What this is Not

This does not attempt to boil the ocean, be all things to all people, ISPs, RIRs, …

We leave ocean boiling to the TVTF

We need to be able to formally certify rights to resources that are soon to get scarce

Not Everyone’s Solution

This is what ARIN things ARIN needs

It is what ARIN thinks its largest members will need

And we suspect other RIRs will need something very similar

But all we care about is compatibility of the certs and the traffic on the wire

Not an Identity System

We are not certifying members' identities

We just need to know that you are the entity that signed our member agreement

Just be able to replay the 'business' key or its child

Not Signing Everything

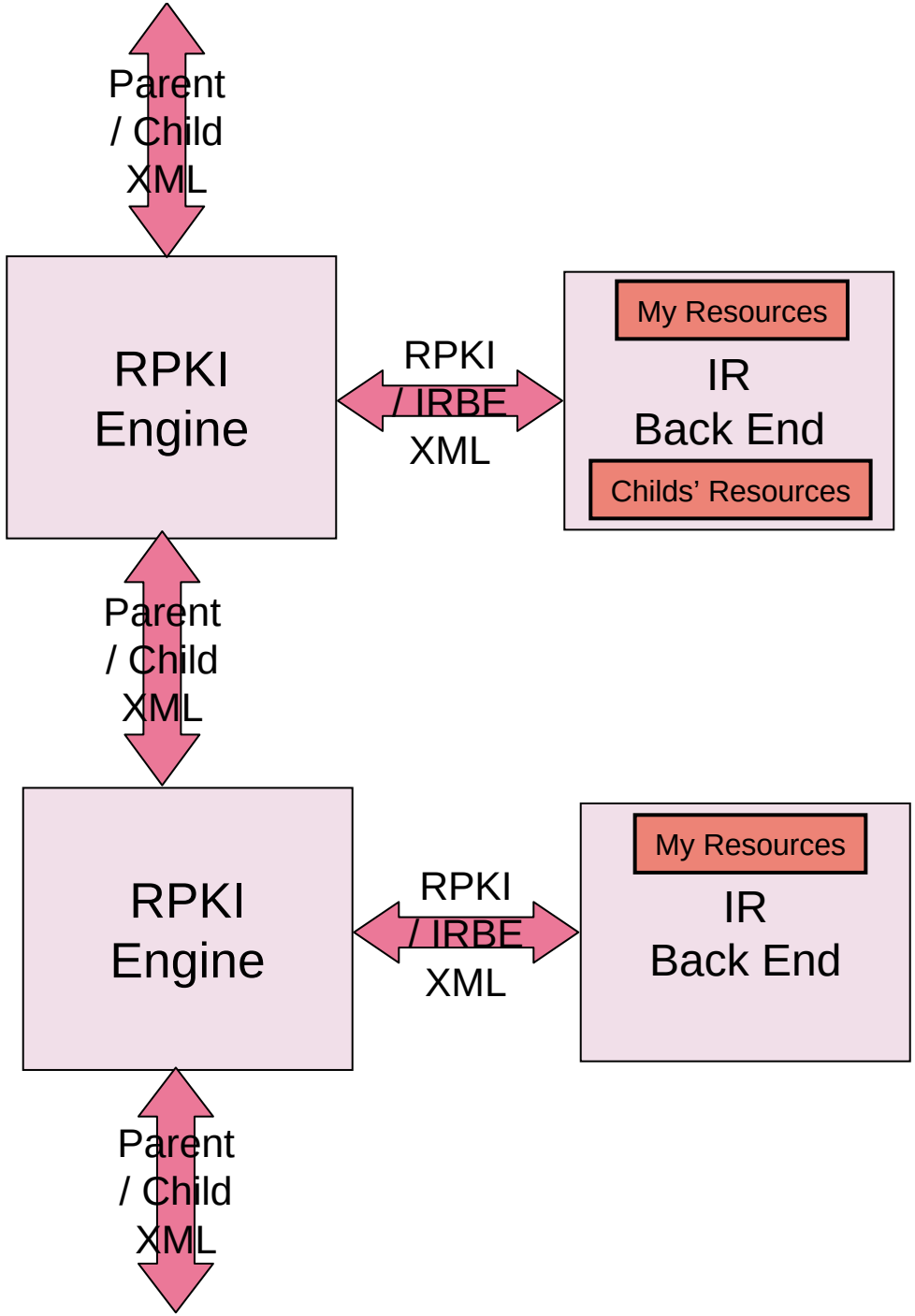
Signing RFC 3779 resource objects

Signing ROAs

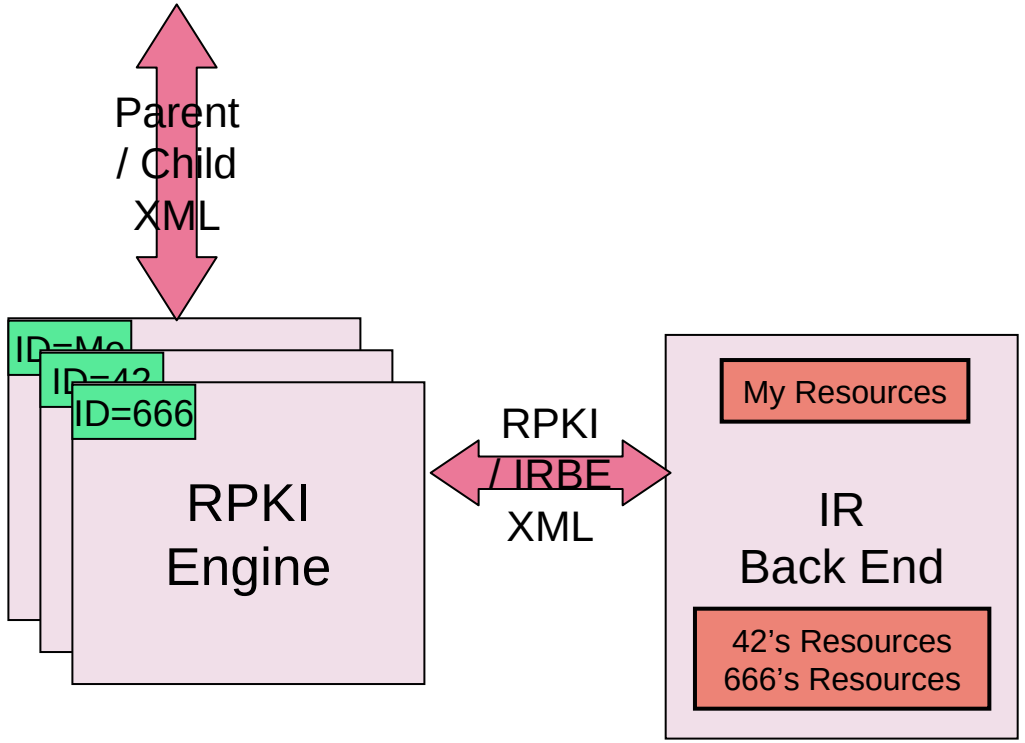
Not signing arbitrary blobs, whois, IRR, …

But the certs are certs with keys, so your members can sign bank transactions if anyone is silly enough to let them

