CMC Extensions: Server Key Generation
draft-turner-pkix-cmc-serverkeygeneration-00

IETF 81 - PKIX

Jim Schaad
Sean Turner
Paul Timmel

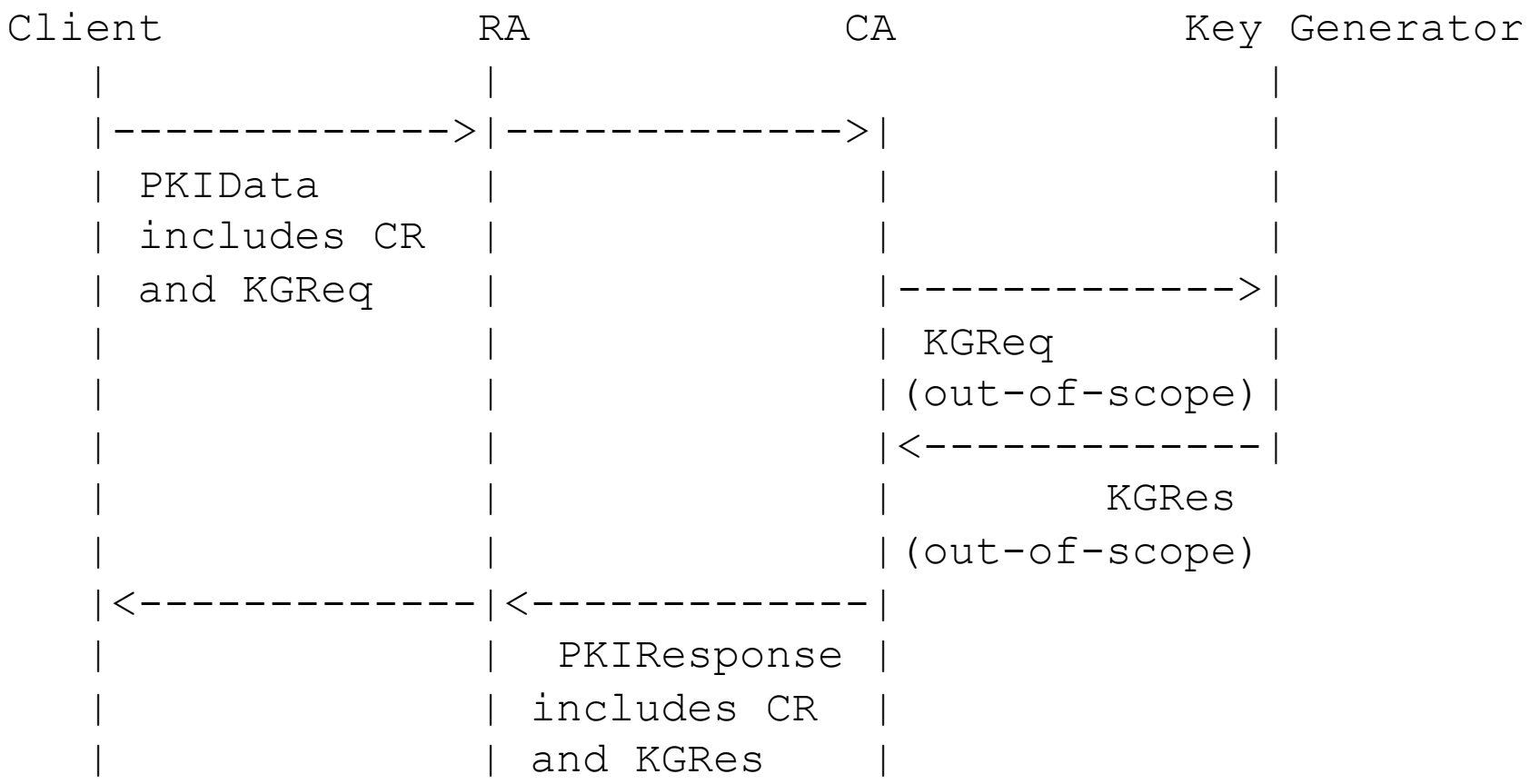
Concept

- Define a set of CMC controls to support server-side generation of keys.
- Based on a expired PKIX draft: draft-ietf-pkix-cmc-archive.
- Why:
  - Clients may have poor, unknown, or non-existent key generation capabilities.
  - Some environments want key recovery.

