

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 thinks 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

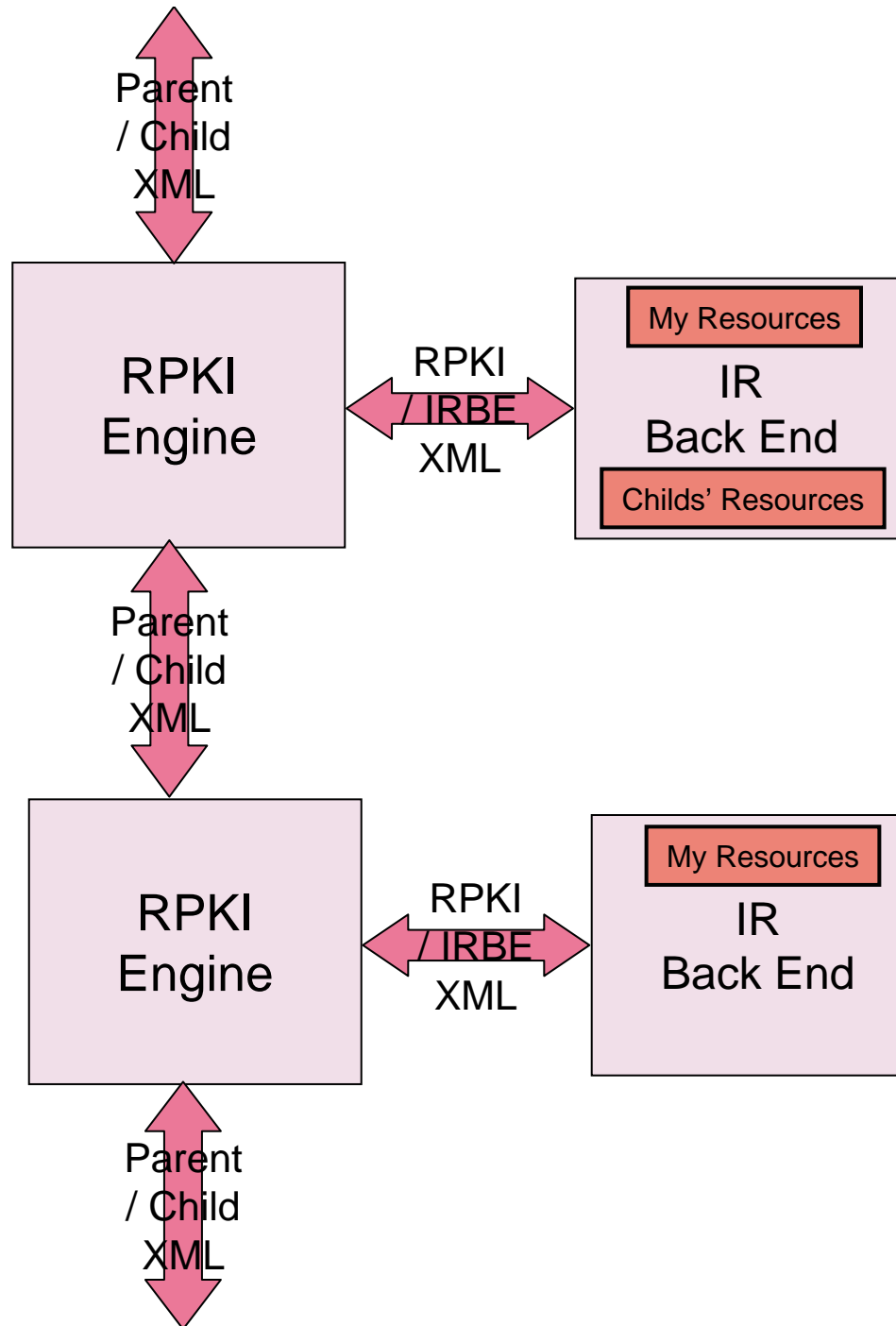
