CoreStreet
REAL TIME CREDENTIALS

DISA Distributed OCSP Project

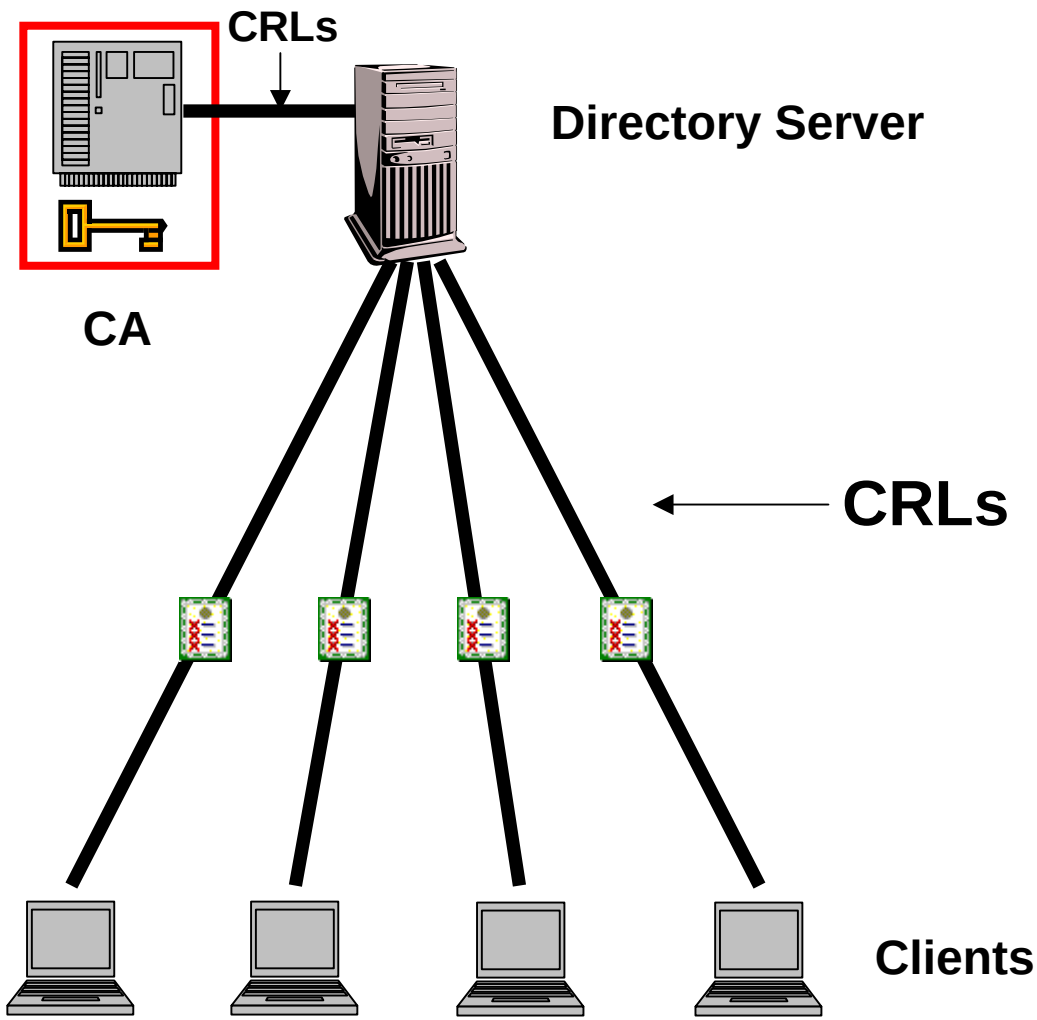
Architecture & Deployment

CoreStreet
REAL TIME CREDENTIALS

Certificate Revocation Choices

