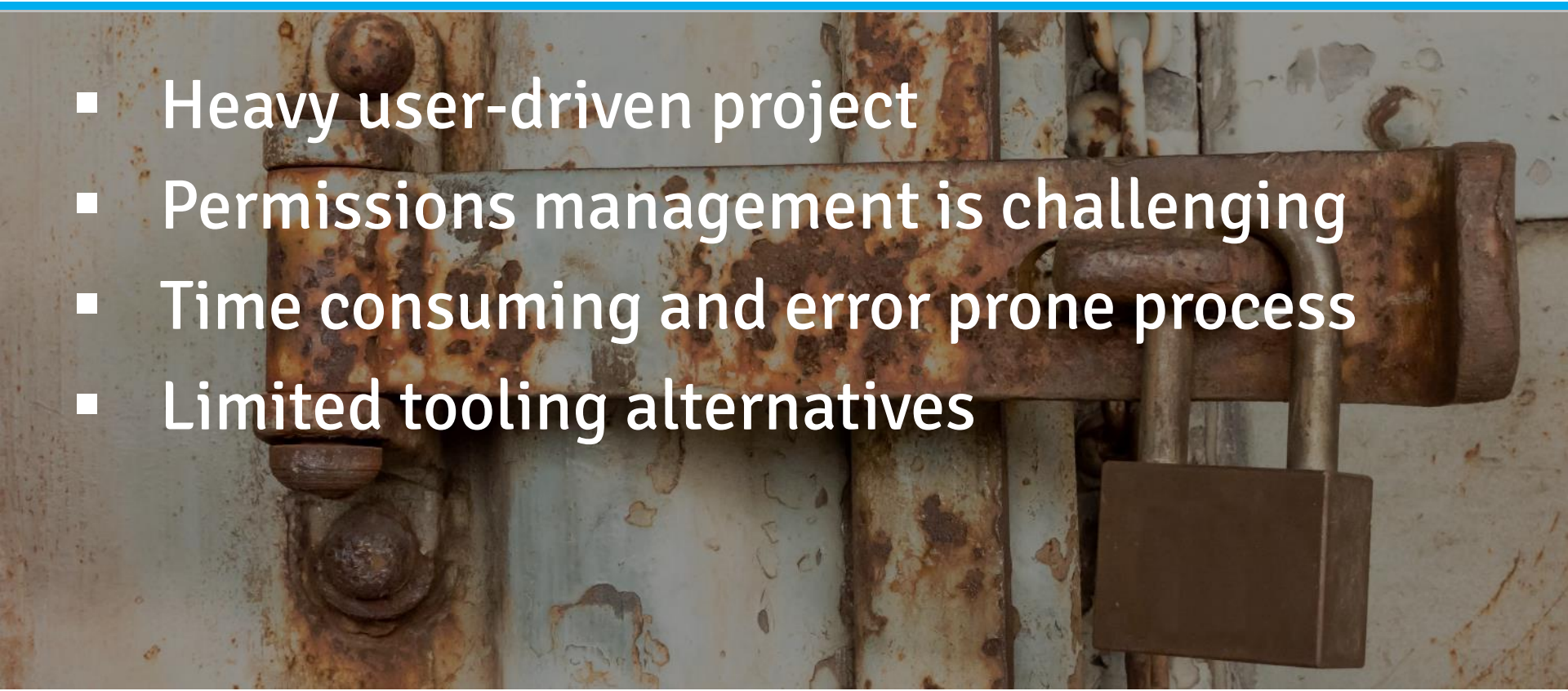
APACHE SLING & FRIENDS TECH MEETUP
BERLIN, 26-28 SEPTEMBER 2016

