Resource Certificate Profile

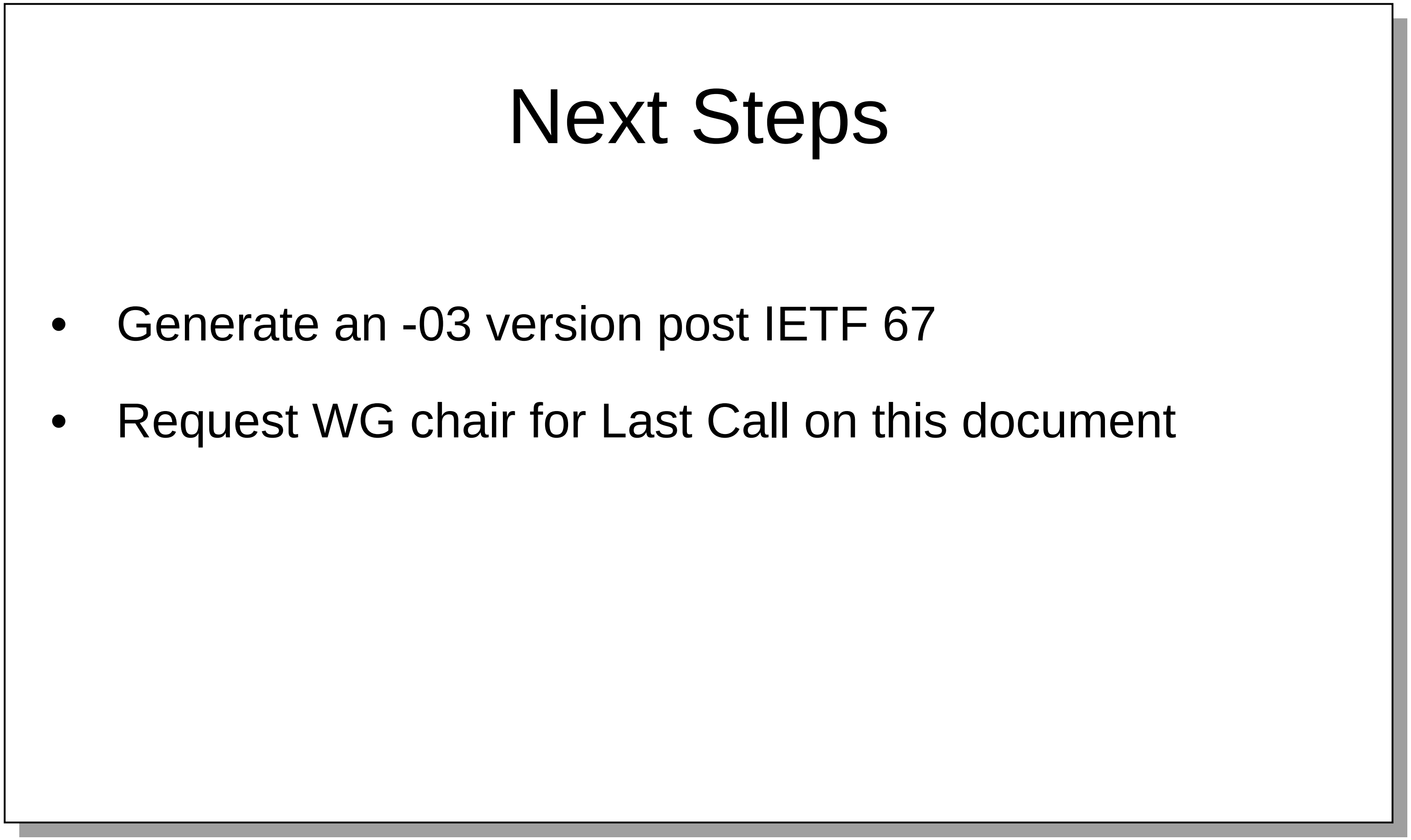
Geoff Huston, George Michaelson, Rob Loomans

APNIC

IETF 70

Was it only a year ago?

