Clearance and CA Clearance Constraints Certificate Extension

draft-turner-caclearanceconstraints-00.txt

Sean Turner

Santosh Chokhani

Outline

- What’s in the ID?
- How’s it used?
- What’s all the controversy?

What's in the ID?

- Defines syntax and semantics for two certificate extensions:
  - *Clearance*. The *Clearance* certificate extension indicates the clearances held by the subject. It uses the clearance attribute's syntax from RFC 3281 (Policy ID, Classification List, and Security Categories).
  - *CA Clearance Constraints*. The *CA Clearance Constraints* extension constrains the effective Clearance of the subject of the last certificate in the certification path. It is a sequence of one or more Clearances.

How’s it used?

- Hierarchy:
  - Root: No constraints
  - CA: CA Clearance Constraints
  - EE: Clearance
- Processing:
  - Collect certificates
  - Process certificate (rules in ID) to determine the effective Clearance of the subject of the last certificate in the certification path.

What’s all the controversy about?

- Don’t put authorization information in public key certificates!
- Processing rules adversely affects infrastructure/relying parties!
- Why not put Clearance and CA Clearance Constraints in SDA?
- Can’t use clearance attribute syntax as an extension?
- Without security categories it’s too open to implement.

Questions

?