Signing RFC 3779 resource objects

Signing ROAs

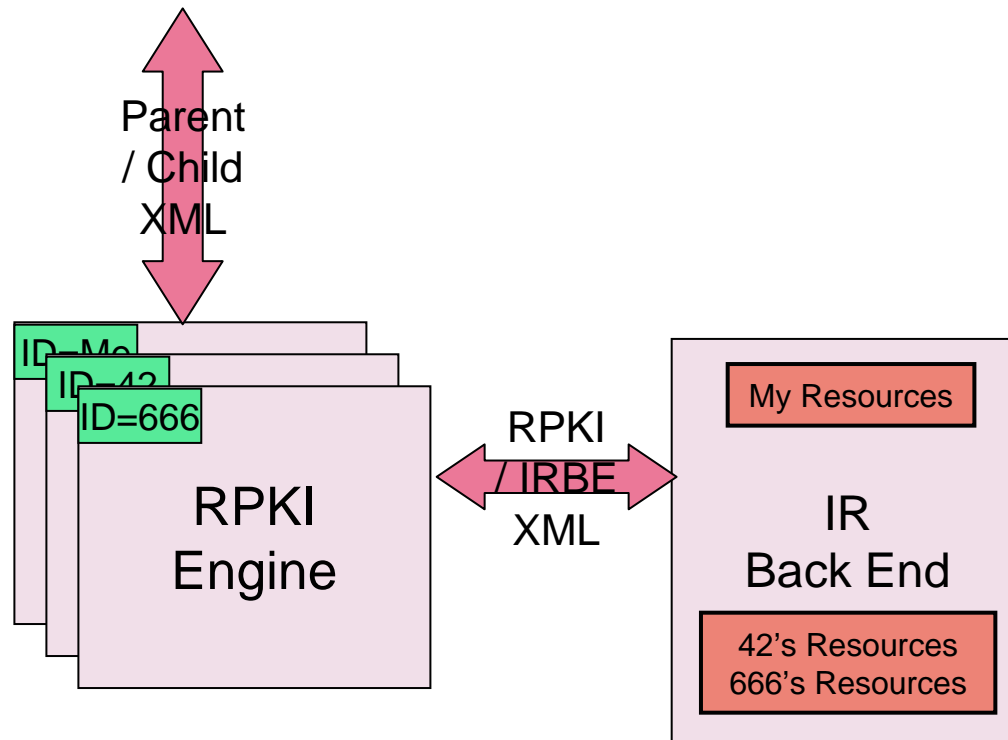
Not signing arbitrary blobs, whois, IRR, ...