SIDR WG Meeting – November 2006



Next Steps

- Generate an -03 version post IETF 67
- Request WG chair for Last Call on this document

Changes for -09

Added:

- Manifests to the SIA field in the profile of the certificate and the profile of the certificate request

Retained:

- RSYNC as a MUST in the access methods for retrieval of RPKI objects
    - This has been the topic of discussion through various stages of review of this profile

Dropped:

- Subject Alternate Name

Next Steps - Again

- Generate an -10 version post IETF 70
  - Complete manifest description in SIA

- Request WG chair for Last Call on this document – again

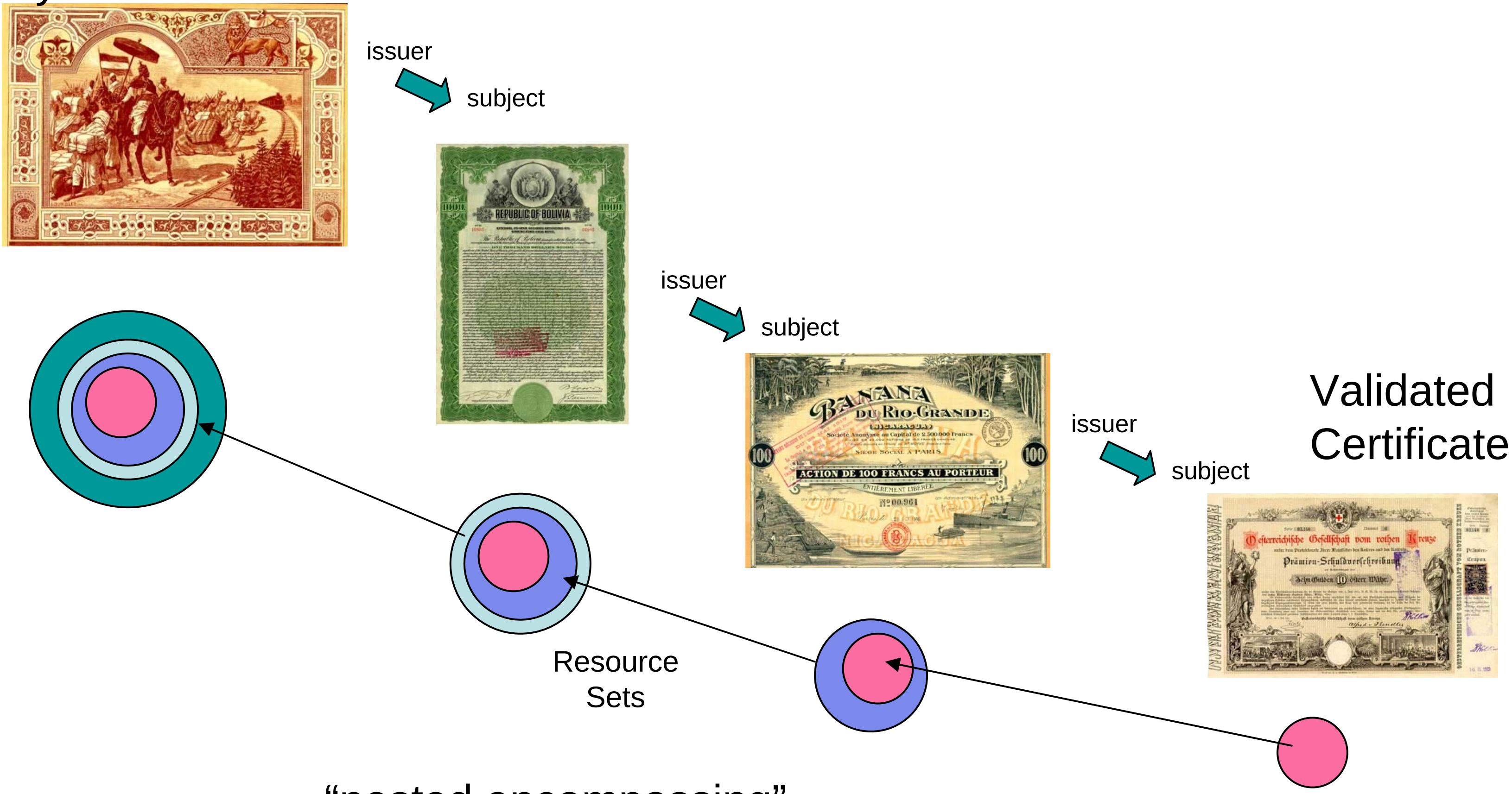
Some Musing about Validation

- Section 7.3 of the draft requires that the immediate superior certificate in the validation certificate path has a resource extension that encompasses the subordinate certificate.

  This is a “nested encompassing” constraint that is placed upon the resource extensions of all certificates in the validation certificate path

ResCert Validation

Certificate Issued
By Trust Anchor



issuer

subject

issuer

subject

issuer

subject

Validated
Certificate

Resource
Sets

REPUBLIC OF BOLIVIA
BANANA DU RIO-GRANDE
ACTION DE 100 FRANCS AU PORTEUR
Oesterreichische Gesellschaft vom rothen Kreuze
Prämien-Schuldverschreibung

“nested encompassing”

