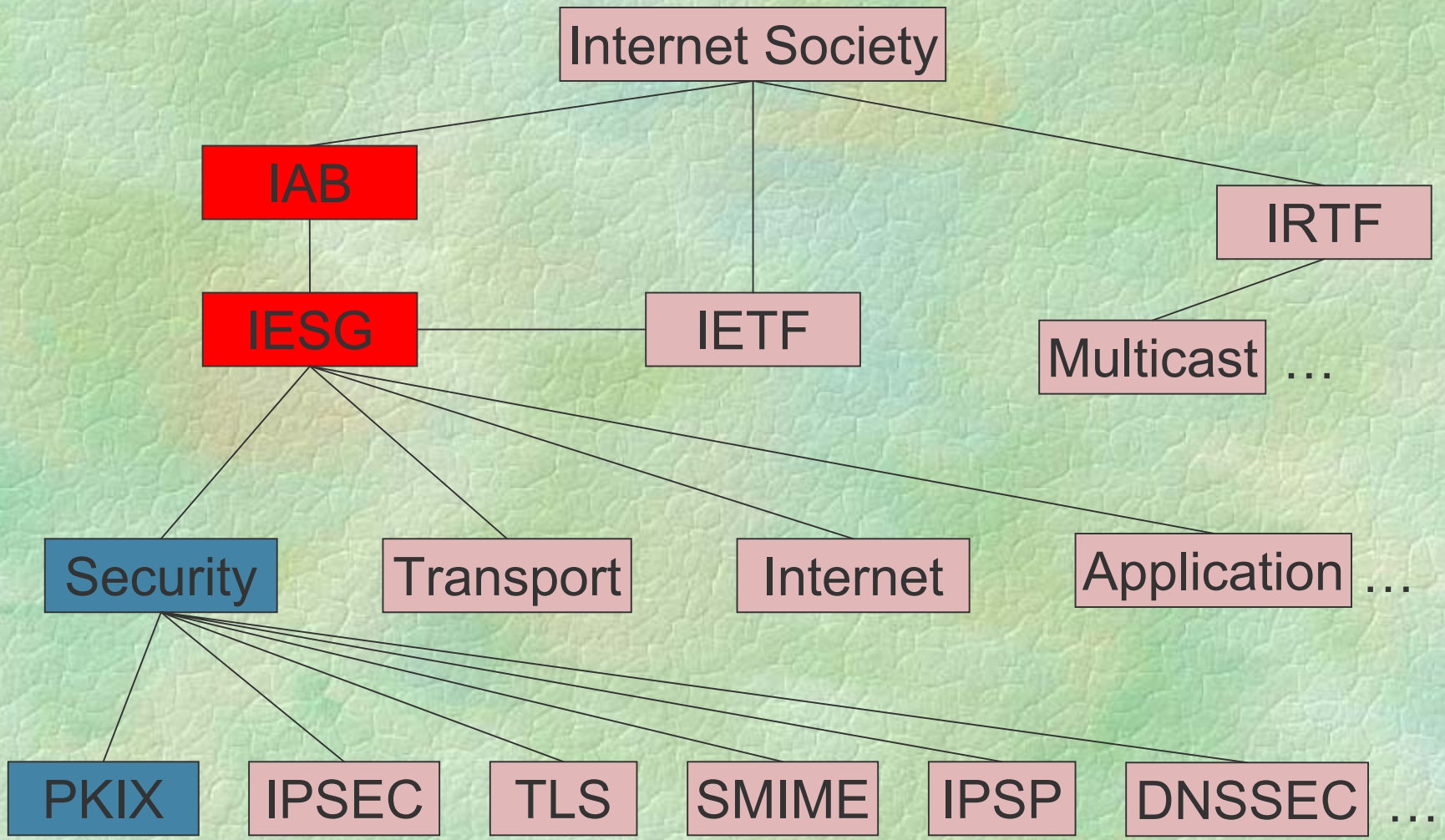
PKIX Standards Status & PKI Directions

Dr. Stephen Kent
Chief Scientist - BBN Technologies
Co-chair: PKIX WG - IETF

What is PKIX?