AEM Permission Management

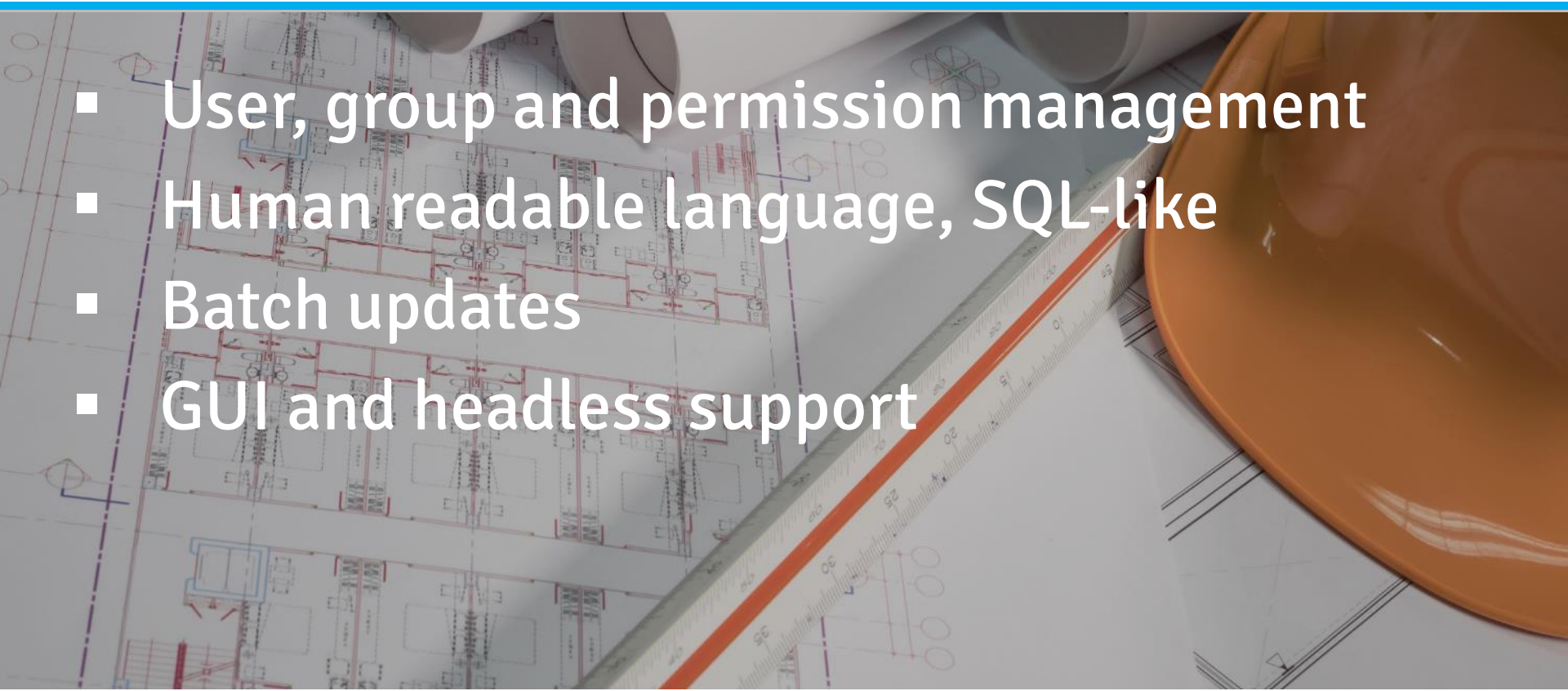
Mateusz Chromiński, Cognifide

Background



- Heavy user-driven project
- Permissions management is challenging
- Time consuming and error prone process
- Limited tooling alternatives

Requirements



- User, group and permission management
- Human readable language, SQL-like
- Batch updates
- GUI and headless support

Introducing...

AEM
Permission
Management

https://github.com/Cognifide/APM

Cognifide Labs

- Continous contribution to open-source
- 15+ active projects
- 40+ contributors
- 4 years of OS presence
- http://cognifide.github.io

Apply!

