# Is the Default Allow or Deny?

# The Issue

"Everything not explicitly forbidden is permitted"

--or--

"Everything not explicitly permitted is forbidden".

- CAs are inclined to argue the former; it provides them the most flexibility, at the cost of the least predictability.

- Browsers are inclined to argue for the latter; what's the point of a certificate profile if it doesn't actually restrict the profile?

# Example

- BR 7.1.4.2.2 explicitly permits additional subject attributes in subscriber certs
- EV 9.2 explicitly limits the list of subject attributes in EV subscriber certs
- BR 7.1.4.3.1 is silent - it neither explicitly permits or forbids additional attributes in a CA (root or intermediate) certificate
- The ballot (199) that made these changes is titled “Require CommonName in Root and Intermediate Certificates”
- ~20 CAs have reportedly issued certificates that contain subject fields other than those listed in BR 7.1.4.3.1

# Another Example

Are cross-certs a form of Subordinate CA?

- Yes (default deny)
- No, they are something else (default allow)
  - If no, then what prevents a CA from making up terms to exempt certs from requirements
  - Example: distinguishing between issuance, reissuance, rekey, and renewal

# Potential Solutions

- Review the guidelines for ambiguities and attempt to resolve them, then adopt a “default deny” interpretation.
  - The only secure interpretation in the face of ambiguity is to assume that something is not permitted

- Accept that ambiguities will always exist and need to be addressed as they are identified.
  - Interpretation is “the requirements are the requirements” (neither default deny or default allow)
  - The guidelines “stand on their own”