Names and Name Constraints in the Federal PKI

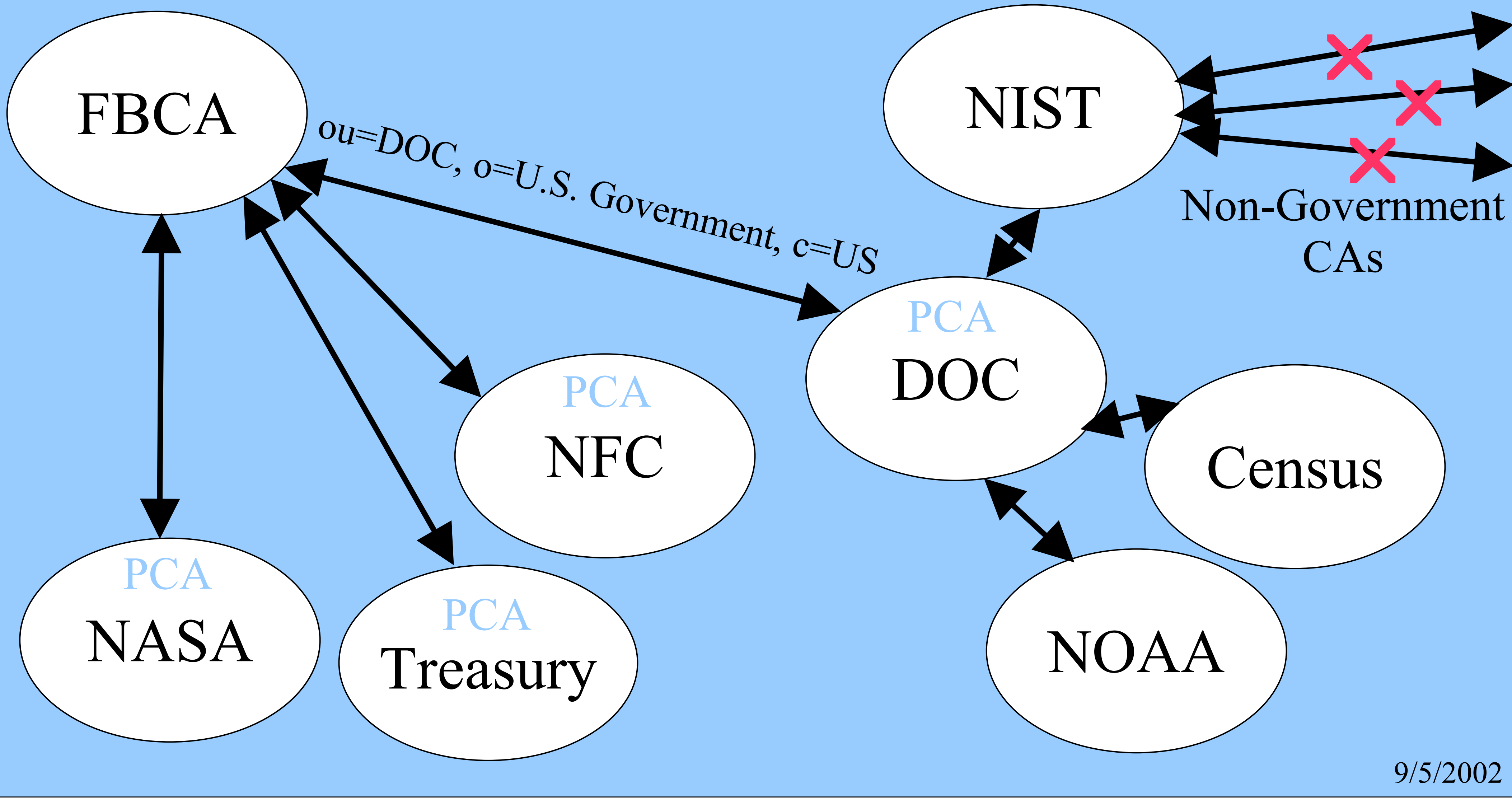
David Cooper
NIST

9/5/2002

Why the FBCA uses name constraints

- Limit each agency to its own name space
- Need to limit transitive trust
- Steer relying parties towards more direct paths
- Shorter paths provide higher assurance:
  - Fewer opportunities for errors
  - Fewer (subjective) policy mapping decisions leads to more reliable policy information