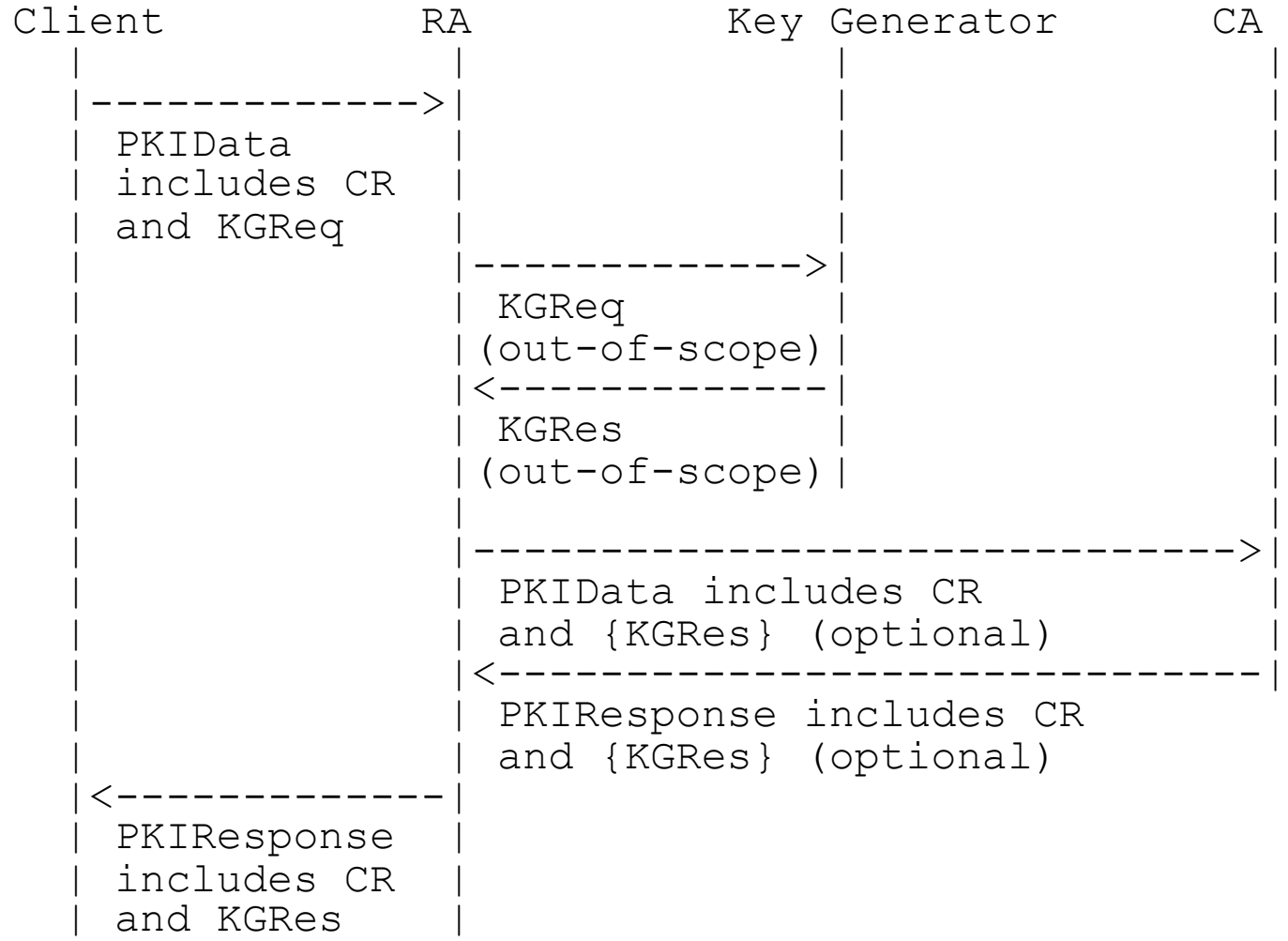
Scenarios

- Requestors may have certificate, but they might not. Supports:
  - Shared Secret for Authentication and Key Protection
  - Shared Secret for Authentication and Uncertified Key for Protection
  - Certificate for Authentication and Uncertified or Certified Key for Protection

Key Generators (1)



Key Generators (2)



Some Issues

- As defined now, the request includes the certificate template. Maybe it shouldn't – maybe it should refer to certificate request from the control.
- As defined now, the mechanism to protect the response is requested using an Algorithm Identifier (OID + parameters). The alg parameters are complex as compared to everything but RSASSA-PSS. Maybe it should be an attribute instead?
- Is the WG willing to adopt this draft?