- Multi-tenant environment (50+ affiliates)
- Two levels of access:
  - author – able to manage **repetitive content**
  - superauthor – able to **configure** the site

multitenancy-create.cqsm

- Create users & groups

```
CREATE USER adaptTo-superuser secret
CREATE USER adaptTo-user secret
CREATE GROUP adaptTo-superusers
CREATE GROUP adaptTo-users

FOR USER adaptTo-user
    ADD TO GROUP adaptTo-users

FOR USER adaptTo-superuser
    ADD TO GROUP adaptTo-superusers
```

multitenancy-superusers.cqsm

- Add access to a single site only

```
DEFINE site adaptTo

FOR GROUP adaptTo-superusers
    ADD TO GROUP contributor
    DENY /content /* [ALL]
    ALLOW /content/${site} [ALL]
```

Create functional blocks and execute them from outside with parameters defined

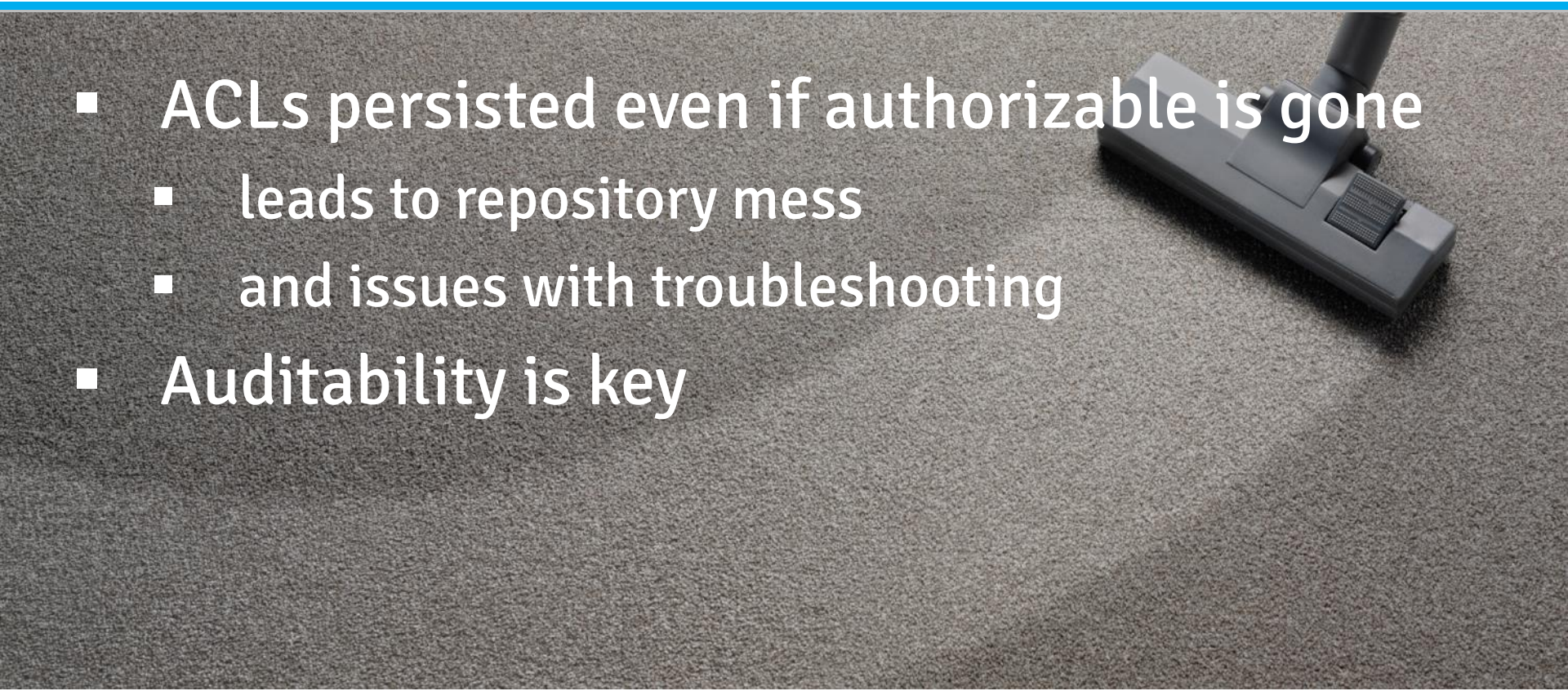
multitenancy-user.cqsm

- Restrict access within site

```
FOR GROUP adaptTo-users
    ADD TO GROUP adaptTo-superusers
    DENY /content/adaptTo/en /* [READ]

    # to see page metadata i.e. title and thumbnail
    ALLOW /content/adaptTo/en/jcr:content [READ]
    # to interact with whole subtree
    ALLOW /content/adaptTo/en/home [ALL]
    # to see only given page, without any subpages
    ALLOW /content/adaptTo/en/config STRICT [READ]
    ALLOW /content/adaptTo/en/config/jcr:content [READ]
```

Clean!



