multi-domain PKI interoperability
Straw man proposal as BCP

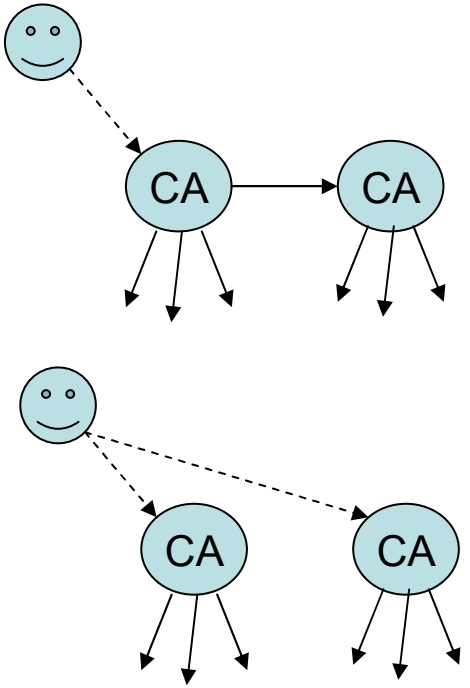
4th Aug, 2004

Challenge PKI Project

Masaki SHIMAOKA

At present

- Various PKIs in the world
  - Many architectures and many policies
    - Hierarchy PKI, Bridge CA, etc.
    - Japanese e-sig law, Korean e-sig act, etc.
- Some PKIs need to be assembled
  - Organizations integration
  - Companies merging
  - International cooperation
- Also various assembling method
  - Cross-certification: CA to CA
    - EE does not need to trust another trust anchor.
    - Single Trust Point Model
  - EE trusts also other PKI (like trust-file PKI)
    - EE trusts multiple trust anchors.
    - Multiple Trust Point Model
- Both is used actually



Issues

- How do we make it interoperable?
  - Cross-certification, or adding trust anchor?
  - Multiple trust point model is easier approach.
    - Is it perfect?
    - No. Cross-certification is stricter method to assemble PKIs.
- What PKI should we make interoperable?
  - To recognize the boundary of PKI
- If you need to make interoperable more than three PKIs?
  - It is too complex

Impact

- Cause the PKIs which is not interoperable
  - Should PKI-X that trusts another PKI-Y by cross-certification also trust the other PKI-Z by cross-certification?
  - Or should it delegate to EEs so that trusts PKI-Z directly?
  - Except for the PKIs that has same architecture and same policy

My proposal

- Guideline for interoperability as BCP about:
  - Showing the typical model for assembling PKIs.
  - Showing a merit/demerit of the models.
  - Preventing to apply the misleading model.

  - Now, it is just my straw man proposal for discussion about these issues.

- Any other proposal?

What practice

- Establish the concept of PKI domain as the boundary of PKIs
  - Different architecture and/or different policy
- Show the typical model to assemble them
  - Model achieving sufficient interoperability
- How to consider the interoperability of multi-domain PKI
  - How to be trusted by the third party else subscriber
  - How to maintain cross-certificate pair
  - How to maintain trust anchors (in trust-file PKI)
  - How to operate the directory system for PKI
  - How to validate the certification path

- Many practices are led from “cross-certification vs. trust-file PKI.”

So far

- Presentation in PKIX at 57th Vienna
  - http://www.ietf.org/proceedings/03jul/slides/pkix-9/index.html
  - Leaded from some PKI interoperability project
    - Japanese GPKI, Asia PKI Forum, and Challenge PKI
  - In that time I had started writing this I-D.
- Closing of PKIX WG
  - This was declared as "out of scope" in PKIX WG.
    - Too wide? – May be YES.
    - My proposal itself does not cover all the remaining issues.
    - We need still some work items are remaining.

Approach

- Define the terminology for multi-domain PKI interoperabililty
  - Basically according to RFC 2828.
- Show the typical assembling method for different PKIs
  - Cross-certification, subordination, adding trust anchor (like trust-file PKI)
- Define the requirements for a set of PKI needed to assemble
  - As PKI domain
- Show the suitable models for participant to multi-domain PKI
  - As Single domain PKI
- Show the real models of assembled PKI
  - As multi-domain PKI