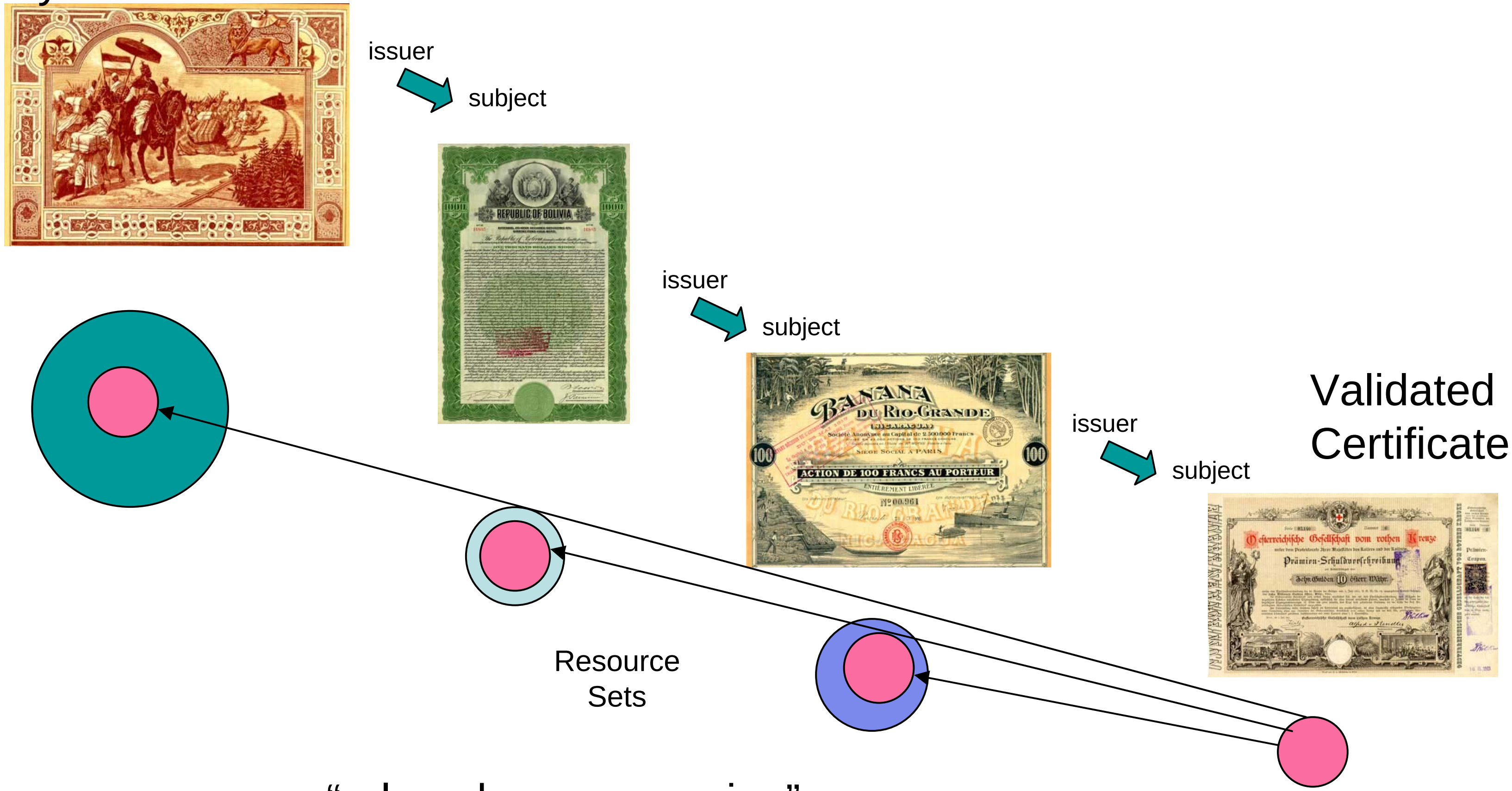
An Alternate Approach

Warning: All this could well be a **Very Bad Idea**

- – Is “nested encompassing” absolutely required in validation?
- – Would it be useful to relax this?

Alternate ResCert Validation

Certificate Issued
By Trust Anchor



Validated
Certificate

Resource
Sets

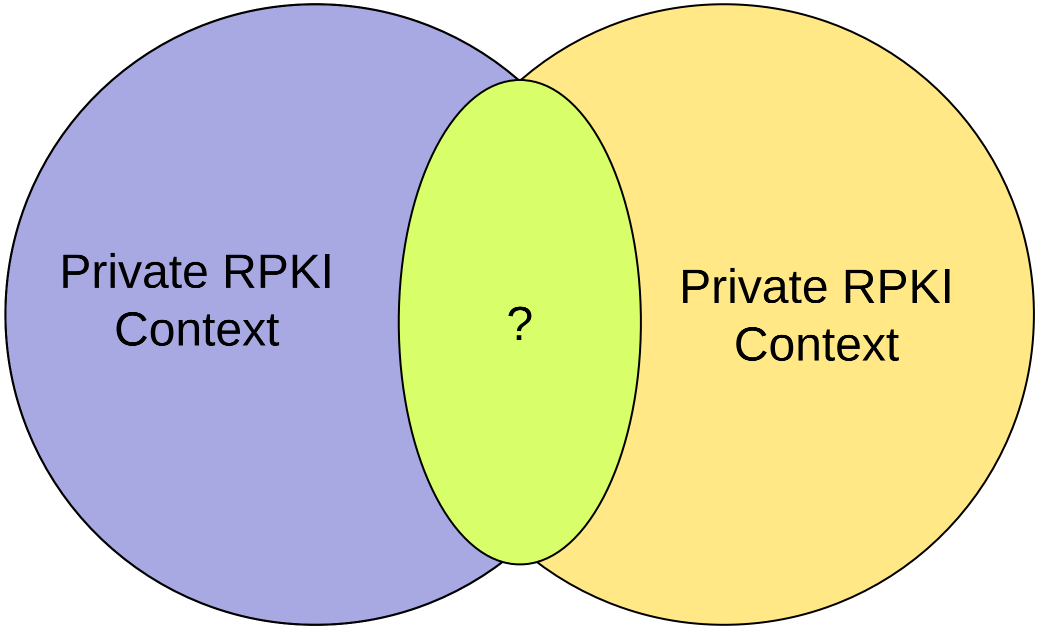
“relaxed encompassing”

Alternate Rescert Validation

- The resources of the certificate being validated are encompassed by the resource extensions in the validation certificate path, but the certificates in this path do not necessarily have to encompass each other

Alternate Rescert Validation

- Potential use in intersecting private use space contexts



Alternate Rescert Validation

This really could be a Very Bad Idea!

But if you have some opinions on this, it would be interesting to hear them!