- ACLs persisted even if authorizable is gone
  - leads to repository mess
  - and issues with troubleshooting
- Auditability is key

recreate-group.cqsm

- Remove and create again

```
REMOVE GROUP adaptTo-superusers
CREATE GROUP adaptTo-superusers
FOR GROUP adaptTo-superusers
    ADD TO GROUP contributor
    INCLUDE adaptTo-superuser
    INCLUDE adaptTo-users
```

Permission are assigned already!

create-safe.cqsm

- Do not fail if authorizable exist already

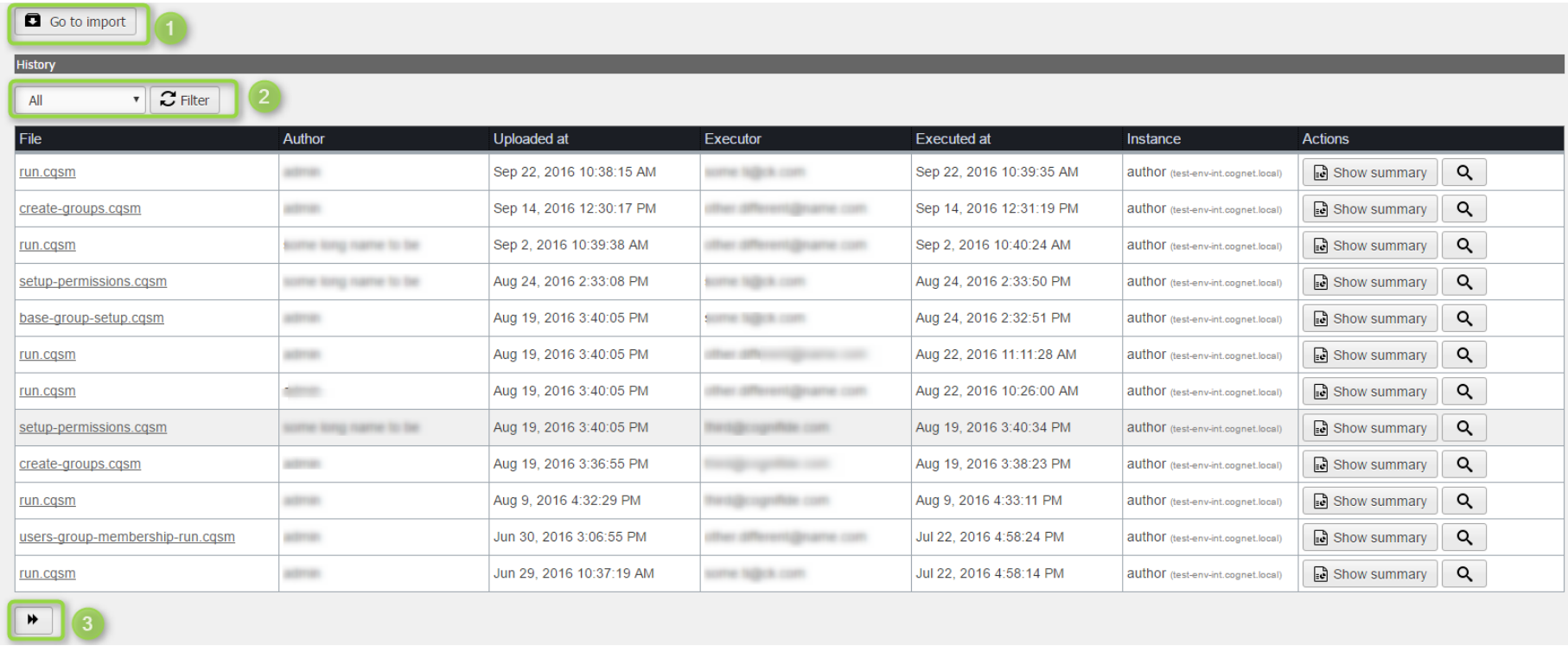
```
CREATE GROUP adaptTo-superusers IF NOT EXISTS
CREATE GROUP adaptTo-users IF NOT EXISTS
```