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

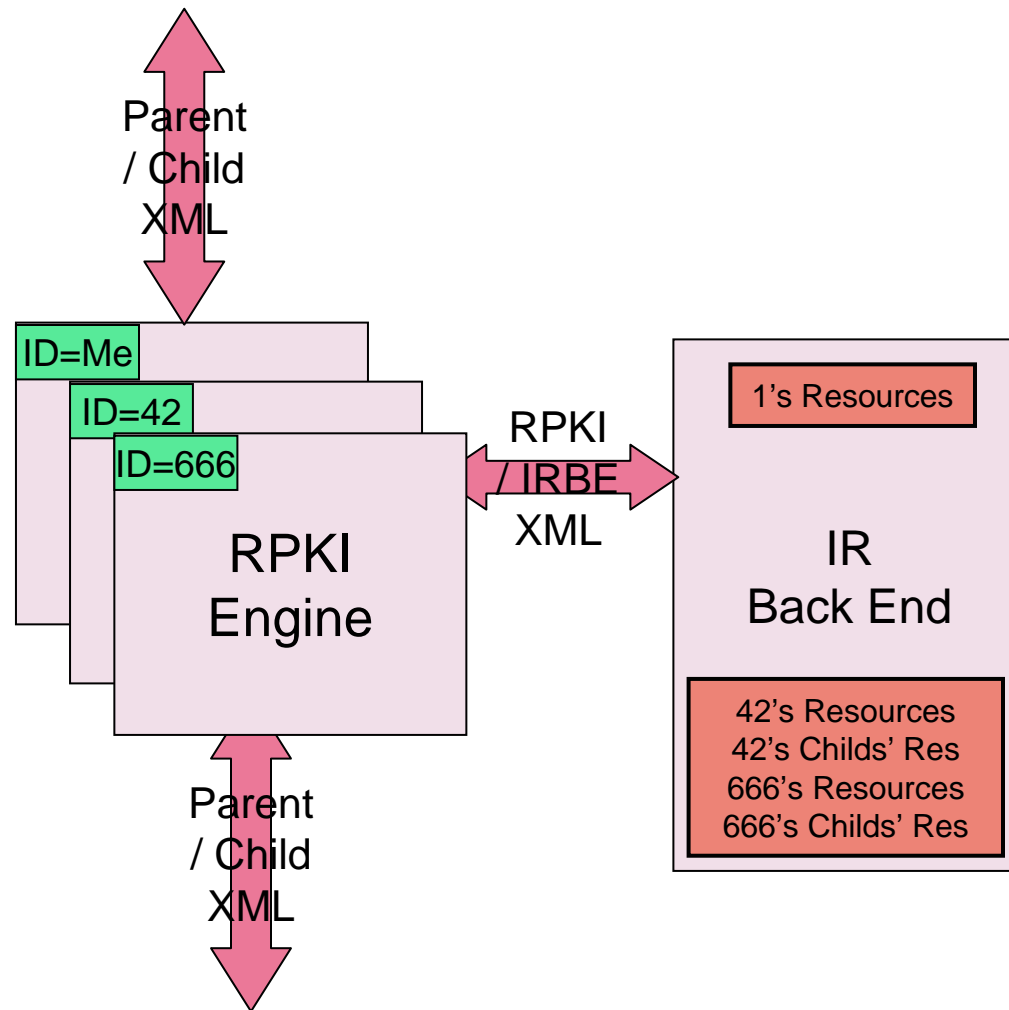
Simple Parent and Simple Child



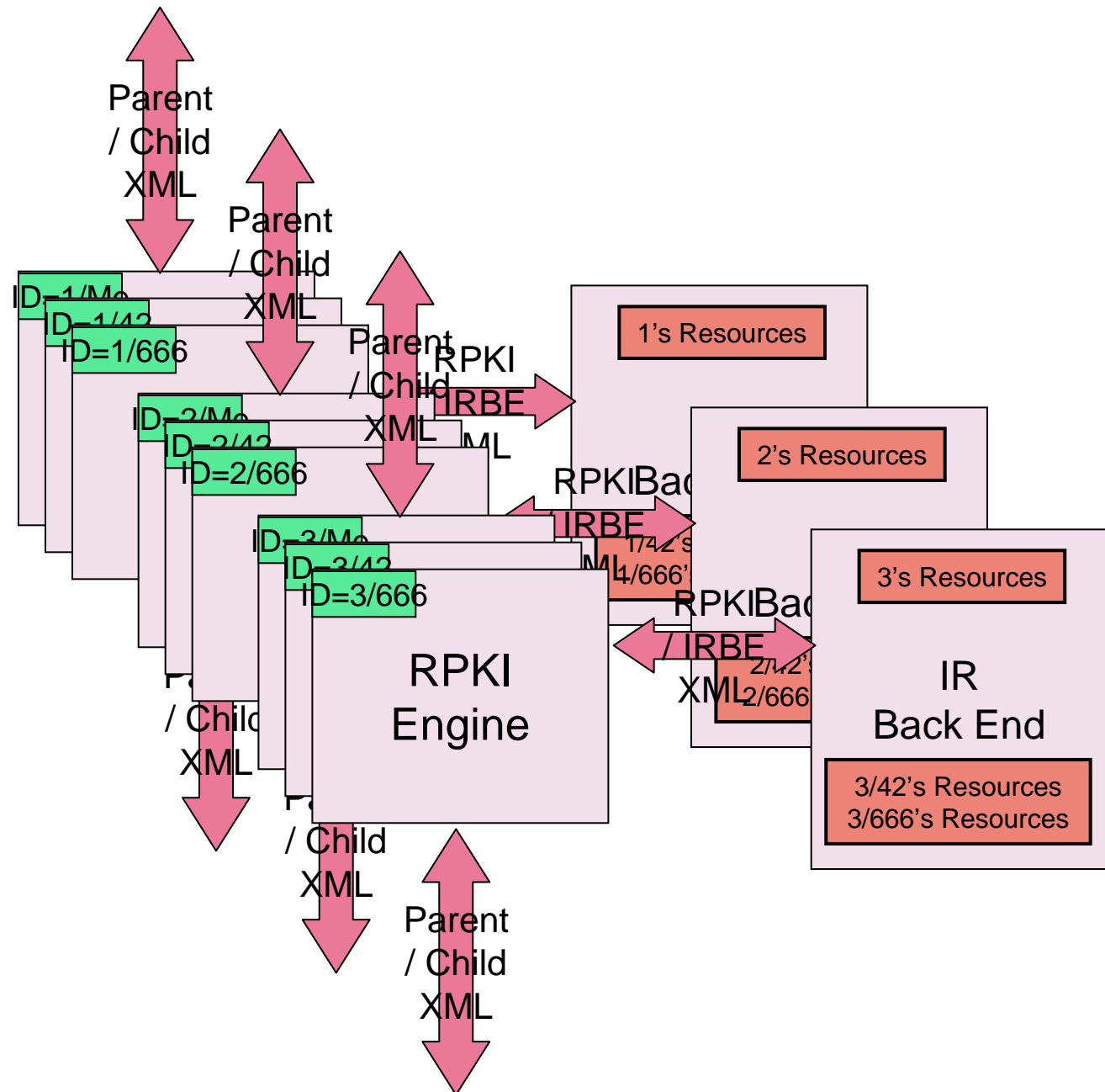