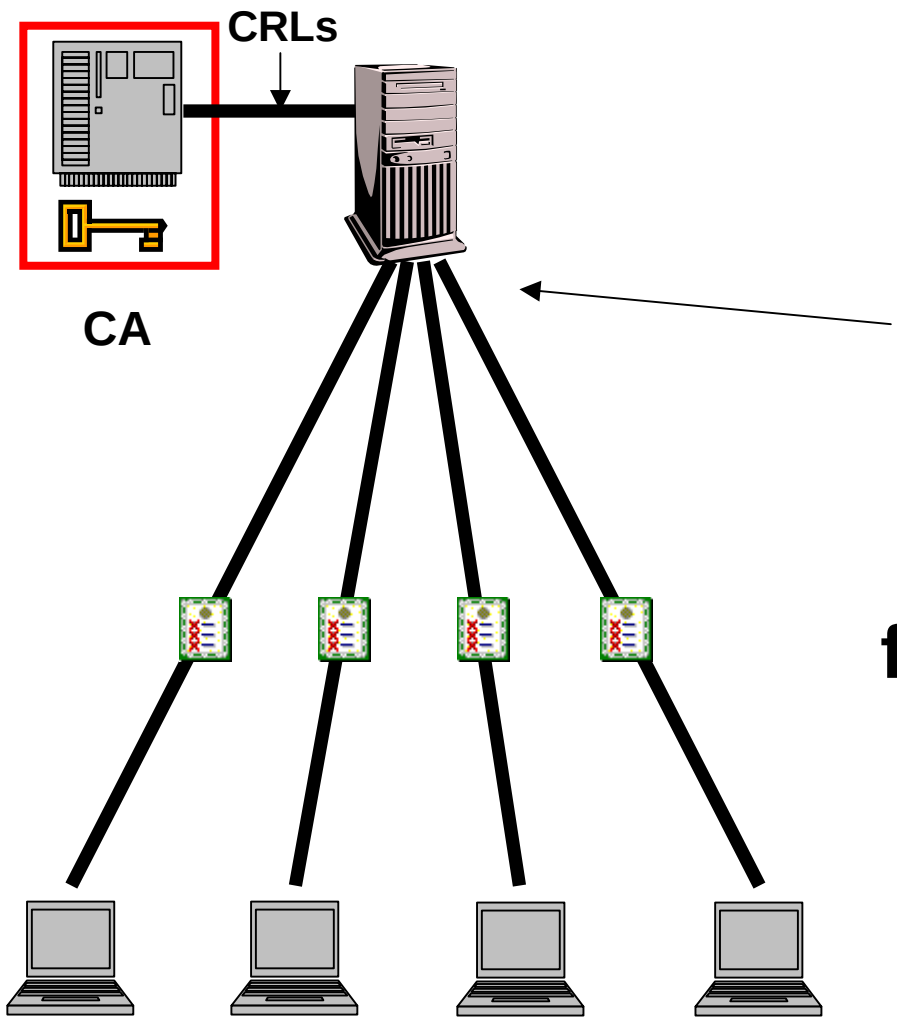
- **Certificate Revocation Lists (CRLs)**
- **Online Certificate Status Protocol (OCSP)**
  - Traditional OCSP
  - Distributed OCSP

