Multicast Security with Authentication, Authorization, and Accounting (AAA)

George Gross, IdentAware™ Security
gmgross@IdentAware.com

IETF-58, Minneapolis, MN

November 10th 2003

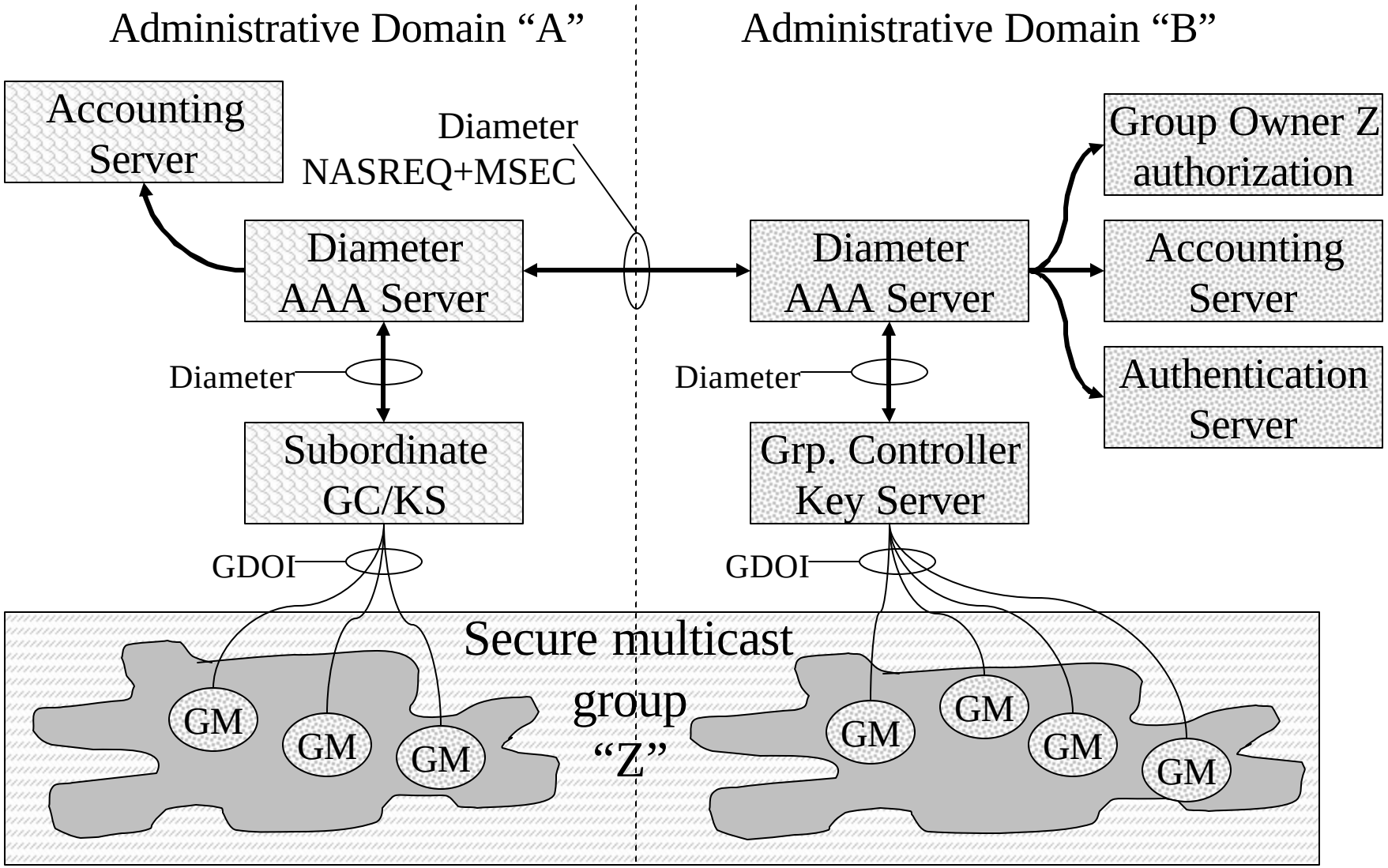
What motivates MSEC/AAA?

