PKI Issues Panel

Rob Austein, Russ Housley, Steve Kent, Job Snijders

Moderator: Randy Bush

Creative Commons: Attribution & Share Alike

Three Items

- Manifest Ops Ooopsie
- Manfests
- CRLs

- I will set each one up
- Then panelists in turn or not
- Then, of course I have opinions

Creative Commons: Attribution & Share Alike

Ops Oopsie

- The NCC manifest oopsie was an ops oopsie
- The RIRS will learn that responsibility weighs heavy
- Take a look at all the checking and care the root DNS requires
- Welcome to the apex of an operationally critical hierarchy

Creative Commons: Attribution & Share Alike

RFC 6486 - Manifests

- RFC 6486 needs to be updated
- How it got published in a weak state was a classic sidr WG social disfunction
- Some of us might be willing to help; but we're not funded, so do not expect any of us to do the heavy lifting; just abusing anyone who does it poorly ☺

Creative Commons: Attribution & Share Alike

CRLs

- CRLs serve a critical purpose
- We actually like them
- CRLs are quite well understood
- We do not have the time, energy, or focus for the revisionist task of unwinding an entire hierarchy of RFCs because some of us are light on x.509 clue

Creative Commons: Attribution & Share Alike

Backup Slides

Creative Commons: Attribution & Share Alike

rb on Ops Ooopsies

- Ops oopsies are not numerable. The key things here are
- There have been oopsies at all CAs <blush>
- We love them anyway; blame does not move packets
- It is time to grow up for all CAs and all CA software
- Growing up is a non-terminating process

Creative Commons: Attribution & Share Alike

rb on Manifests

- 6486 really really needs to be updated
- By [R]PKI experts, not us kiddies
- But the meeting needs to establish the basic rules of the manifest road; and we do know them; we just did not document them well
- There is no need to get excited and be creative, tyvm
- The CA/pub software is supposed to know how to update the pub point atomically; if not, it is a resume creating event
- If an object is in repo but not in manifest, it is a publication bug or an attack. detecting these is why manifests exist
- If desperate you MAY use an older one which is still time-valid; but that will have consequences, i.e. likely raise errors

Creative Commons: Attribution & Share Alike

rb on CRLs

- The current docs are clearer, mainly because CRLs are from PKIX history
- There MUST be one per CA == pub point
- They serve a very different function than manifests
- The CA/pub software is supposed to know how to update atomically; if not, it is a resume creating event

Creative Commons: Attribution & Share Alike