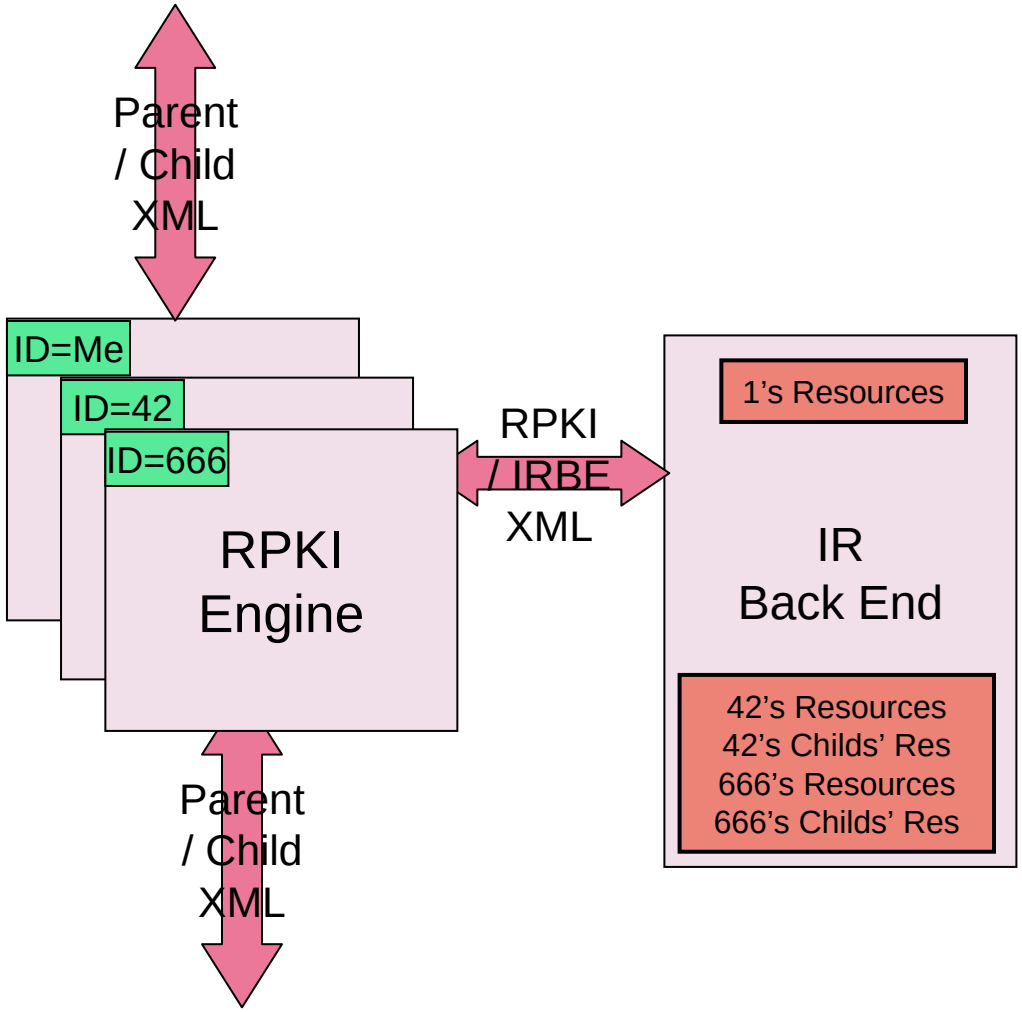
Simple Parent and Simple Child



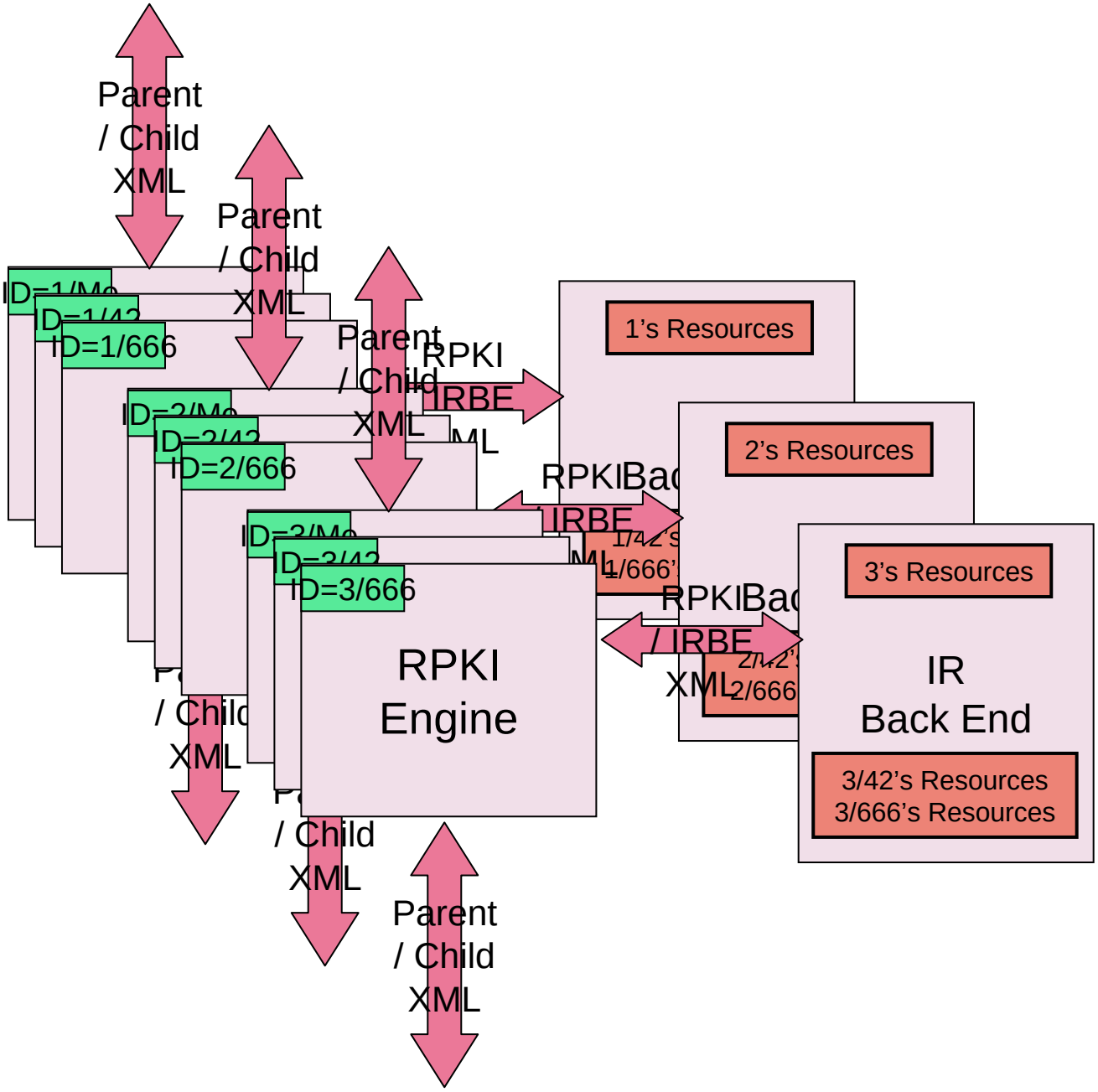
Hosting of Stub Children



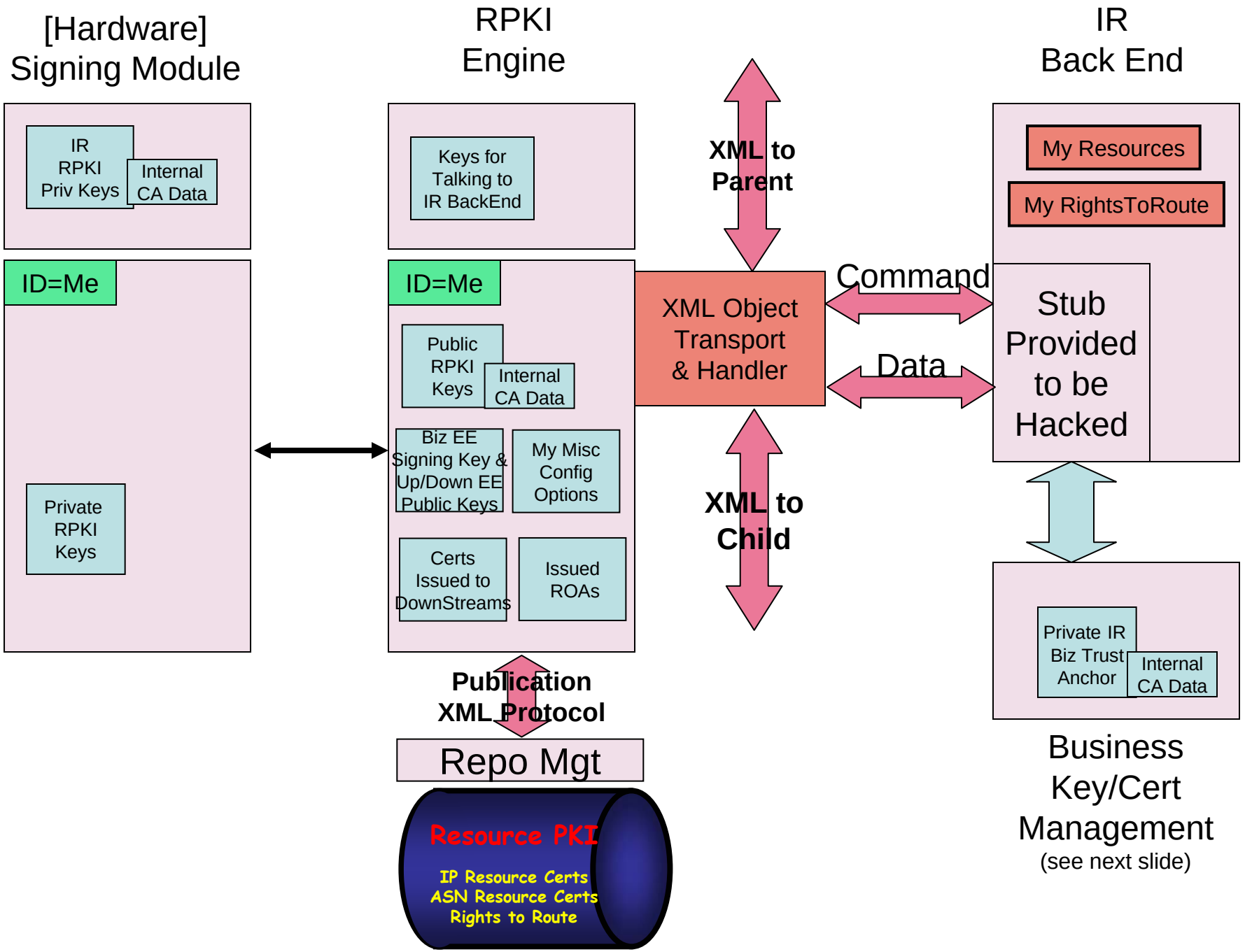
Hosting of a Sub-Alocator



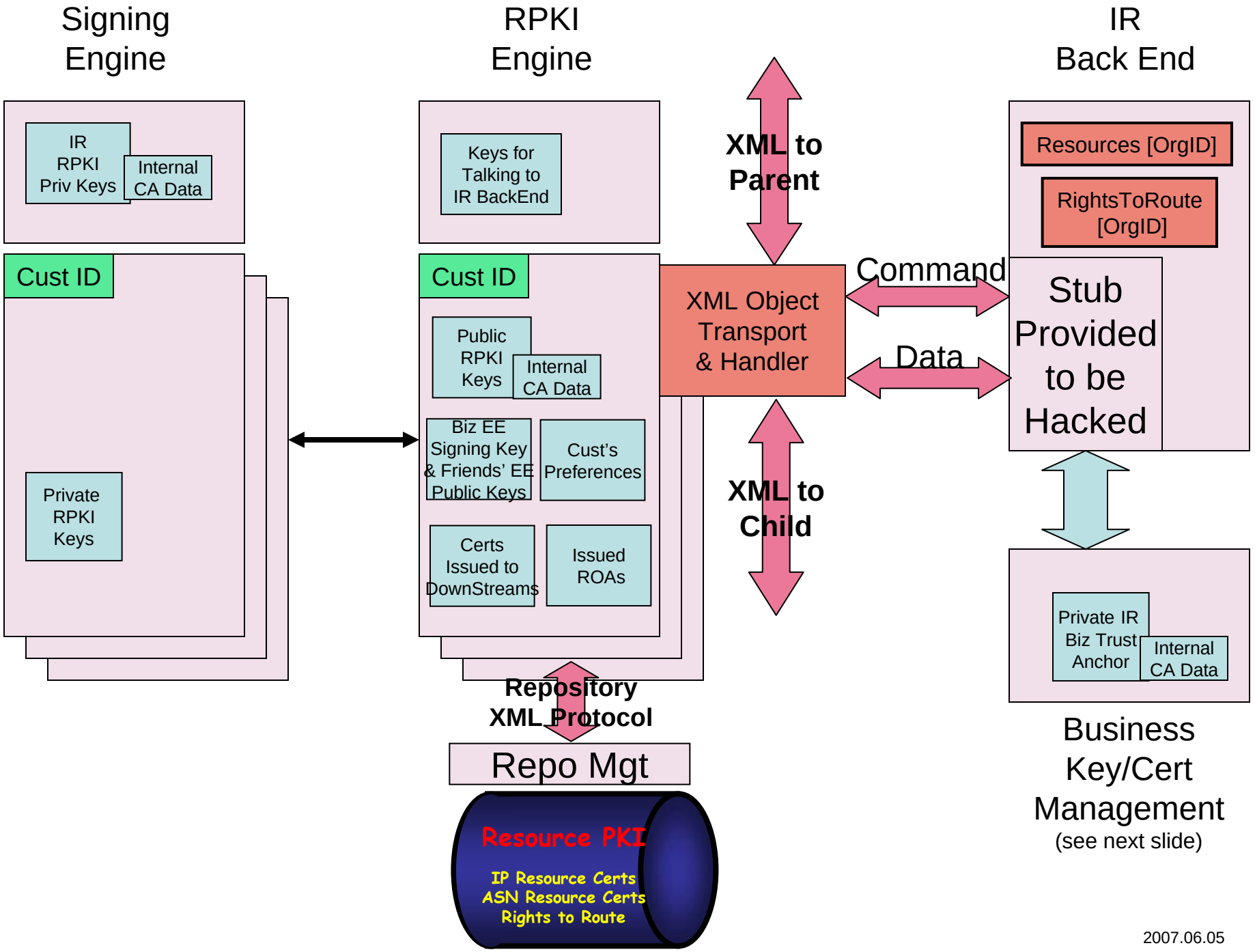
Hosting of many Sub-Alocators



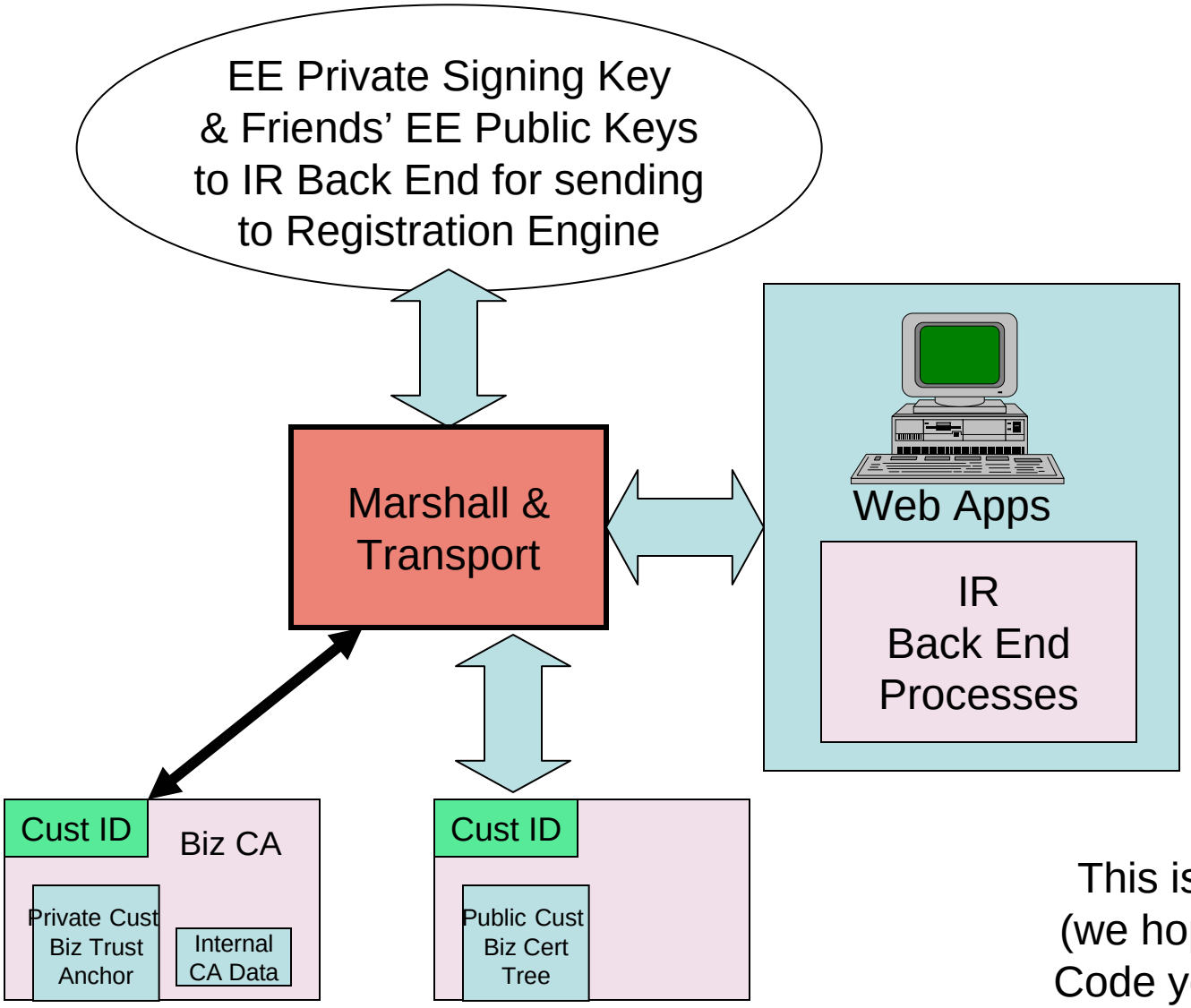
2007.03.20


[Hardware]
Signing Module
IR
RPKI
Priv Keys
Internal
CA Data
ID=Me
Private
RPKI
Keys
RPKI
Engine
Keys for