CRLs



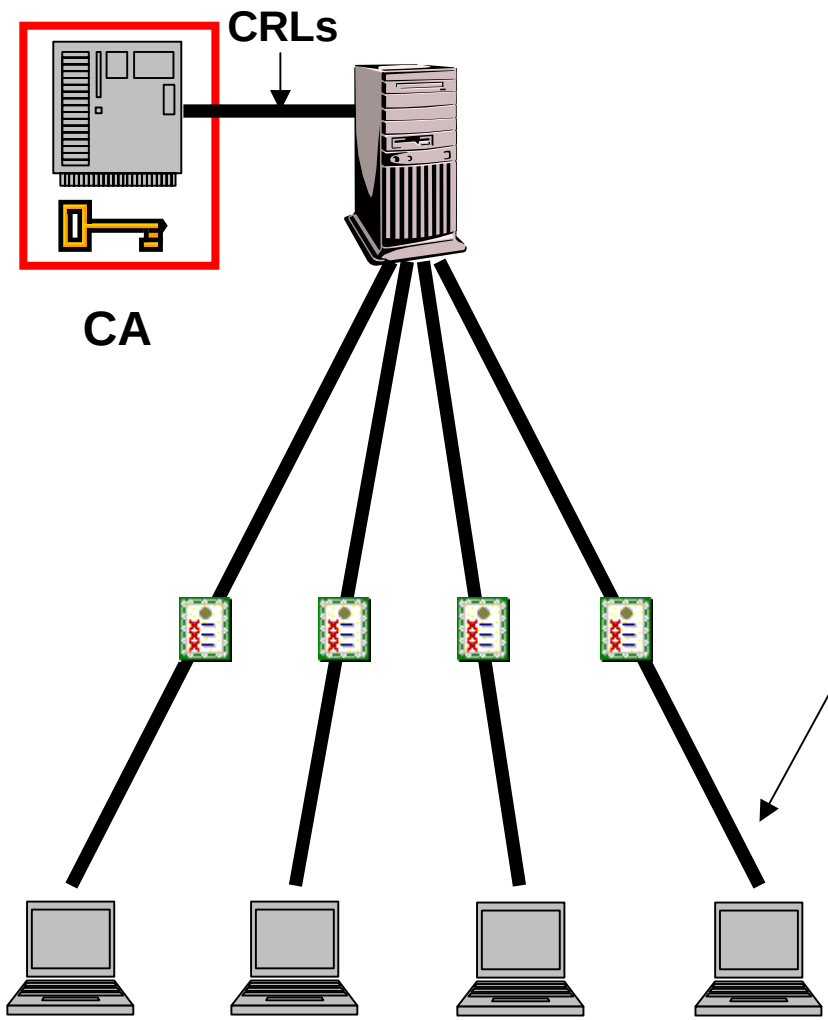
= requires trust
(physical and data security)