- The Internet Engineering Task Force (IETF) that addresses generic (vs. application-specific) PKI issues
- Membership is defined by mail list participation, not live meetings, although we do meet 3 times each year, along with the rest of the IETF WGs
- Recent meeting attendance ~100 people, but has been as high as 250
- PKIX = PKI for X.509 (as distinguished from PKI based on any other certificate format)
- PKIX profiles X.509 documents and creates its own PKI standards

The IETF Structure



PKI “Users” in the IETF

- Some working groups that make use of PKI:
  - IP layer security (e.g., VPNs) (IPsec)
  - Secure web access (TLS)
  - Secure E-mail (S/MIME)
  - IPv6 Mobility
  - IPv6 Secure Neighbor Discovery (SEND)
  - IP Secure Remote Access (IPSRA)
  - DNSSEC (bit not an X.509 PKI)
- Note that none of these WGs make use of PKI for legally binding signatures

Major PKIX RFCs

- 3280: Certificate & CRL syntax and processing
- 3281: Attribute Certificate Profile
- 2511 & 2797: Certificate request, renewal, reissue and revocation protocols (CMP, CMC)
- 2560: Realtime certificate revocation status (OCSP)
- 3039: Qualified Certificates
- 3161: Time Stamp Protocol (TSP)
- 2527: CA Policies & Practices (Informational, being revised)

The Next Major PKIX Standard

- Delegated path discovery & validation (DPD/DPV)
  - Motivated by several considerations:
    - Limited bandwidth contexts
    - Limited client computational capability
    - Desire for centralized certificate validation policies management
    - Complexity of certificate path validation
  - Requirements defined: RFC 3379
  - Selected protocol: SCVP
  - Next step: refining SCVP to meet all the requirements

What's Holding PKI Back?

- People often ask what else needs to be done for PKI to "take off"
- But, one should really ask who needs PKI and for what purposes?
- Too often, PKIs have been built (or proposed), without careful attention to
  - the applications that will make use of the technology
  - whether PKI is essential, or just a "gee whiz" option
  - the scope of the PKI that is needed
  - …
- PKI is NOT a silver bullet!
- We probably don't need more standards

Who Needs a PKI?

- A public key infrastructure (PKI) is not intrinsically useful!
- Applications that rely on digital signatures for "broadcast authentication" or non-repudiation, or that make use of key agreement usually need a PKI
- Applications make use of certificates for authentication and/or authorization of users, devices, organizations, processes, …
- A PKI can provide authentication or authorization, or both
- Authentication need not be based on trust; authorization is rarely based on trust

What's Trust got to do with PKI?

- The term "trust" is almost always used when discussing PKIs, yet trust is a separable topic
- Trust is not transitive, not quantitative, not well understood, relative, culturally-biased, …
- Many PKIs can be created that do not require explicit trust
- PKIs can be used to move relationships from the physical world to cyberspace, which is a great way to save money and improve security
- Many people think of trusted third party (TTP) CA's as THE model for PKI, but it's not the only model, and it is often a bad fit for real needs

Authentication & PKI

- Most PKIs are designed to authenticate individuals or computers (e.g., web sites)
- Authentication usually is performed as a precursor to an authorization decision, so it's not just authentication for authentication's sake!
- The form of the name used for authentication is a critical element of the process
- But, who gets to choose the names, what is their scope, and how do you know that the name is the right one for the person or web site?

