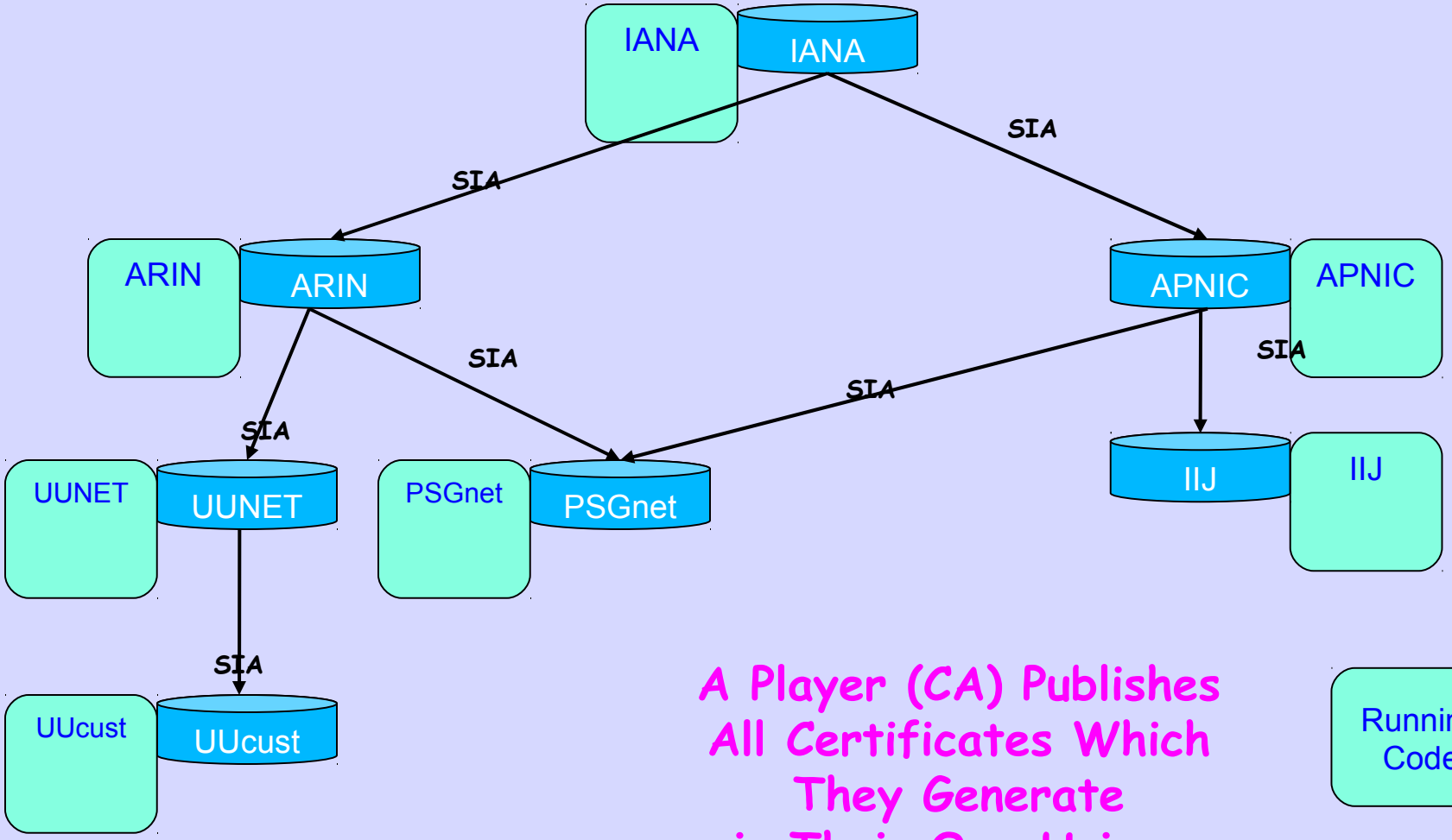
draft-weiler-sidr-publication

Samuel Weiler

IETF78, Maastricht
28 July 2010

Distributed RPKI DataBase



