RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Signed TAL

Tim Bruijnzeels | 16 July 2017 | IETF 99

Problem Statement

- TALs distributed / configured with deployed RPs

```
rsync://rpki.example.org/rpki/hedgehog/root.cer
rsync://rpki.example.org/rpki/warthog/root.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAovWQL2lh6knDx
GUG5hbtCXvvh4AOzjhDkSHlj22gn/1oiM9IeDATIwP44vhQ6L/xvuk7W6
Kfa5ygmqQ+xOZOwTWPcrUbqaQyPNxokuivzyvqVZVDecOEqs78q58mSp9
nbtxmLRW7B67SJCBSzfa5XpVyXYEgYAjkk3fpmefU+AcxtxvvHB5OVPIa
BfPcs80ICMgHQX+fphvute9XLxjfJKJWkhZqZ0v7pZm2uhkcPx1PMGcrG
ee0WSDC3fr3erLueagpiLsFjwwpX6F+Ms8vqz45H+DKmYKvPSstZjCCq9
aJ0qANT9OtnfSDOS+aLRPjZryCNyvvBHxZXqj5YCGKtwIDAQAB
```

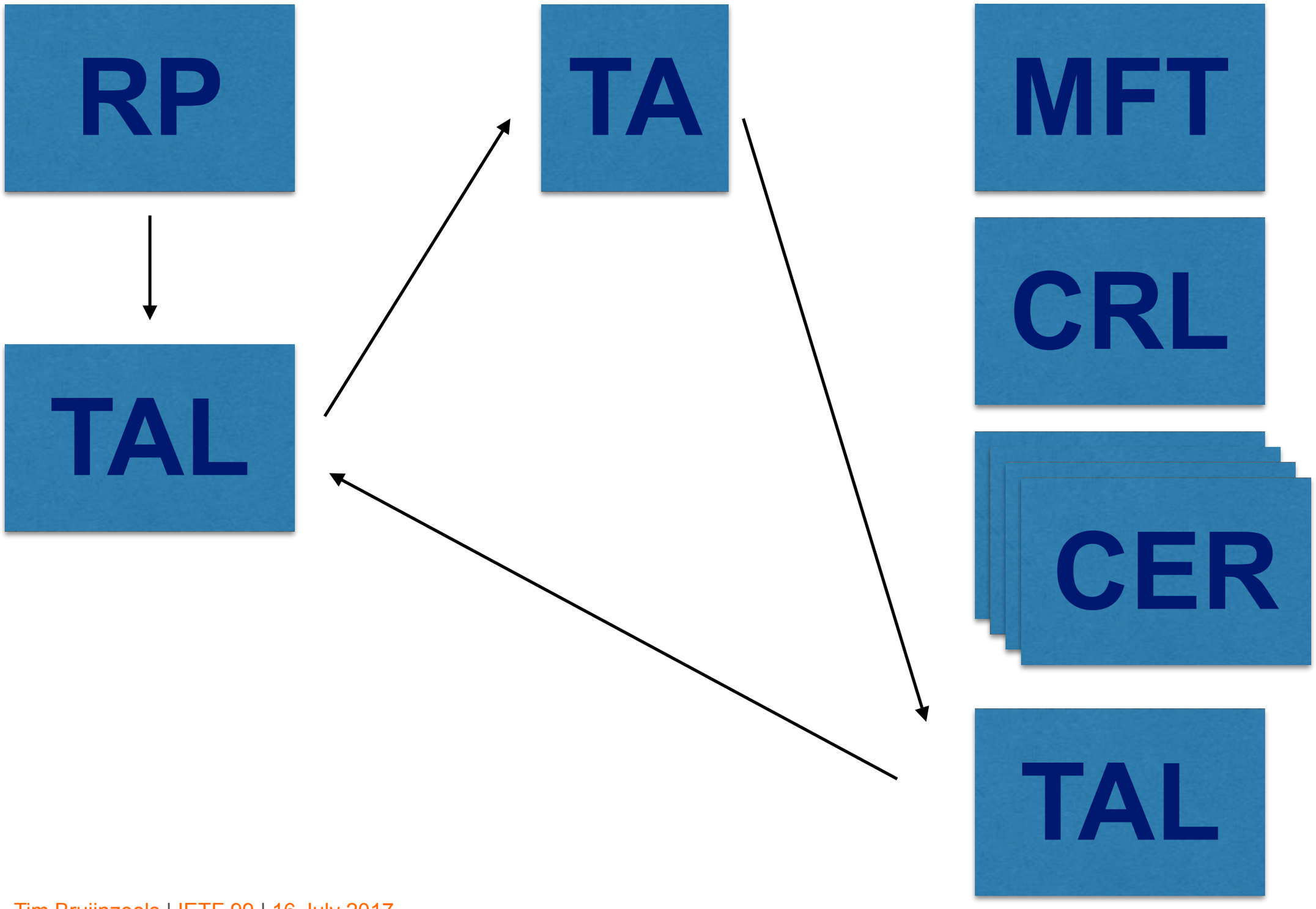
- What if I want to use https? Or additional URIs?
- What if I want to do a planned roll of the key?
  (HSM vendor lock-in)

Going Forward - disclaimer

- Made draft to have a structured discussion about one possible way forward - not married to it, no pregnancies

- Not against solutions that included unplanned key rolls, but..
  - It's a problem I fortunately do not have today
  - I don't have a great idea about how to solve it
  - I believe a solution to this should not delay a solution to the practical use cases of changing URIs and a planned key roll

Signed TAL



Key Roll

- Prepare new
  - Publish ALL object of old under new (except TAL)
  - Publish TA certificate
  - Publish TAL under old TA

- Staging (24 hours ?): publish old AND new

- Keep old?
  - Just a long-lived CRL, MFT and TAL pointing at new, so that RPs can find new
  - Destroy old key

New URIs

- Add URI
  - MUST publish certificate before publishing TAL

- Remove URI
  - SHOULD still publish certificate for 24 hours (?)

- Withdraw TAL
  - SHOULD withdraw TAL after 24 hours (?)

Summary and going forward

- Adopt as WG item and discuss further?

- Again, not married to the proposal - it's intended as a start of conversation, but our use case is real

Questions