CRL Problem #1: Scalability



19 DoD CRLs (20MB)
x
4 million clients
=
80 Terabytes per day from directory service

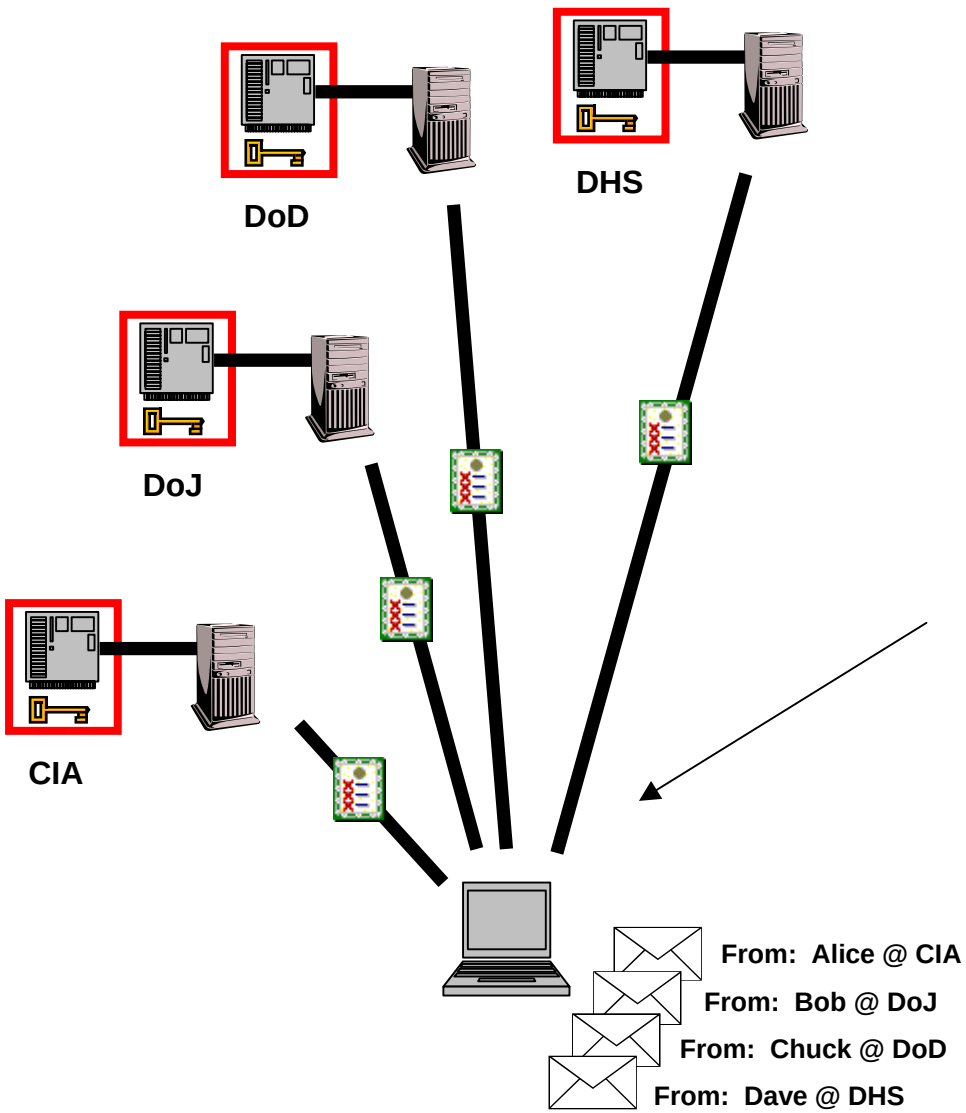
CRL Problem #2: Performance