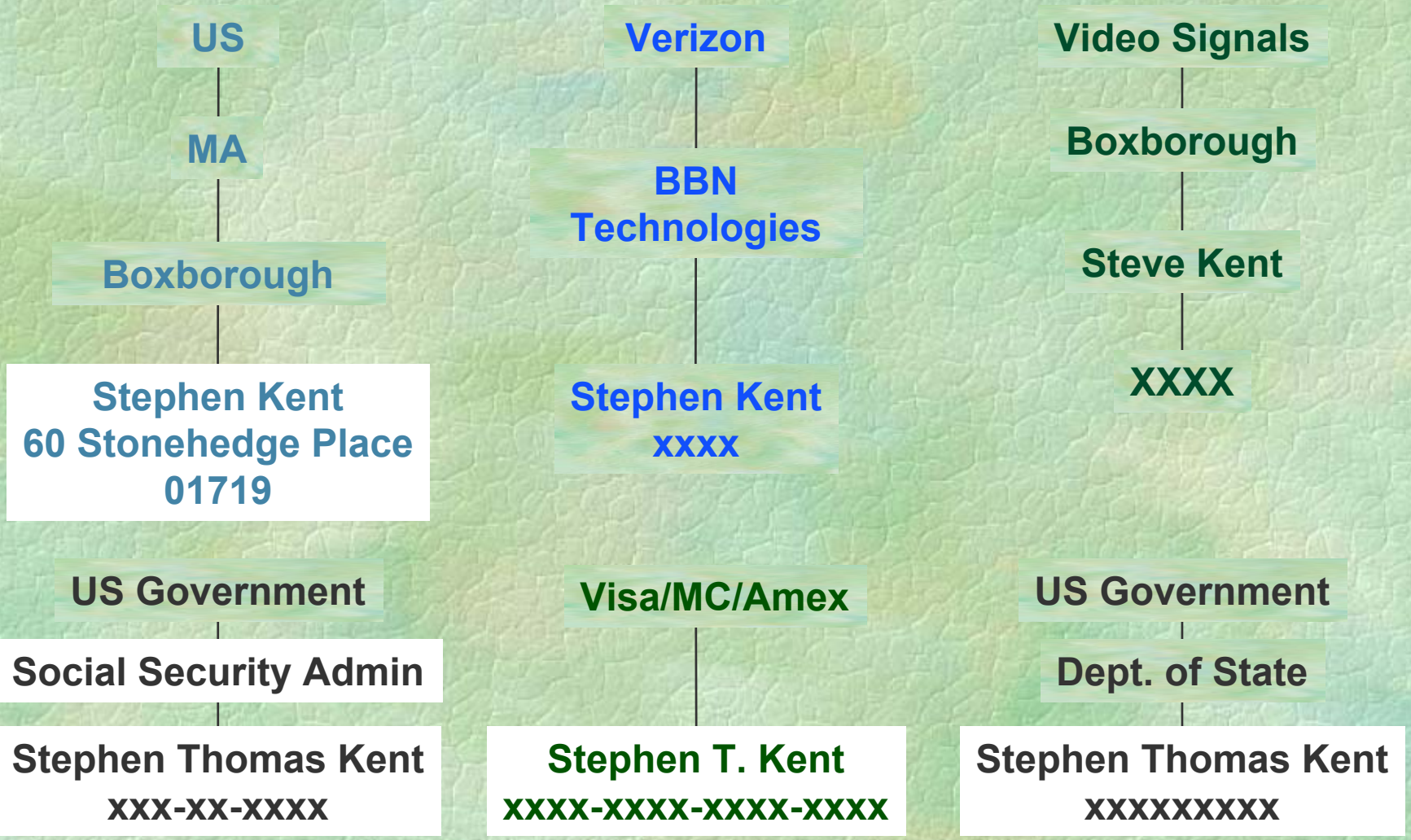
What's in a Name?

- A name is only one attribute of an individual, a contributor to identifying the individual
- Personal identity is a complex concept
- Identity attributes often are inputs to an explicit authorization algorithm, or may be inputs to a human-executed value judgment
- For most types of names, there exist physical world entities who are authoritative, i.e., they manage the spaces from which the names are assigned, and these entities make ideal CAs