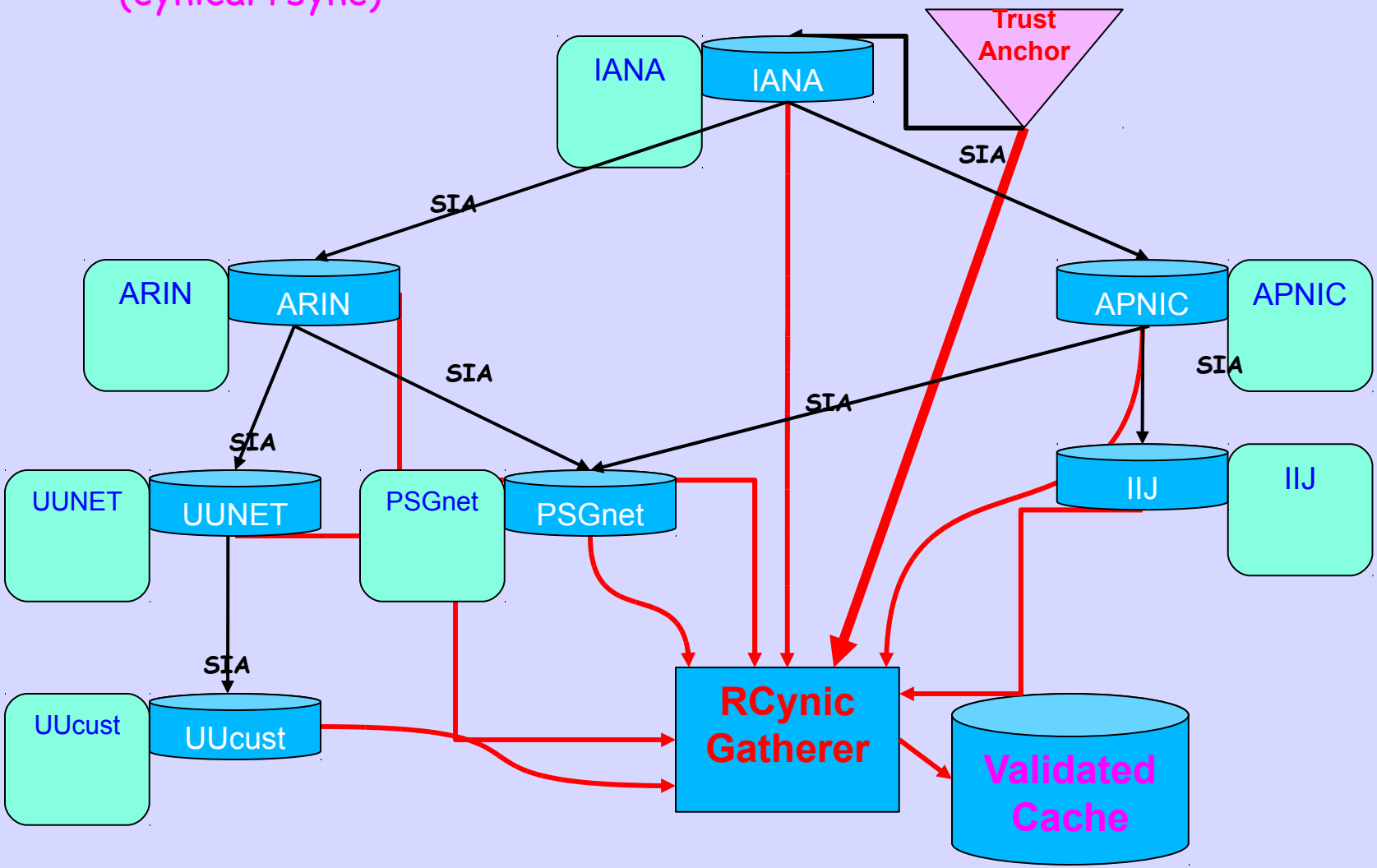
A Player (CA) Publishes All Certificates Which They Generate in Their Own Unique Publication Point