- Large-scale secure multicast groups straddle administrative/business domain boundaries
- AAA enforces contractual relationships, generates data usable for service accounting
- Allows Service Provider to securely control their multicast transit routing service
- Enables dynamic MSEC groups with the Service Provider AAA as the broker

Relevant Background Reading

- RFC3588, Diameter base protocol spec
- RFC2904, generic authorization framework
- NASREQ Diameter application
  - ietf-draft-aaa-diameter-nasreq-13.txt
- next rev of generic policy token draft
  - msec-gspt-04.txt
  - missed the ID cut-off

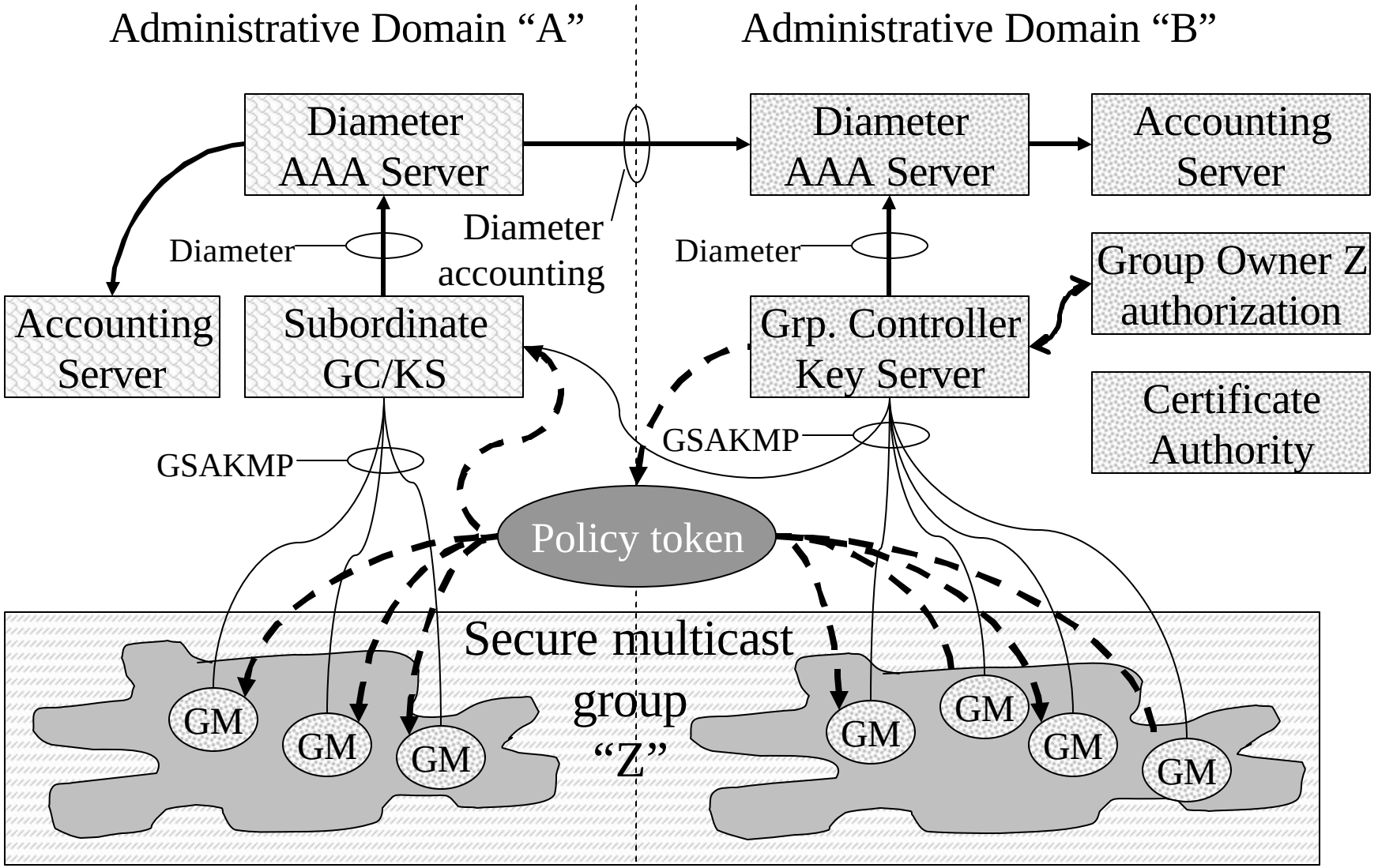
GDOI *Roaming Pull* AAA Model



Observations about GDOI/AAA

- Can leverage existing IKE/ISAKMP AAA
  - Q: does the group member have a NAI?
  - Reasonable design: extend NASREQ Diameter application to handle GDOI
- Undefined how to add a S-GC/KS to group
- Issue: currently no way to separate KS from the S-GC role if the S-GC domain is not trusted with the group's encryption key

GSAKMP *Push* AAA Model



GSAKMP/AAA Observations

- PKI based authentication only, no NAI
- Multicast policy token encodes membership authorization, acts as AAA service ticket
- Diameter back-end used for accounting
- Does not fit Diameter NASREQ model
- Like GDOI, can not withhold group key from S-GC in partially trusted domain

Future MSEC/AAA directions

- Need to separate the S-GC and key server roles in both GSAKMP and GDOI
- Introduce “generic” policy token attributes to encode multiple service authorizations
  - nesting the tokens will avoid layer violations
  - multicast PT is scalable, but it is not part of GDOI today, is this feasible to add?
- Long-term: Diameter extensions for MSEC