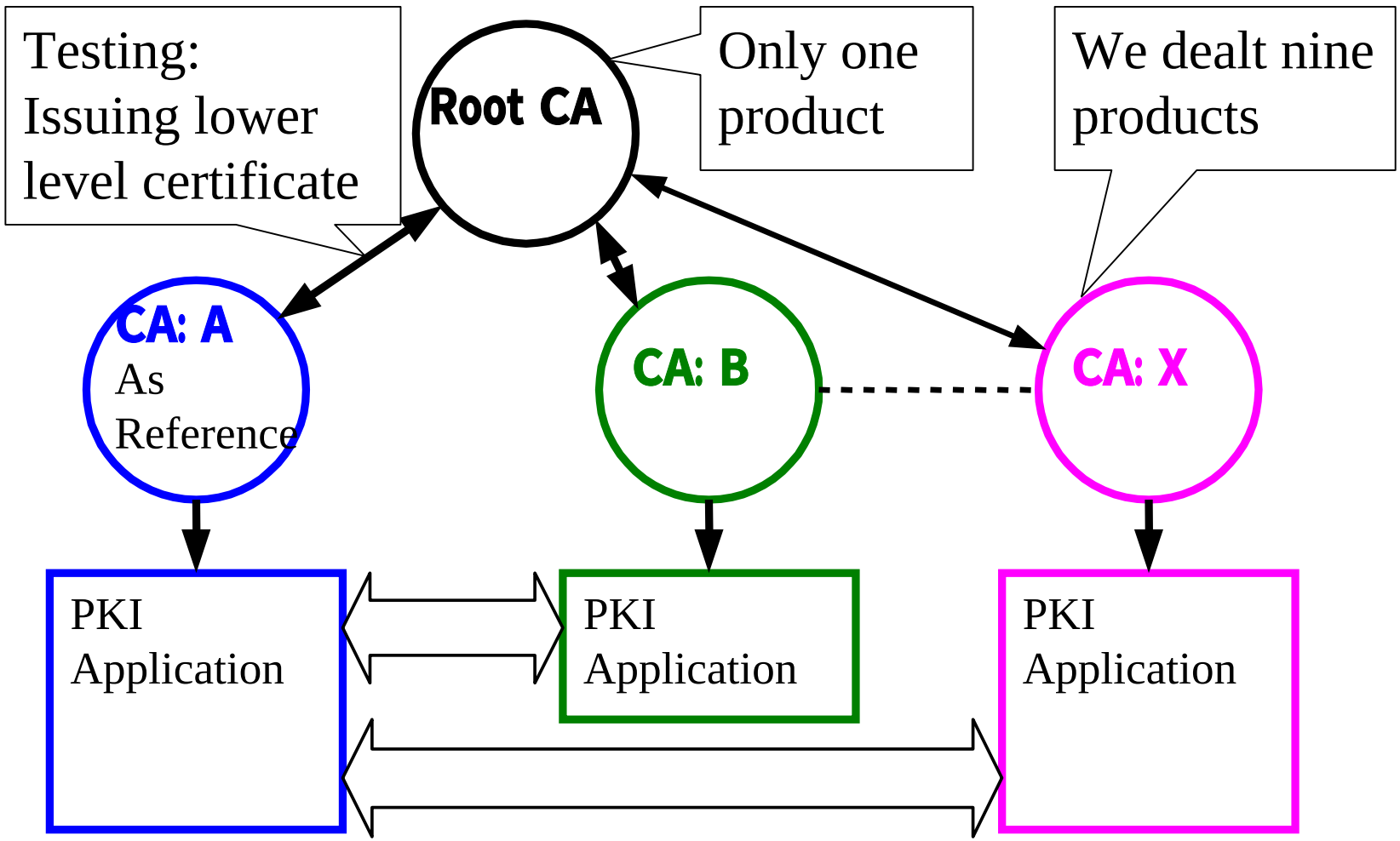
Specification Problem around Multi PKI domain