Running Code

Repository

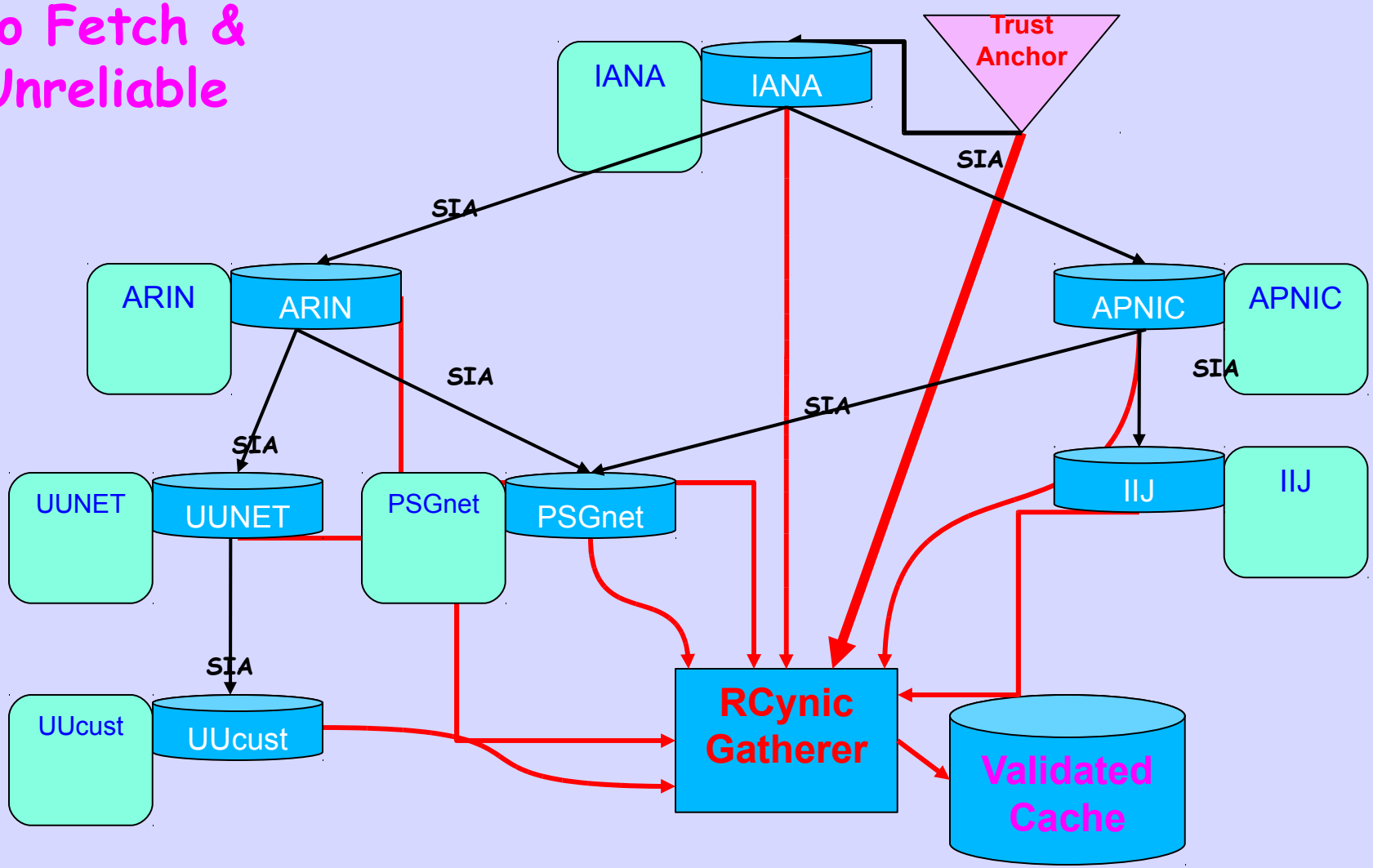
RCynic Cache Gatherer

(cynical rsync)

