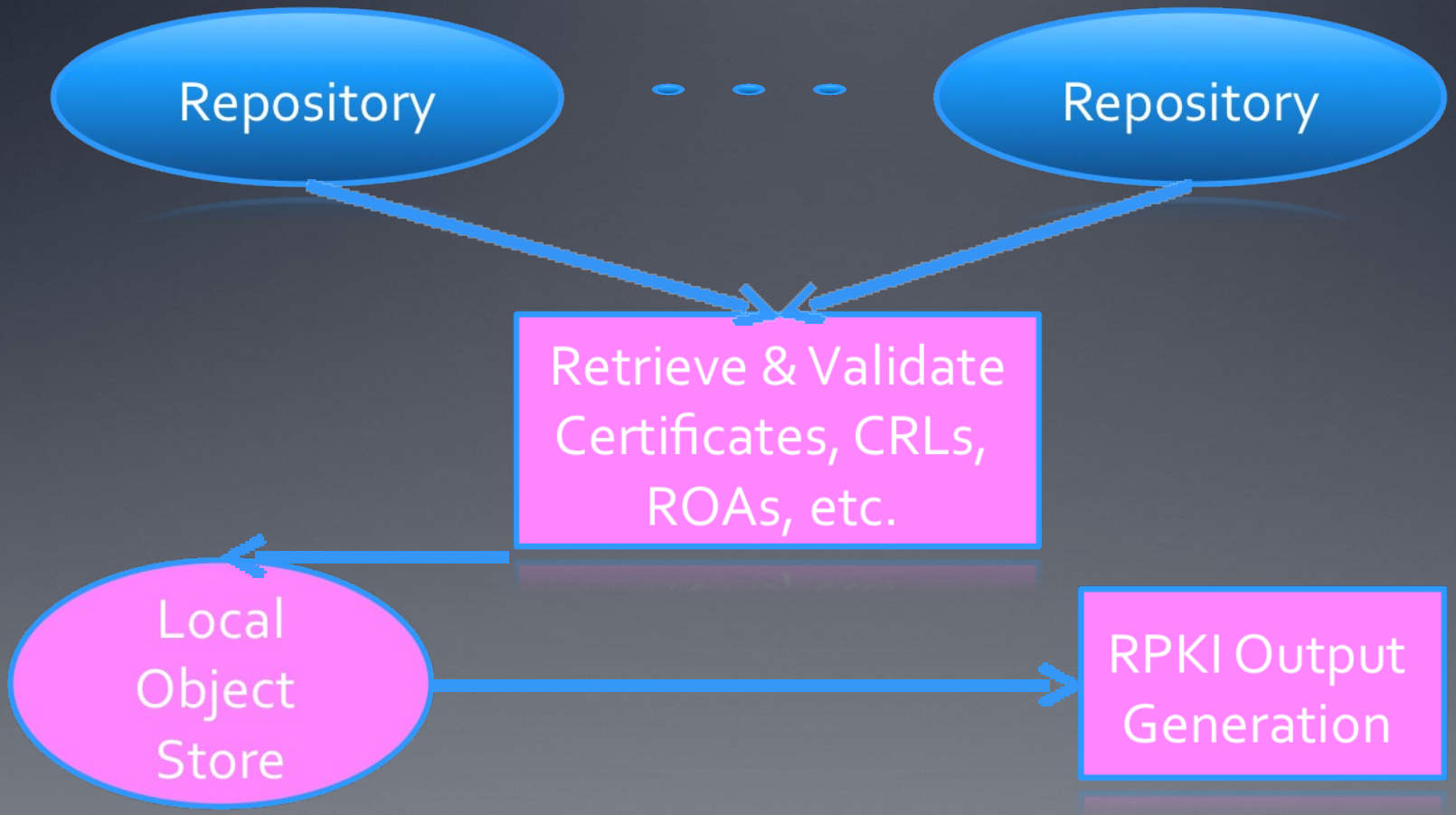
Local Control Options for RPKI Objects

Stephen Kent

BBN Technologies

RPKI Local Processing Model



RPKI Relying Party Software

- BBN is producing open source Relying Party (RP) software for use with the RPKI
- We are soliciting inputs for local management controls for this software
- The following presentation describes some of the controls we are implementing, and raises questions about what other controls RPs may desire
- Please send comments to kent@bbn.com

Local RPKI Control

- Each RP in the RPKI has the ability (in principle) to control how it views objects acquired from the distributed RPKI repository system
  - Each RP can decide which entities will be treated as Trust Anchors (TAs)
  - Each RP can decide what to do with “stale” or expired objects
    - Stale CRLs
    - Stale manifests
    - Expired certificates
    - Expired ROAs
  - The question is what controls really are available in your RP software

Stale vs. Expired

- Certificates expire
  - A certificate contains a validity interval (not before and not after)
  - In general RP software considers expired certificates to be invalid
  - One can provide local controls to override this, at the discretion of the RP, with attendant risks!
- CRLs (and manifests) do not expire
  - A CRL (or manifest) contains a next issue date/time, and after that date/time the data is stale, but not invalid
  - It is common for RP software to allow certificate validation with stale (or missing) CRL data, and to provide a warning (which is then ignored by the user ☺)

Stale/Expired Controls

- Currently the BBN RP software allows an RP to makes decisions on what to do about stale objects
  - Insist on current (vs. stale) objects
  - Warn about stale CRLs
  - Want about stale manifests
  - Accept stale CRLs
  - Accept stale manifests
- Currently the BBN RP software requires that all certificates be not expired
  - It probably would be possible to offer a control to allow an RP to set a “grace period” for certificate expiration (for all certificates) if this is necessary

“Bad” Revocation?

- In any PKI, the CA that issues certificates is empowered to revoke those certificates
- The circumstances under which a CA can revoke a certificate are spelled out in the CPS for the
- The RIRs are member-controlled organizations, so members should require that the CPS for their RIR spells out acceptable revocation policies
- The CPS also describes technical procedures by which revocation is effected, e.g., multi-party crypto controls
- Nonetheless, RPs may be able to adopt purely local measures to protect themselves against bad revocation actions

Overriding a CRL?

- Certificate validation software typically does not allow an RP to ignore a CRL, i.e., if a certificate is listed on a CRL, and the CRL is valid, the certificate is considered to be invalid and cannot be used
- If RPs in the RPKI context feel that it is important to be able to (locally) override a CRL entry, to protect themselves against inappropriate (accidental) revocation actions, we could add that capability
- But, manual operator approval of CRLs may impose an operational burden (see next slide)

CRL Override Algorithm

- Applies only to CRLs issued to cover CA certificates (vs. CRLs that cover EE certificates used for ROAs, manifests, etc.)
- Applies only to non-empty CRLs
- When a CRL is encountered with a new entry, require operator approval before accepting the new CRL entry
- Once the new CRL entry is accepted, it will not require operator approval again
- Removal of an entry from a CRL (e.g., because the revoked certificate timed out) does not require re-approval

What Would an Operator See?

- Remember that a CRL specifies revoked certificates as a series of certificate serial numbers, relative to the CA that issued the revoked certificates
- So, a new CRL entry is just a certificate serial number
- RP software could locate the certificate in question (from the local cache, since it would have been deleted form the repository system)
- The certificate does NOT contain a meaningful Subject (or Issuer) name, so the only useful info to display may be the allocations contained in the certificate
- Is this good enough?

Questions?