--- Experience in Challenge PKI 2001 ---

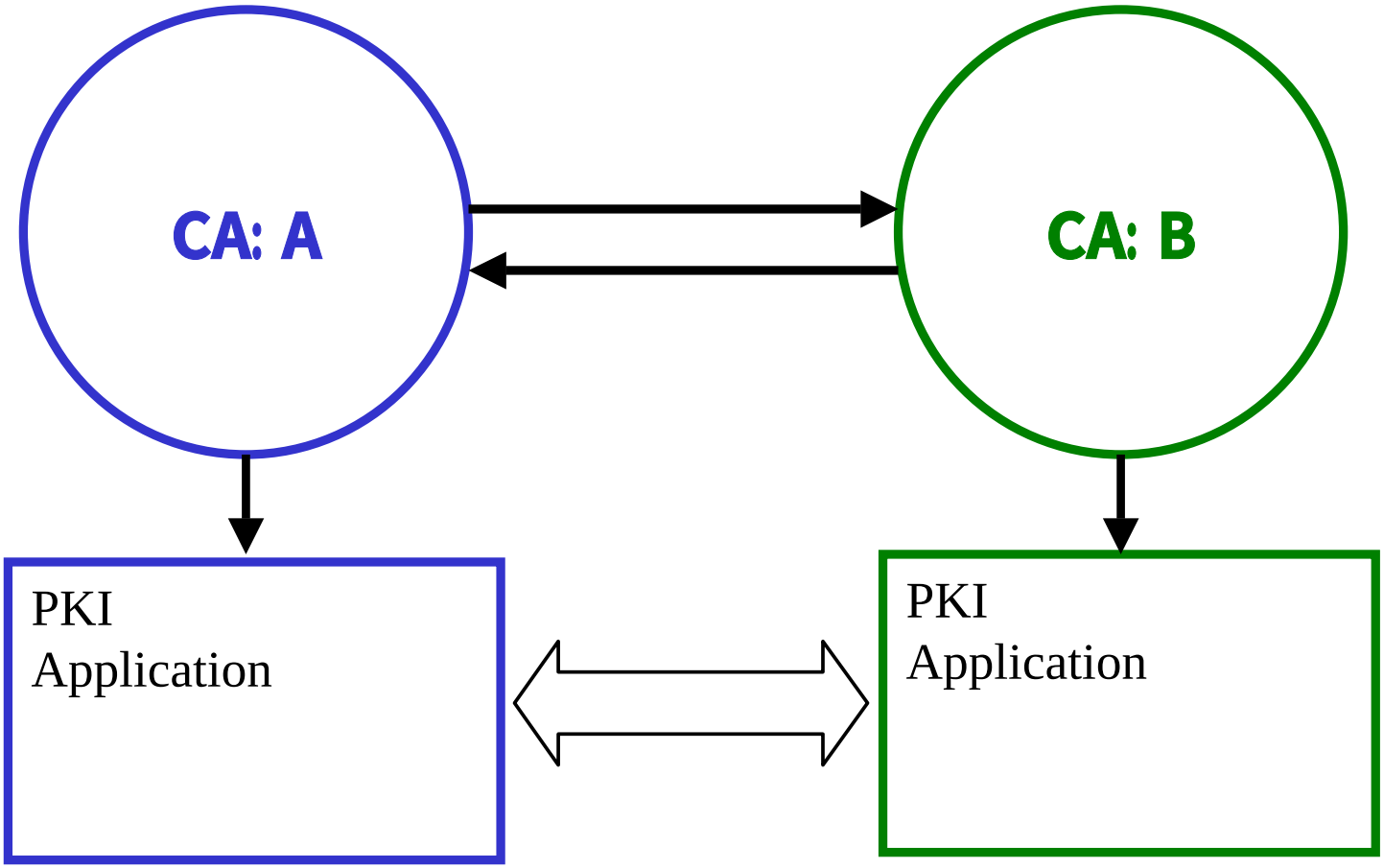
Ryu Inada <Ryu.Inada@fujixerox.co.jp>
As representative of
NPO Japan Network Security Association
Sponsored by IT Promotion Agency, Japan