Talking to
IR BackEnd
ID=Me
Public
RPKI
Keys
Internal
CA Data
Biz EE
Signing Key &
Up/Down EE
Public Keys
My Misc
Config
Options
Certs
Issued to
DownStreams
Issued
ROAs
XML to
Parent
XML Object
Transport
& Handler
XML to
Child
Command
Data
IR
Back End
My Resources
My RightsToRoute
Stub
Provided
to be
Hacked
Private IR
Biz Trust
Anchor
Internal
CA Data
Business
Key/Cert
Management
(see next slide)
Publication
XML Protocol
Repo Mgt
Resource PKI
IP Resource Certs
ASN Resource Certs
Rights to Route

2007.05.08


Signing Engine
RPKI Engine
IR Back End
IR RPKI Priv Keys
Internal CA Data
Cust ID
Private RPKI Keys
Keys for Talking to IR BackEnd
Cust ID
Public RPKI Keys
Internal CA Data
Biz EE Signing Key & Friends' EE Public Keys
Cust's Preferences
Certs Issued to DownStreams
Issued ROAs
XML to Parent
XML Object Transport & Handler
XML to Child
Command
Data
Resources [OrgID]
RightsToRoute [OrgID]
Stub Provided to be Hacked
Private IR Biz Trust Anchor
Internal CA Data
Repository XML Protocol
Repo Mgt
Resource PKI
IP Resource Certs
ASN Resource Certs
Rights to Route
Business Key/Cert Management
(see next slide)
2007.06.05

Business Key/Cert Management



This is a clarifying (we hope) example. Code your own. We just want the keys!

2007.06.05

What is in RE Per-Cust Data?

- Biz EE Signing Key so XML engine can sign and optionally encrypt XML objects
- Up-streams' and down-streams' Biz EE Public Keys so we can decrypt & verify received XML objects
- Ability to request from IR Back End list of current resources in cannonicalized from as received
- Collection of issued certs that might still be current (expired or revoked?)
- Ability to request from IR Back End list of Rights to Route
- Collection of issued ROAs
- Customer's “Preferences”
  - which of the 6/7 customer types
  - ...