Hosting of Stub Children

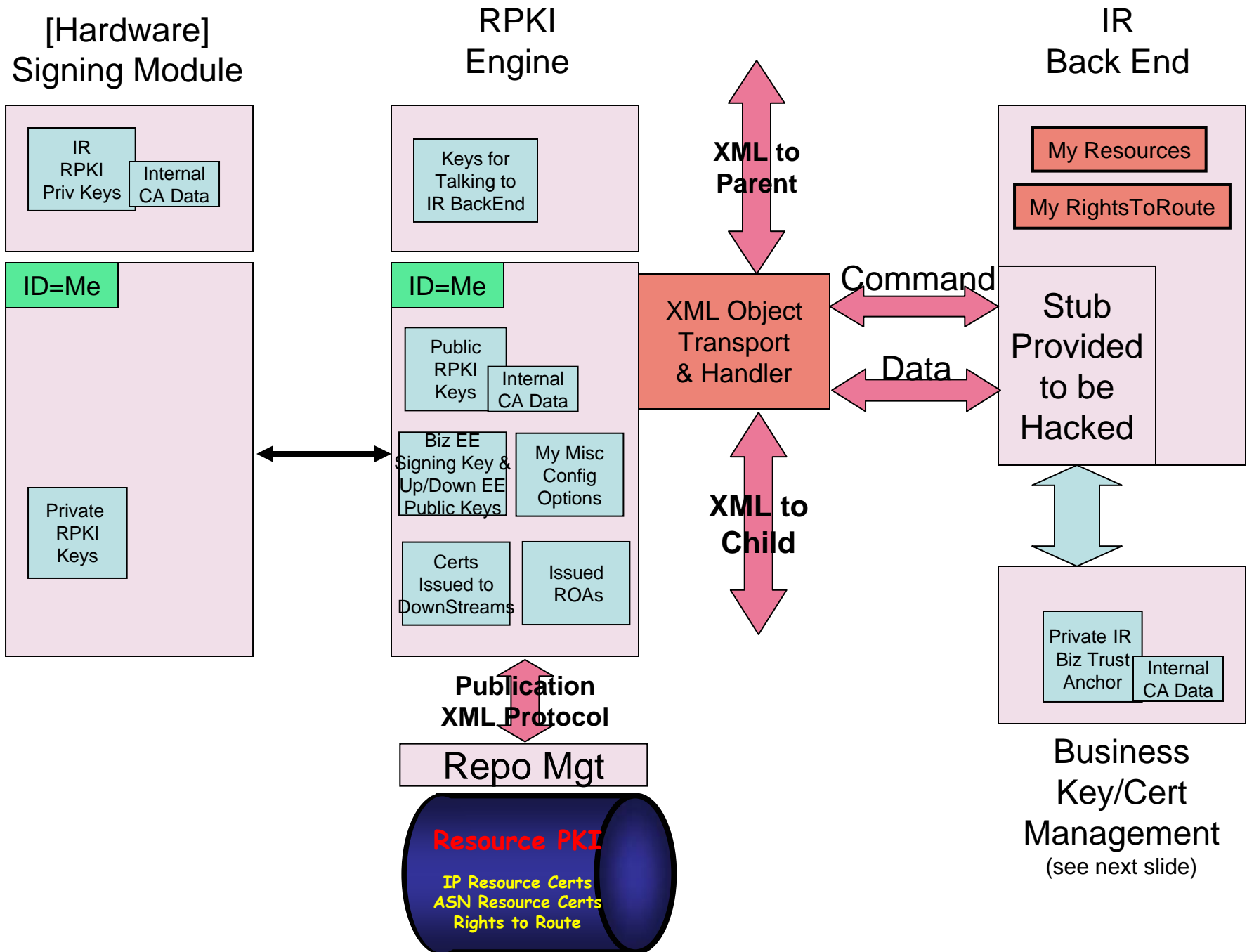


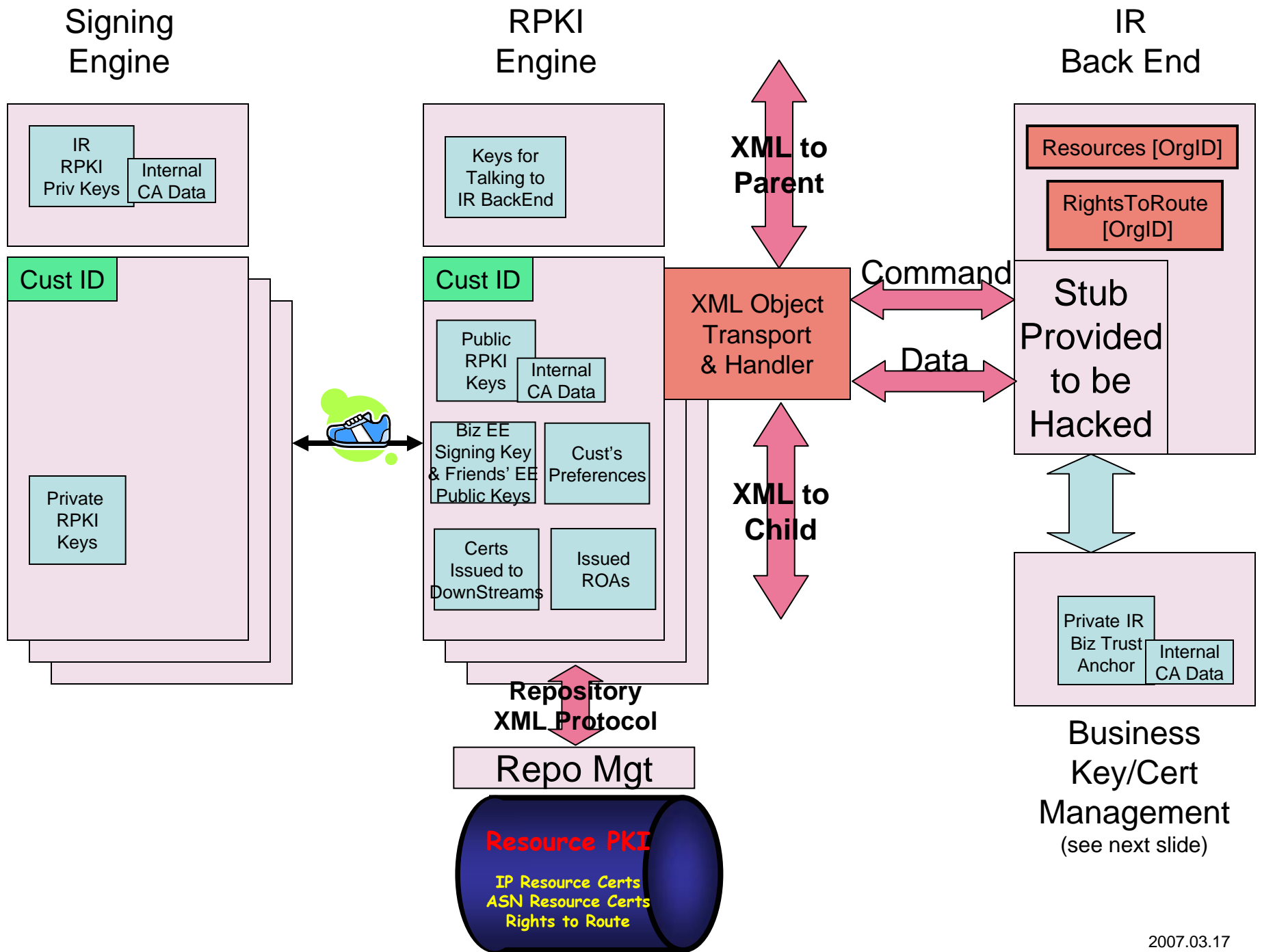
Hosting of a Sub- Alocator