FBCA use of name constraints

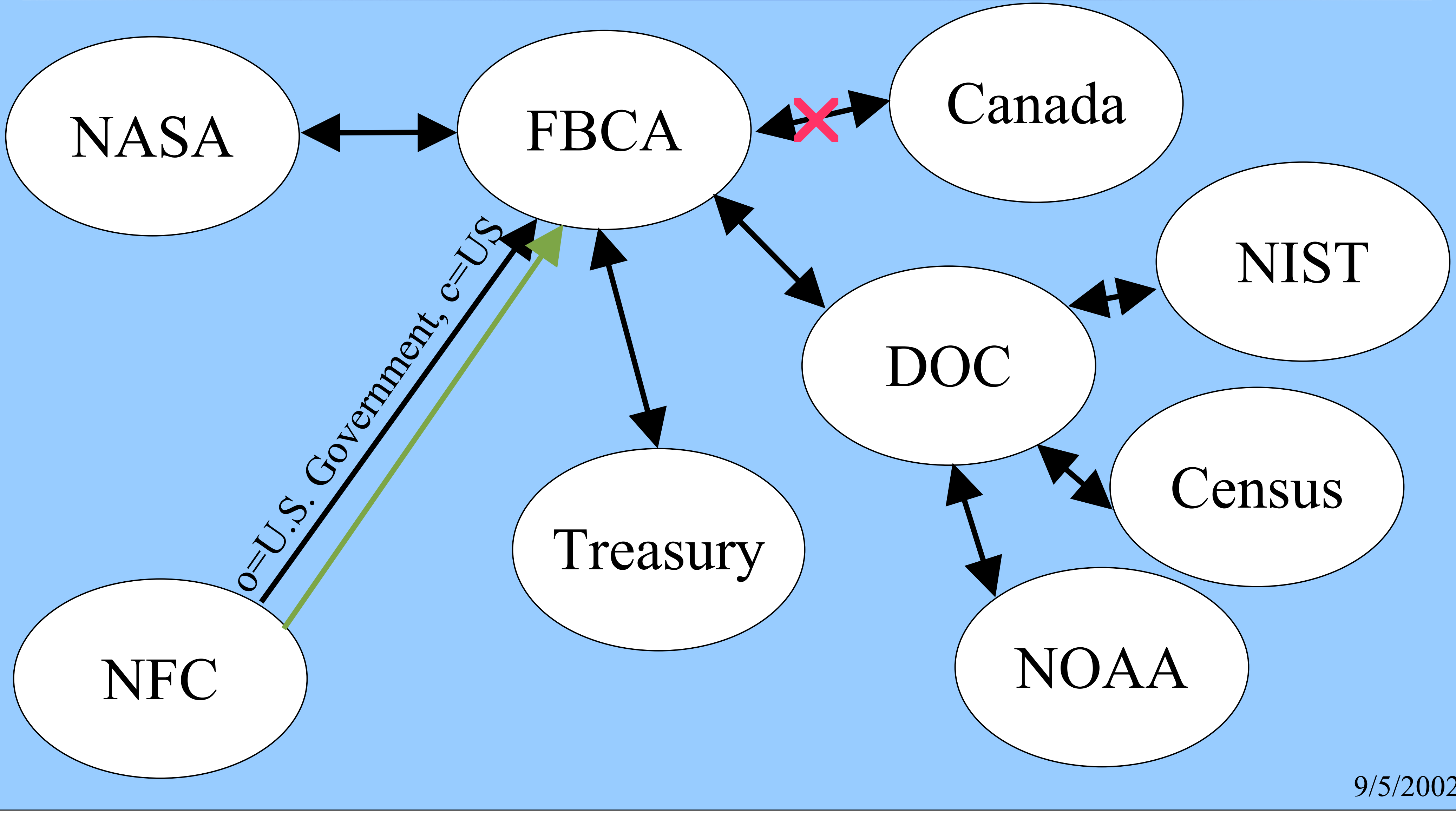


9/5/2002

Why agencies may use name constraints

- Some applications may be more local in scope than others:
  - e-mail is universal, TSP is not.
- Name constraints can be combined with policies to apply different constraints for different applications