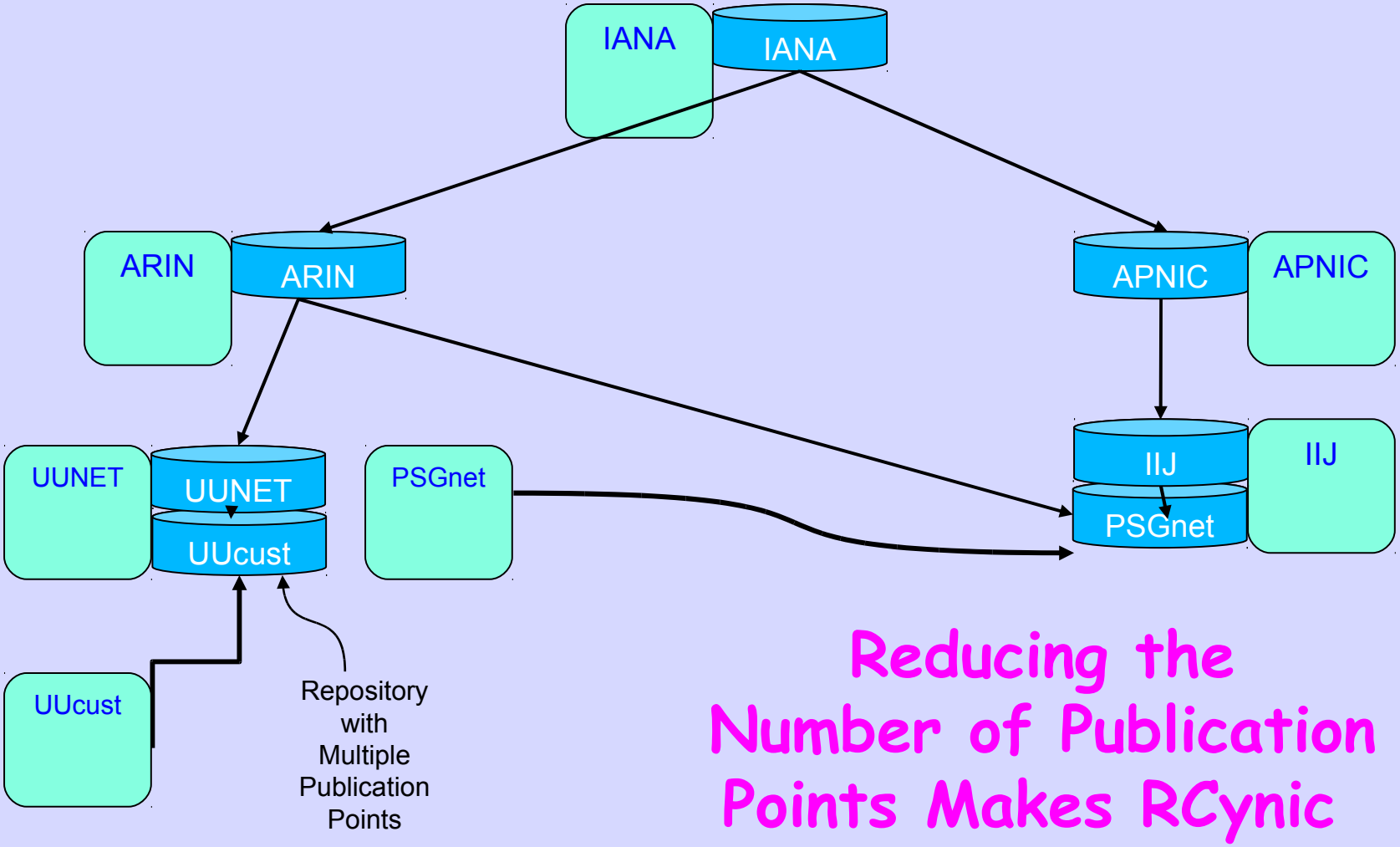


Reliability Issue

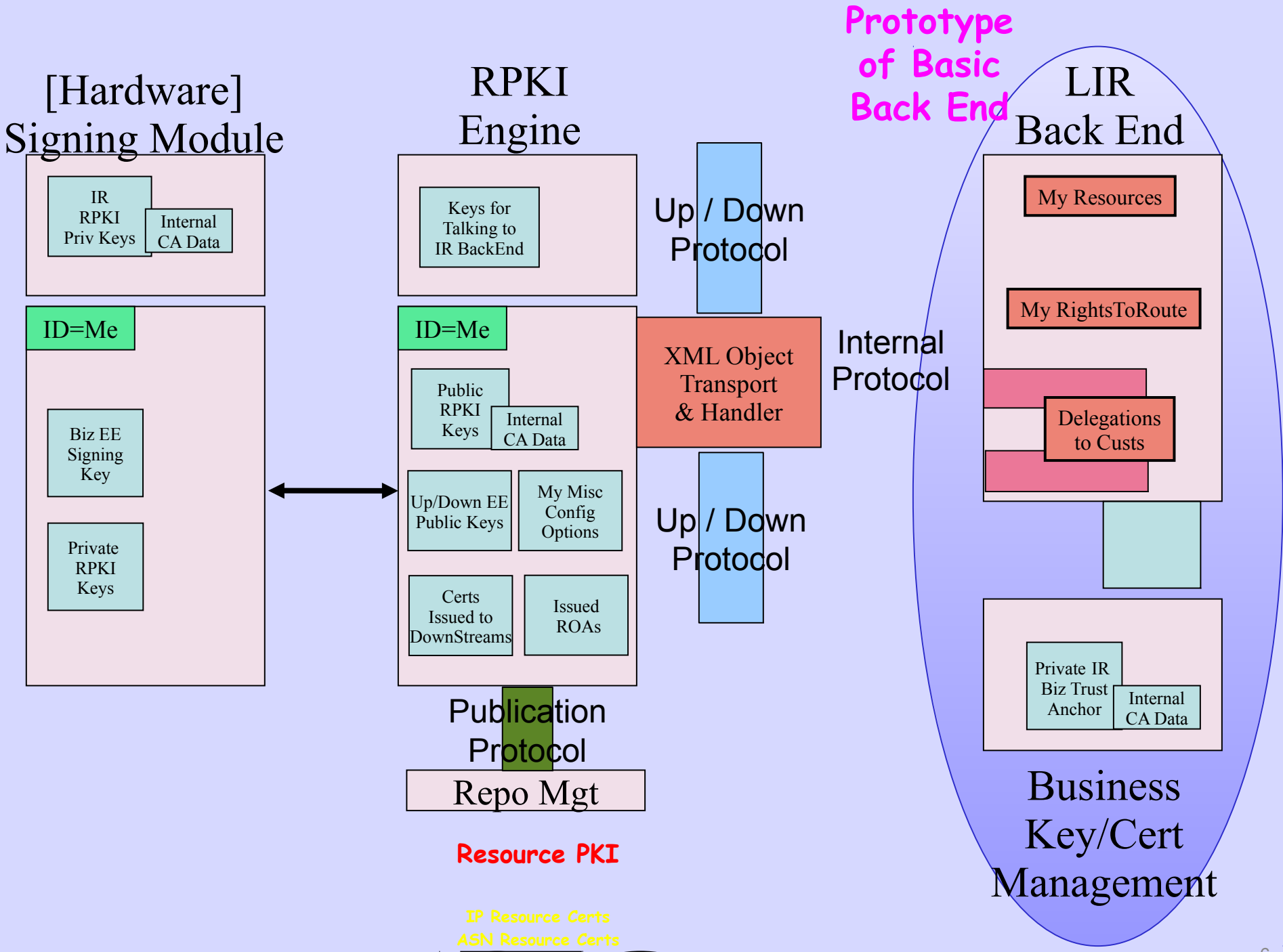
Expensive
To Fetch &
Unreliable



Reliability Via Hosted Publication



Reducing the Number of Publication Points Makes RCynic More Efficient


Prototype of Basic Back End
[Hardware] Signing Module
IR RPKI Priv Keys
Internal CA Data
ID=Me
Biz EE Signing Key
Private RPKI Keys
RPKI Engine
Keys for Talking to IR BackEnd
ID=Me
Public RPKI Keys
Internal CA Data
Up/Down EE Public Keys
My Misc Config Options
Certs Issued to DownStreams
Issued ROAs
Up / Down Protocol
XML Object Transport & Handler
Up / Down Protocol
Internal Protocol
LIR Back End
My Resources
My RightsToRoute
Delegations to Custs
Private IR Biz Trust Anchor
Internal CA Data
Business Key/Cert Management
Publication Protocol
Repo Mgt
Resource PKI
IP Resource Certs
ASN Resource Certs
Route Origin Attestations

Publication Protocol

- XML in CMS over HTTP
- Two sub-protocols

- Config proto: configure a client
  - URI
  - (BPKI) cert to authorize the client
  - (optional) glue cert

Publication Protocol, part 2

- Actions: publish, withdraw, (list?)
- Objects: cert, CRL, manifest, or ROA
- Example:

```
<msg version="1" type="query" xmlns="http://example.com/pub/">
      <certificate action="publish" uri="rsync://foo/j7ghjwblCrcCp9lt.cer">
MIIE+jCCA+KgAwIBAgIBDTANBgkqhkiG9w0BAQsFADAzMTEwLwYDVQQDEyhERjRBODAxN0U2
      </certificate>
</msg>

<msg version="1" type="reply" xmlns="http://example.com/pub/">
    <certificate action="publish" uri="rsync://foo/j7ghjwblCrcCp9lt.cer"/>
</msg>
```

Adopt as WG draft?