RIPE NCC

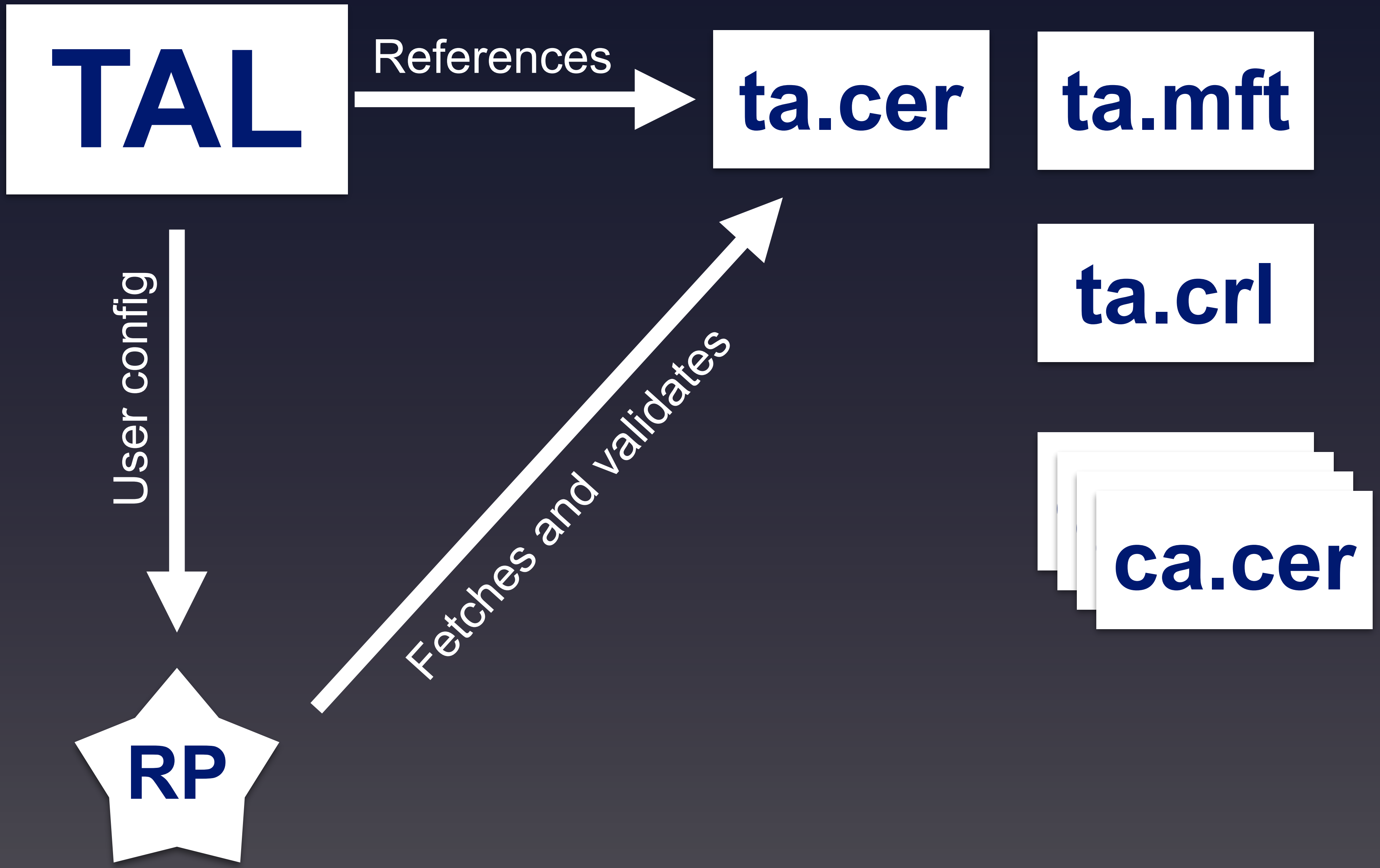
RIPE NETWORK COORDINATION CENTRE

RPKI signed object for TAL

draft-ietf-sidrops-signed-tal

Tim Bruijnzeels | IETF101

Current RPKI structure

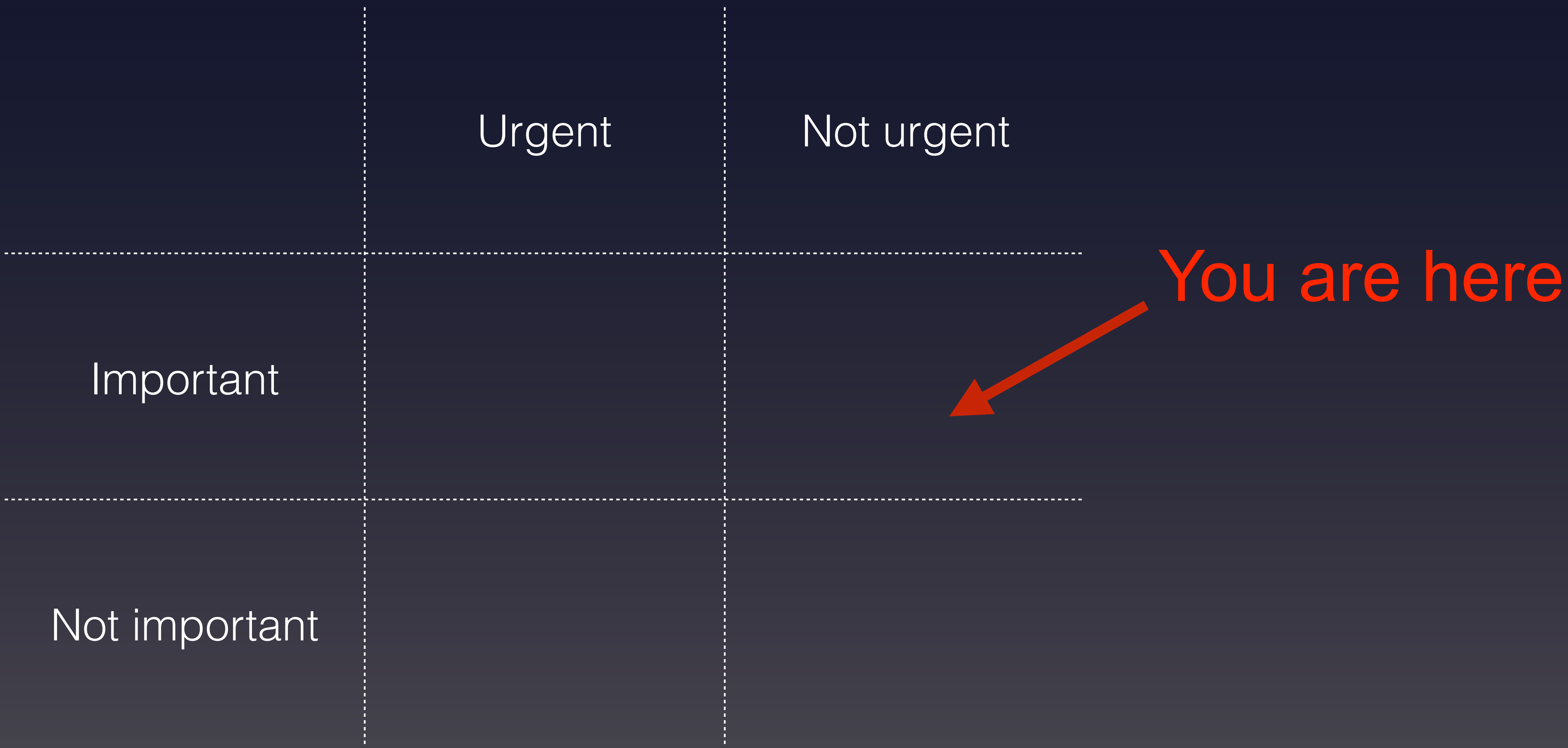


What’s the issue here?

- New URI?
- New key?

- New TALs need to be installed by hand
  - Defaults okay, but modify TAs on update questionable
  - Hard to reach deploy base

Why talk about this now?



	Urgent	Not urgent
Important		
Not important		

You are here

This draft

- Covered
  - Planned rolls, e.g. HSM vendor lock-in
  - Communicate new publication URIs, e.g. HTTPS
- Not (yet) covered
  - Unplanned rolls, e.g. key loss
- Open to suggestions…
  - NOT looking for a quick hack, don’t claim to know it all..

Planned roll

1. TA sets up new key and publishes all objects

2. TA publishes TAL pointing to cert for new key
   - RP MUST use new key immediately
   - TA MUST manage both keys for at least 24 hours?!

3. TA retires old key
   - SHOULD keep signed TAL under old key for discovery

Add Publication Location

1. TA publishes TA.cer in new location

2. TA publishes TAL including new location
   - RP MUST use new TAL immediately
     (MAY therefore use new location)

Remove Publication Location

1. TA publishes TAL excluding location
    - RP MUST use new TAL immediately
      (MUST no longer use old location)
    - TA SHOULD continue to publish old location for 24 hours?
      (give RPs time to discover, typically revalidate sooner)

Issues with draft

- Double encoding (thanks Tom)

- Magic staging times
  - Old and new key, retire publication point.
  - Do we need them? Which values?

- Everything is immediate, is this okay?
  - Seems simplest to me..
  - RPs can do diff

Cover unplanned rolls?

- HSMs can be used to protect keys
  - Extremely unlikely that keys are stolen
  - Key can be lost
  - Access to the keys, N out of M card set, can be lost

➡ If to be covered, we should have one mechanism for both planned and unplanned.

Possible key roll mechanism

1. TA always publishes TA Object
   - Defines current key and location(s)
   - Defines future use key and location(s)
   - Defines old keys if any, see below
   - Will need a structured object

2. RP verifies new key TA*
   - No action if TA* object matches TA object
   - If TA* revokes TA, use new key NOW

Need your feedback

- Need for flagging future changes?
  - My RP: prefer to find when ready, rather than track
- Magic times?
  - My RP: no need to keep old key operational
  - My RP: old location - 24 hours is a bit aggressive
- Cover unplanned as well?
  - Use same mechanism for planned an unplanned
  - Will need a TA object with more details than a simple TAL

Questions ?