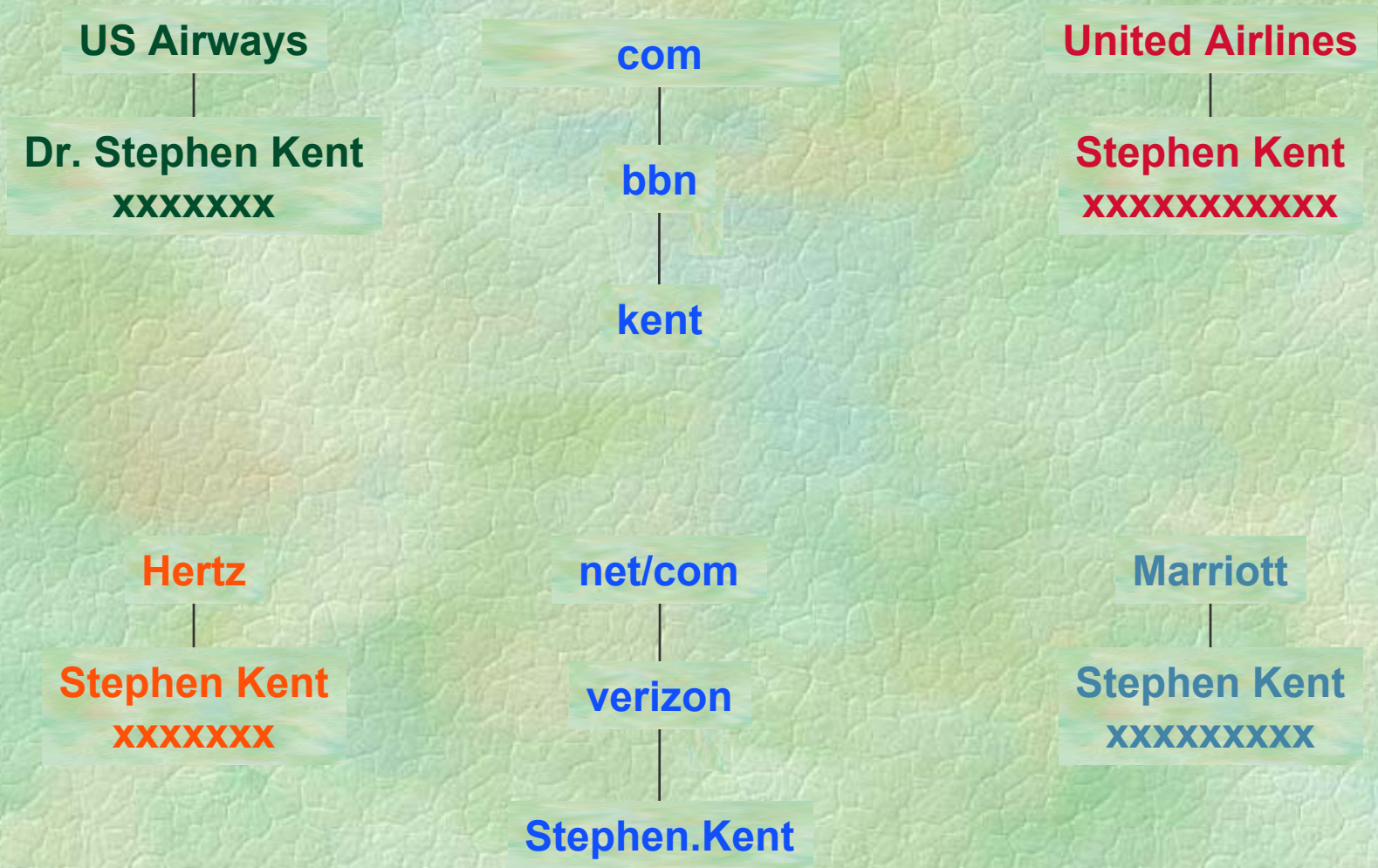
Names in a PKI

- Names in a PKI must be unique relative to a well-defined context, but may not be globally unique
- A CA issuing a certificate must ensure uniqueness among subject names in the certificates it issues
- It's easy to make a name globally unique: just add qualifiers, e.g., ID numbers
- However, most names that are globally unique are not globally meaningful!
- Most names are meaningful only in context
- Relying parties problems need meaningful names for authorization decisions or value judgments
- People have multiple identities!

Personal Example Name Spaces



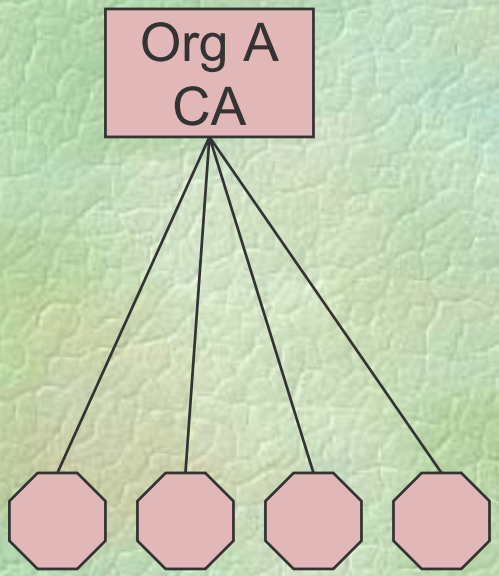
More Name Space Examples



CAs, Names, and Trust

- Individuals typically have lots of names, each of which can be made globally unique, but most of which are meaningful only in well-defined contexts
- Many organizational names are only locally unique (trademarks are scoped!)
- Transactions should use names that are meaningful to the participants
- As we move physical world relationships to cyberspace, we often can make use of the same names, and existing organizations can act as CAs
- Such CAs do not require explicit trust, since they are authoritative for the names they assign
- The hardest part of being a CA is the RA function, which these organization have already performed!