July 17th 2002, 54th IETF Yokohama, Japan

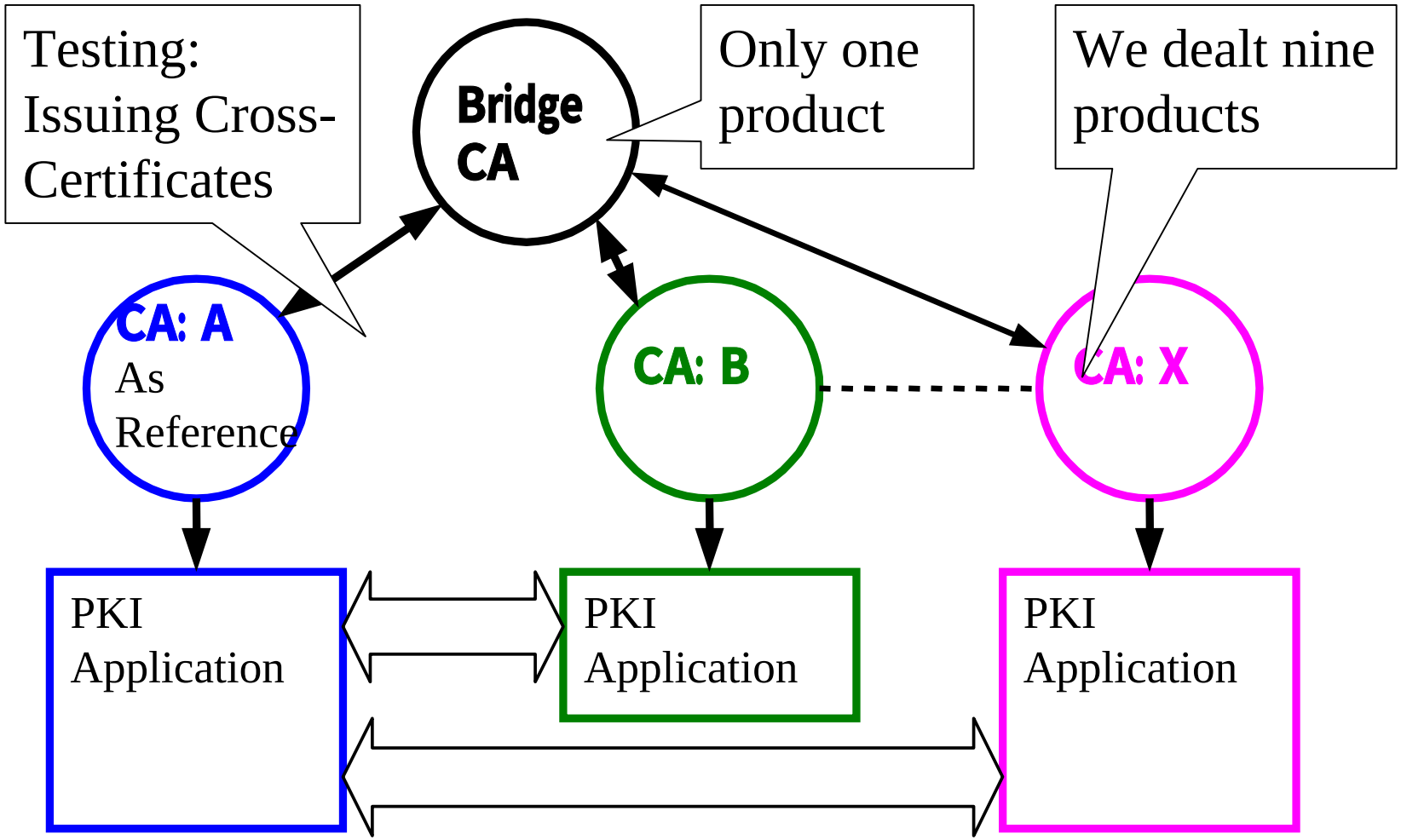
Testing environment: Strict Hierarchy model



Testing environment: Mutual Cross Certification Model



Testing environment: Bridge Model



Based on Japanese Government's GPKI profile.

Clarification is necessary !!

- Path Validation issues:
  - KeyIdentifier
  - Critical-flag
  - CRLDP/AIA evaluation order/rules.
  - CRL/ARL specification for CRLDP
- Policy Mapping issues:
  - Some CA can issue Cross Certificate
  - But critical-flag is still ‘non-critical’
  - CRL/ARL extensions are not supported

Other Findings: Based on RFC 3280

- DER encoding
  - Some CAs are using BER encoding for keyUsage field.
- DN comparing
  - UTF8String problem, case-sensitive problem, etc.
- DirectoryString order
  - There are two patterns.
- serialNumber
  - Definition is insufficient.
- basicConstraints.cA
  - Some End Entity Certificates include basicConstraints
- basicConstraints.pathLenConstraint
  - It should be used when CA is True.
- keyUsage
  - DigitalSignature, KeyEncipherment
- Issuing Distribution Point
  - It must be critical on Multi-PKI environment.
  - And client must be recognize this extension.

Related URLs:

- Challenge PKI 2001
  - http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.html
  - (Sorry Japanese only, English Version will be available Sep/2002)

- IPA
  - http://www.ipa.go.jp/ipa-e/index-e.html
- JNSA
  - http://www.jnsa.org/english/e_index.html

Next ?

- To clarify of requirements of Multi-Domain PKI environment.
- To feedback additional profile for Multi Domain PKI to son of RFC 3280 ?
- Any interest on this issue, please join !
  1515 - 1600 Informal meeting @ Room 514
- Or please send mail to multi-domain-pki@jnsa.org
- Any comments / suggestions are welcome.