Agency use of name constraints

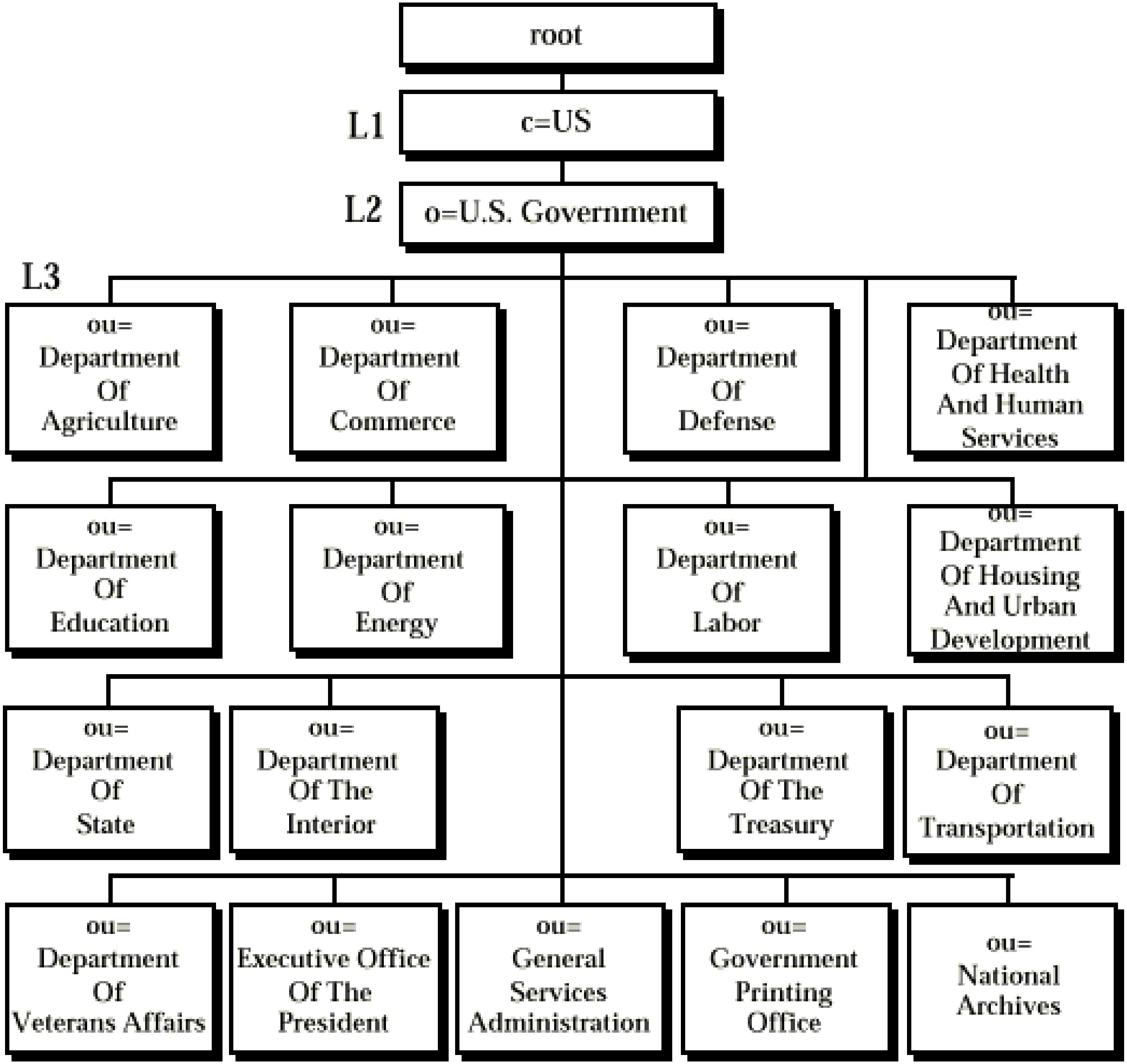


What names should be used?

- Consistent use of names makes imposing name constraints easier.
- For the FBCA each cross-certificate must specify the name space of the subject PKI domain:
  - Need to know the name space of PCA and any other CAs within agency that are cross-certified with PCA
  - Consistent use of names within agency will name cross-certificates smaller

What names should be used?

- For agencies in cross-certificate to FBCA:
  - Should exclude their own domain
  - May limit included domain
  - Consistent naming within domain of interest makes specified permitted subtrees easier.
- The US Gold Schema specifies a consistent naming scheme for U.S. Government.



root

L1 c=US

L2 o=U.S. Government

L3

ou= Department Of Agriculture

ou= Department Of Commerce

ou= Department Of Defense

ou= Department Of Health And Human Services

ou= Department Of Education

ou= Department Of Energy

ou= Department Of Labor

ou= Department Of Housing And Urban Development

ou= Department Of State

ou= Department Of The Interior

ou= Department Of The Treasury

ou= Department Of Transportation

ou= Department Of Veterans Affairs

ou= Executive Office Of The President

ou= General Services Administration

ou= Government Printing Office

ou= National Archives

Recommendations

- New agency PKIs
  - Follow US Gold
- New CAs within an existing agency PKI
  - Maintain consistency with existing CAs within PKI