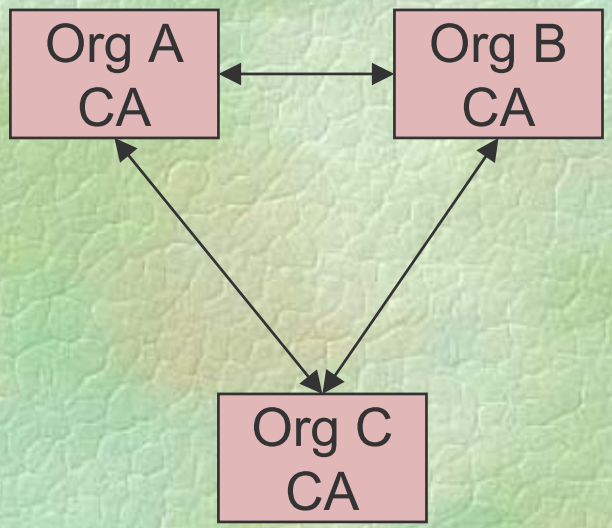
An Organizational PKI



CA operations can be out-sourced when authoritative organizations are PKI-challenged

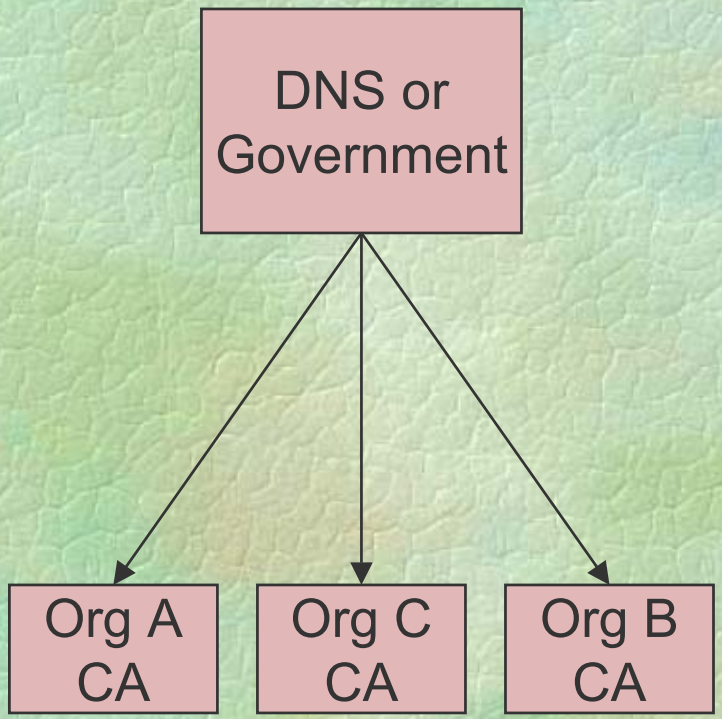
- A PKI for use only within the organization
- Organizations: companies, colleges, professional societies, …
- Subjects are employees, students, members, clients, …
- Subject names are drawn from existing databases
- A PKI for secure e-mail, web access, single signon, …

An Inter-Organizational PKI



- Connects organizational PKIs
- Direct cross-certification using NameConstraints, avoids "trust" issues, just recognizes organizations as authoritative for name spaces
- Helps if organizations choose their CA names wisely
- $O(n^2)$ cross certificates, but often that's OK
- Users within each organization see it as a root

Large Scale PKIs



- To avoid $O(n^2)$ cross certification, need a CA with broad scope, e.g., an organization that is authoritative for many names
- The DNS provides one obvious choice
- Government agencies are good candidates for individuals and some types of organization names
- The Japan Government PKI is an excellent example

Advantages of Authoritative CAs

- Clear scope for a CA's authorization
- No complex trust models are required
- Easy certificate validation and revocation (often no need to propagate revocation info)
- Liability limited to the application context
- Lower costs than a TTP CA
- Assurance appropriate to the application context
- Clear policy scope (vs. a TTP CA)
- Islands of PKI are OK for many contexts
- But, user software must make it easy to manage multiple certificates, preferably automatic

Conclusions

- We don't need more PKI standards to enable PKI use
- PKIs are about more that legally binding signatures
- Explicit trust is unnecessary for many PKIs
- Names in certificates must be contextually meaningful, or they will be dangerous
- Users cannot understand or manage complexity in PKIs (the "VCR programming Principle")
- TTPs have been important in promoting PKI, but authoritative CAs are preferable, to minimize complexity and maximize security
- Large scale CAs can be operated by governments, DNS TLD managers, etc.
- Organizations can safely cross certify, without "trust"

Questions