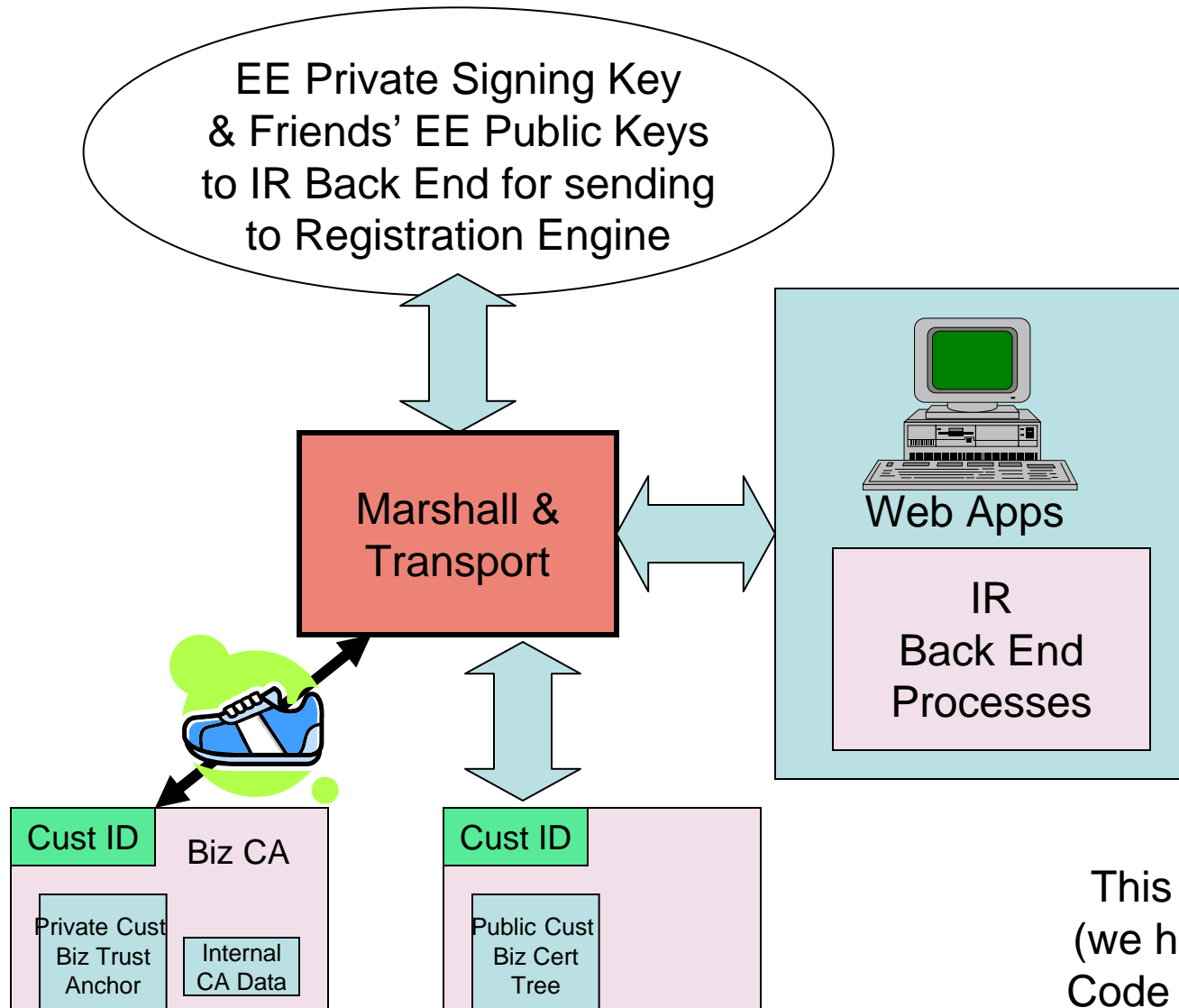
Hosting of many Sub- Alocators







Business Key/Cert Management



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

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 canonicalized form 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
 - ...