Class 3 CA-3 CRL (5MB): 14 minutes over 56kbps dial-up or wireless

All 19 DoD CRLs (20MB): One hour

CRL Problem #2: Performance

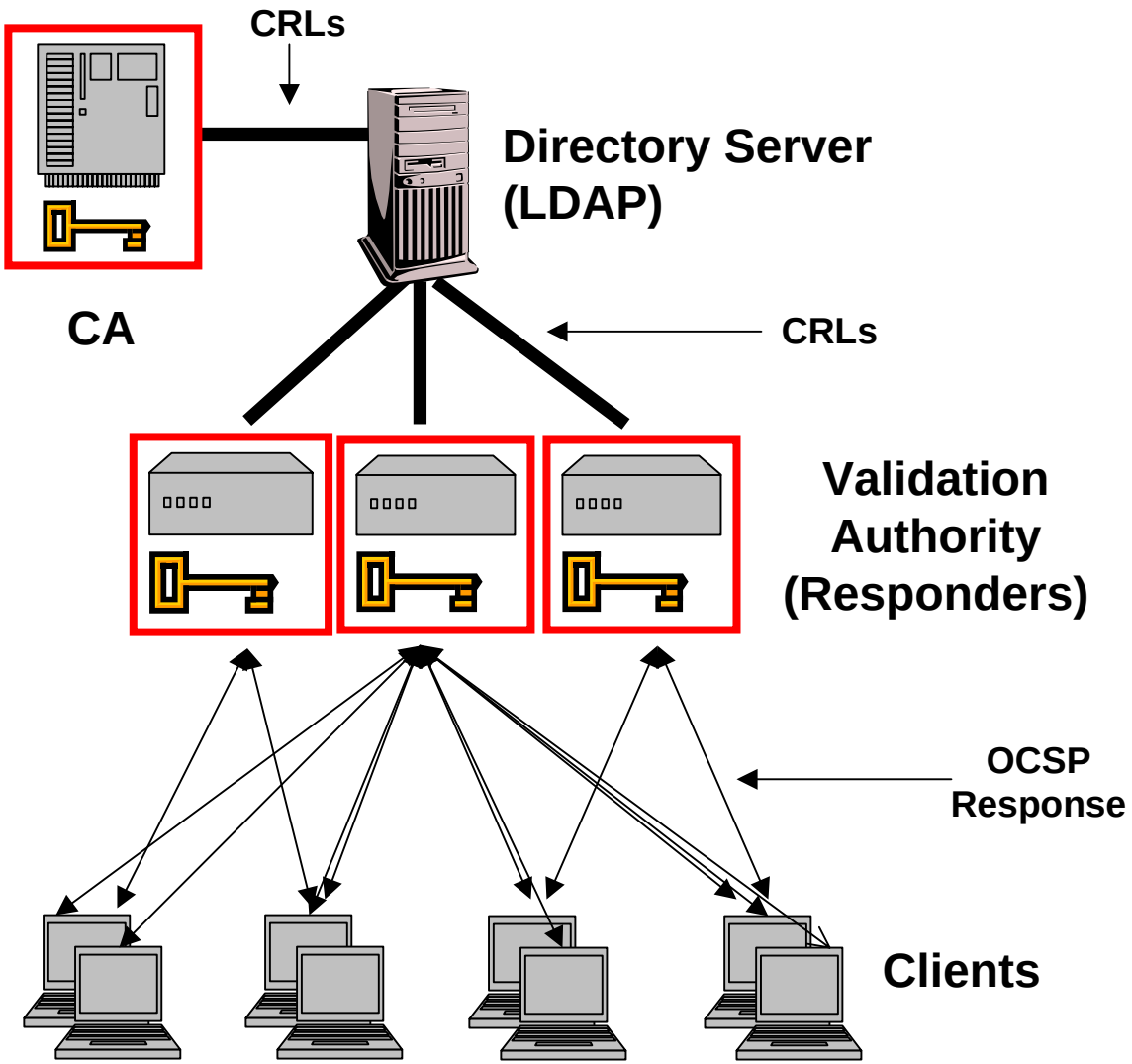


Need CRLs for all accepted certificates:

Federation explodes performance problem

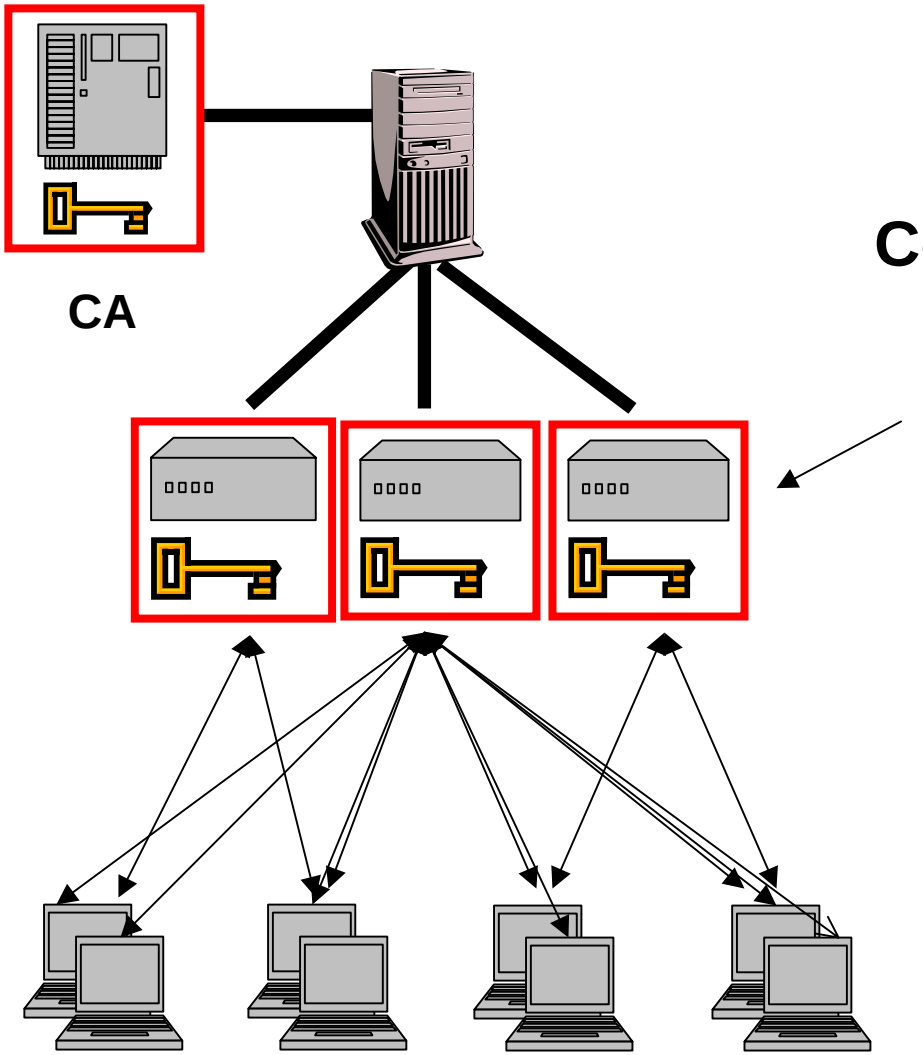
CoreStreet
REAL TIME CREDENTIALS

Traditional OCSP (T-OCSP)



= requires trust
(physical and data security)

T-OCSP Problem #1: Security

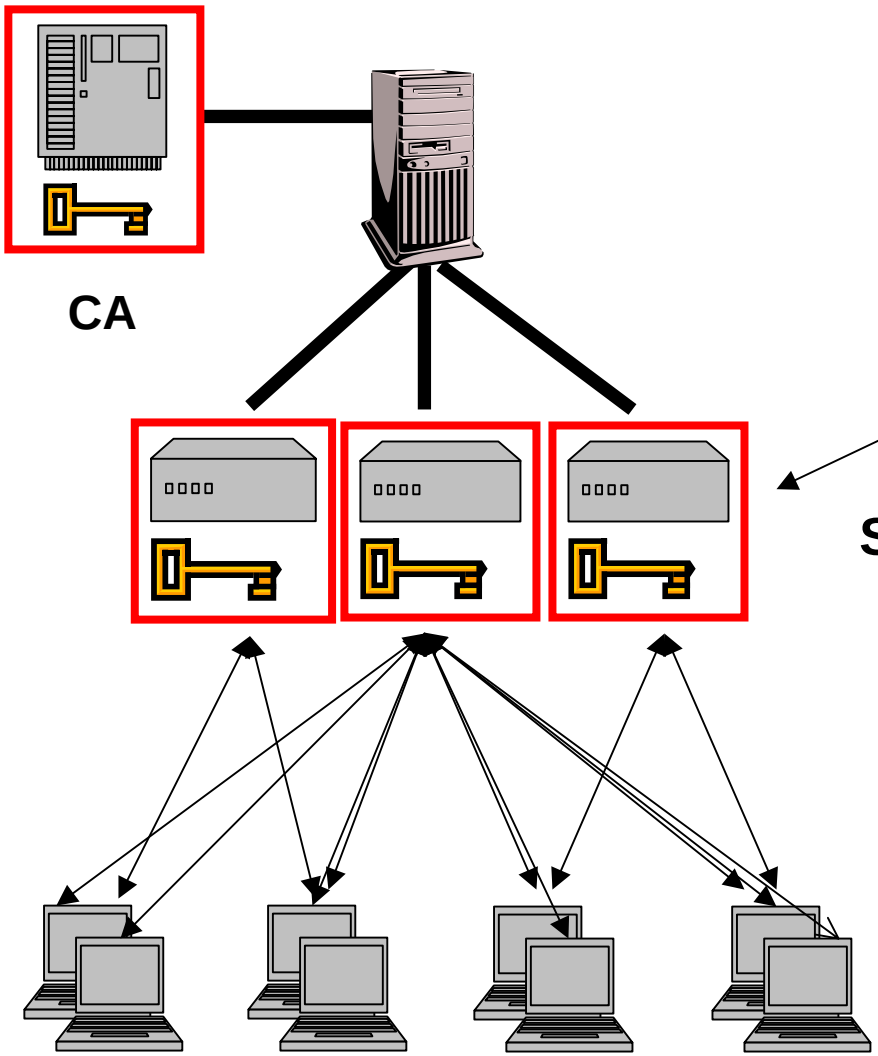


Compromise <u>any</u> responder, unrevoke <u>any</u> certificate.