Concept of PKI domain

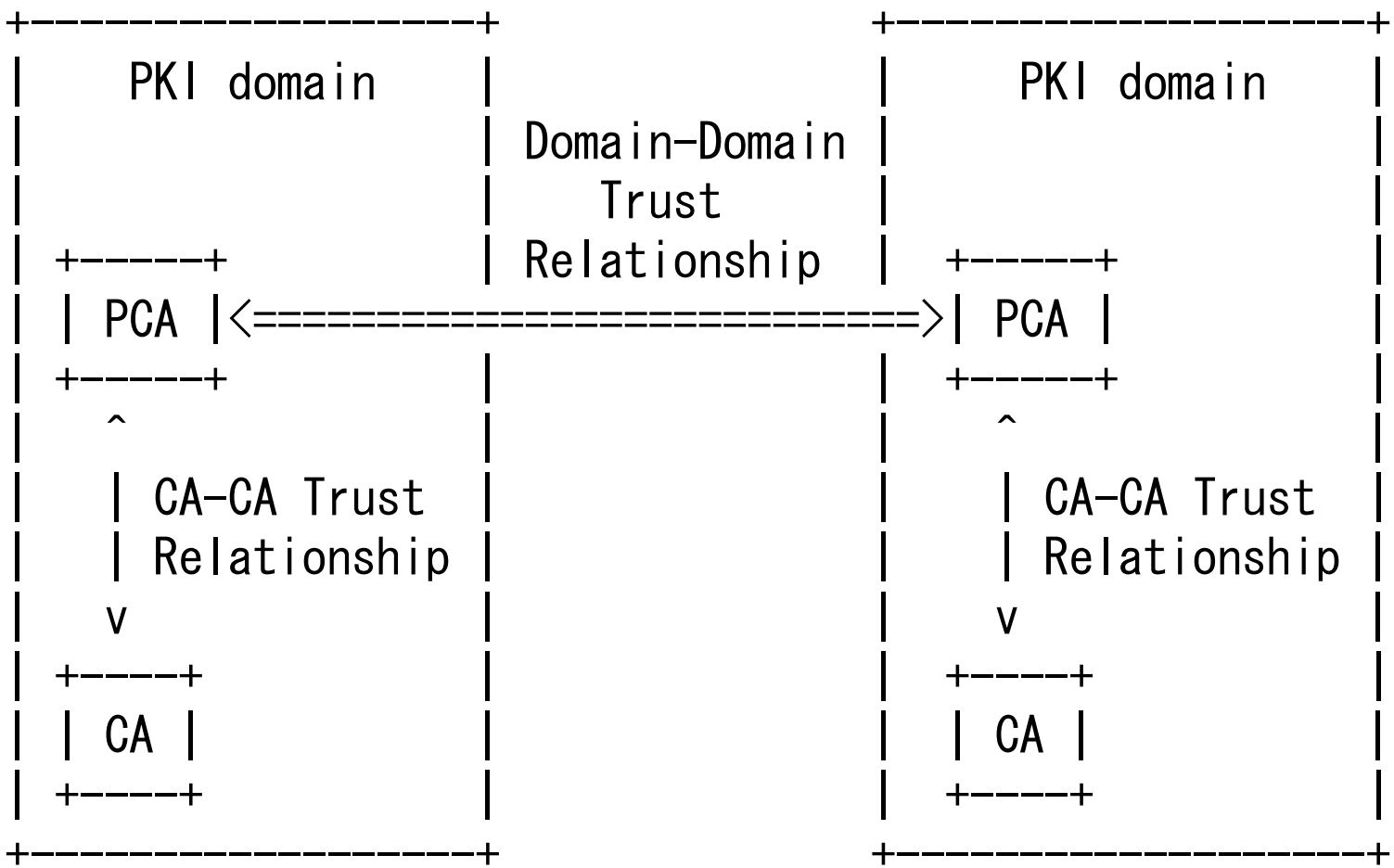


Table of Contents

Future plan

- Till 61st IETF
  - Recruiting co-author
  - Expert review with other WG concerning PKIX
  - Release -04 with co-author
- 61st IETF @ Washington DC or later
  - Last call for submitting to IESG
  - Make a presentation
    - But did not decide yet where WG.
- After 61st IETF
  - IESG review

My question

- Should we establish the consensus for such multi-domain PKI?
- Is there somebody who has doubt for this ambiguity?

- About my proposal:
  - What should we consider in addition?
  - What is unnecessary?
- Or, should we try another approach, not my proposal?

Let me know

- How many people or what kind of people have doubt or motivation for these problems?
- For achieving the better interoperability, we need another view based on the other architectures.
  - Our motivation is almost based on the experience of Japanese GPKI, which is Bridge CA architecture against trust-file PKI.

Challenge PKI Project

- My activity is contributed by Challenge PKI Project in NPO JNSA
  - Japan Network Security Association
  - http://www.jnsa.org/mpki/

- *We currently have a very complex PKI; multi-domain and multi-vendor PKI, vague standards and various implementations.*
- *Complex PKI is inevitable and imperative because it results from the growth of PKI, and it requires interoperability between domains and vendors.*

- *Our goal is to ensure PKI interoperability and to contribute actively to development and spread of reliable PKI applications in future electronic society.*