Manifest EE Certificate Validity Times

Proposed Change to RFC 6486

In the case of a "one-time-use" EE certificate, the validity times of the EE certificate MUST exactly match the thisUpdate and nextUpdate times of the manifest.
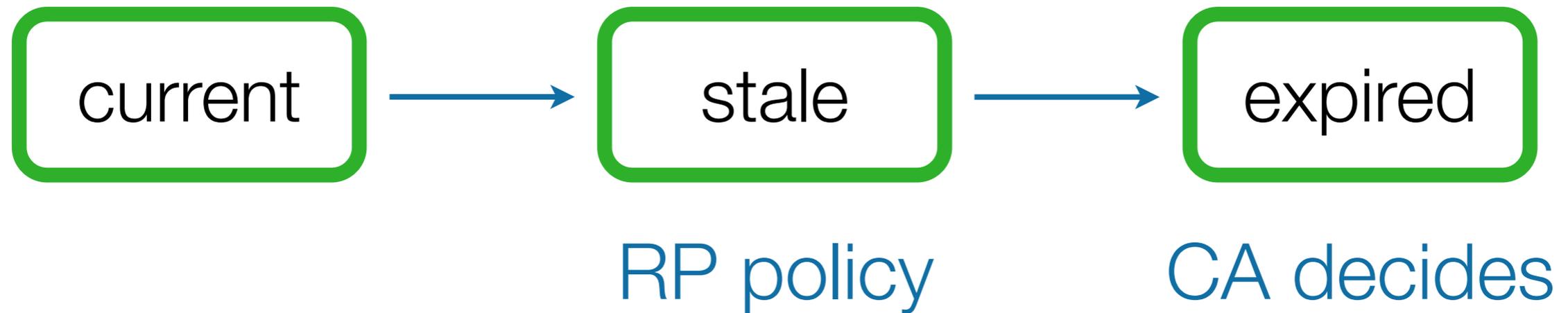
In the case of a "sequential-use" EE certificate, the validity times of the EE certificate MUST encompass the time interval from thisUpdate to nextUpdate

↓

The validity times of the EE certificate MUST encompass the time interval from thisUpdate to nextUpdate.

Tuesday, July 30, 13

Rationale

current → stale → expired

RP policy   CA decides

- Let RP use local policy to deal with failure to retrieve updates, regardless of cause

- Let CAs 'fiddle' with soft limits: "we will most likely republish by..., but please don't reject everything if we're late, or.. you are.", and hard limits: "reject everything that's expired, I am not willing to risk my data replayed after this much time ".

- Arguments against?
- Best practices?