- Purge all existing permissions

```
FOR GROUP adaptTo-superusers
    PURGE /
FOR GROUP adaptTo-users
    PURGE /
```

Make the scripts idempotent

Full execution trackrecord



File	Author	Uploaded at	Executor	Executed at	Instance	Actions
run.cqsm	admin	Sep 22, 2016 10:38:15 AM	some.t@ck.com	Sep 22, 2016 10:39:35 AM	author (test-env-int.cognet.local)	Show summary
create-groups.cqsm	admin	Sep 14, 2016 12:30:17 PM	other.different@name.com	Sep 14, 2016 12:31:19 PM	author (test-env-int.cognet.local)	Show summary
run.cqsm	some long name to be	Sep 2, 2016 10:39:38 AM	other.different@name.com	Sep 2, 2016 10:40:24 AM	author (test-env-int.cognet.local)	Show summary
setup-permissions.cqsm	some long name to be	Aug 24, 2016 2:33:08 PM	some.t@ck.com	Aug 24, 2016 2:33:50 PM	author (test-env-int.cognet.local)	Show summary
base-group-setup.cqsm	admin	Aug 19, 2016 3:40:05 PM	some.t@ck.com	Aug 24, 2016 2:32:51 PM	author (test-env-int.cognet.local)	Show summary
run.cqsm	admin	Aug 19, 2016 3:40:05 PM	other.different@name.com	Aug 22, 2016 11:11:28 AM	author (test-env-int.cognet.local)	Show summary
run.cqsm	admin	Aug 19, 2016 3:40:05 PM	other.different@name.com	Aug 22, 2016 10:26:00 AM	author (test-env-int.cognet.local)	Show summary
setup-permissions.cqsm	some long name to be	Aug 19, 2016 3:40:05 PM	friend@cognifide.com	Aug 19, 2016 3:40:34 PM	author (test-env-int.cognet.local)	Show summary
create-groups.cqsm	admin	Aug 19, 2016 3:36:55 PM	friend@cognifide.com	Aug 19, 2016 3:38:23 PM	author (test-env-int.cognet.local)	Show summary
run.cqsm	admin	Aug 9, 2016 4:32:29 PM	friend@cognifide.com	Aug 9, 2016 4:33:11 PM	author (test-env-int.cognet.local)	Show summary
users-group-membership-run.cqsm	admin	Jun 30, 2016 3:06:55 PM	other.different@name.com	Jul 22, 2016 4:58:24 PM	author (test-env-int.cognet.local)	Show summary
run.cqsm	admin	Jun 29, 2016 10:37:19 AM	some.t@ck.com	Jul 22, 2016 4:58:14 PM	author (test-env-int.cognet.local)	Show summary

Extend!

- Not a definite solution - an extensible framework
- Create new actions with ease

CustomActionMapper.java

- Implement new mapper

```
@Mapper
public class CustomActionMapper extends BasicActionMapper {

    @Mapping(reference = „Full description for autogenerated docs”,
             args = {userId, paths},
             value = „CUSTOM ACTION” + SPACE + STRING + SPACE + LIST)
    public Action resolveAction(String userId, List<String> paths) {
             ...
```

regexp

CustomAction.java

- Implement custom action

```
public class CustomActionMapper implements Action {

    public boolean isGeneric() { return false; }

    public ActionResult simulate(Context context) { ... }

    public ActionResult execute(Context context) { ... }
```

Whether in context or not

pom.xml

- Describe the mapper

```
<plugin>
    <groupId>org.apache.felix</groupId>
    <artifactId>maven-bundle-plugin</artifactId>
    ...
    <configuration>
            <instructions>
                    <CQ-Security-Management-Actions>
                            package.with.custom.actions
                    </CQ-Security-Management-Actions>
```

adaptTo()

APACHE SLING & FRIENDS TECH MEETUP

BERLIN, 26-28 SEPTEMBER 2016

Thank you

mchrominski | mateusz.chrominski@cognifide.com