20 online responders = 20 keys to compromise

= requires trust (physical and data security)

T-OCSP Problem #2: Deployment



Each responder requires:

Server: $5k

HSM: $20k

Secure Hosting: $65k - 125k / year

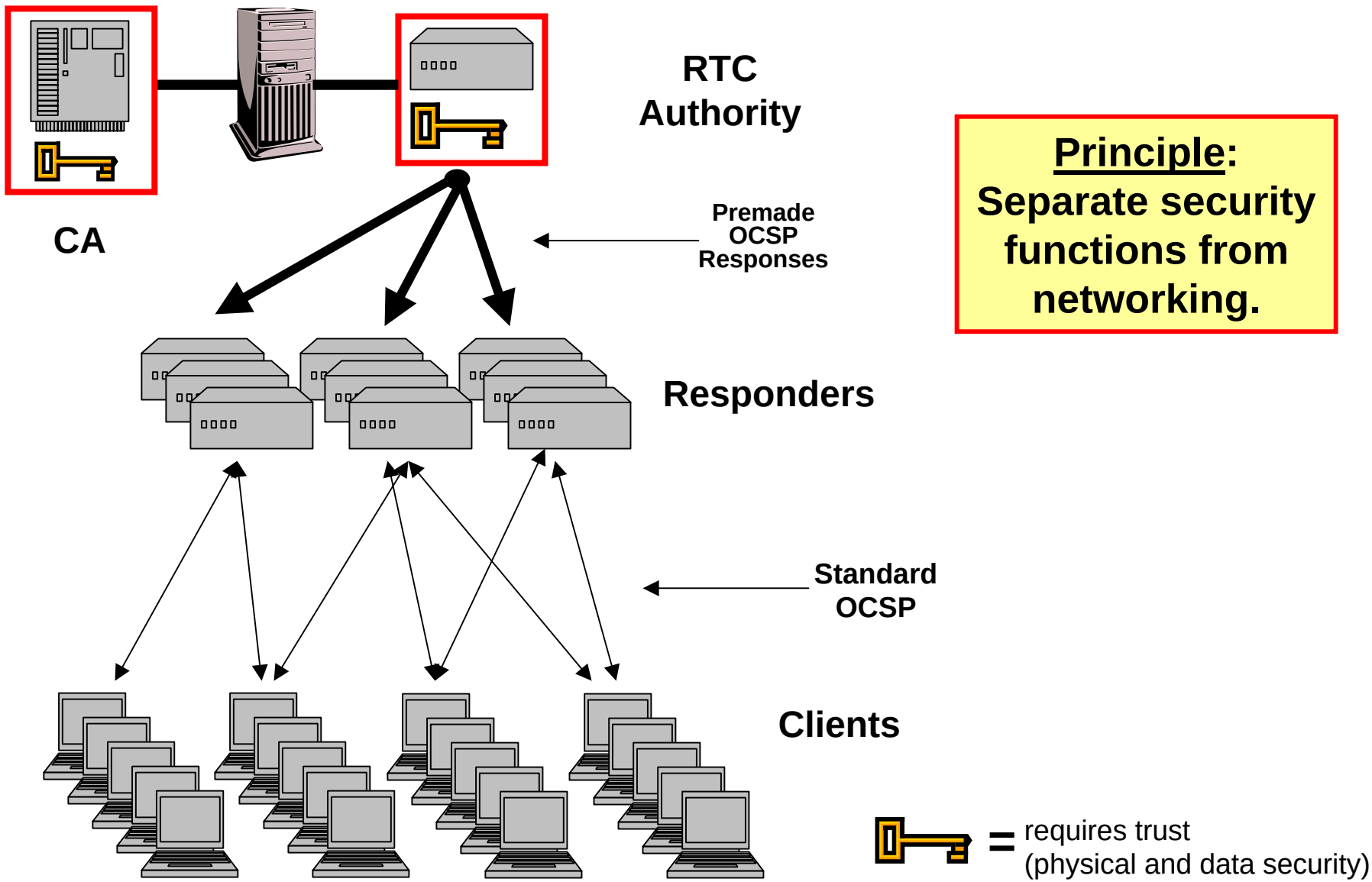
Managing Server Security Patches:

Priceless

= requires trust
(physical and data security)

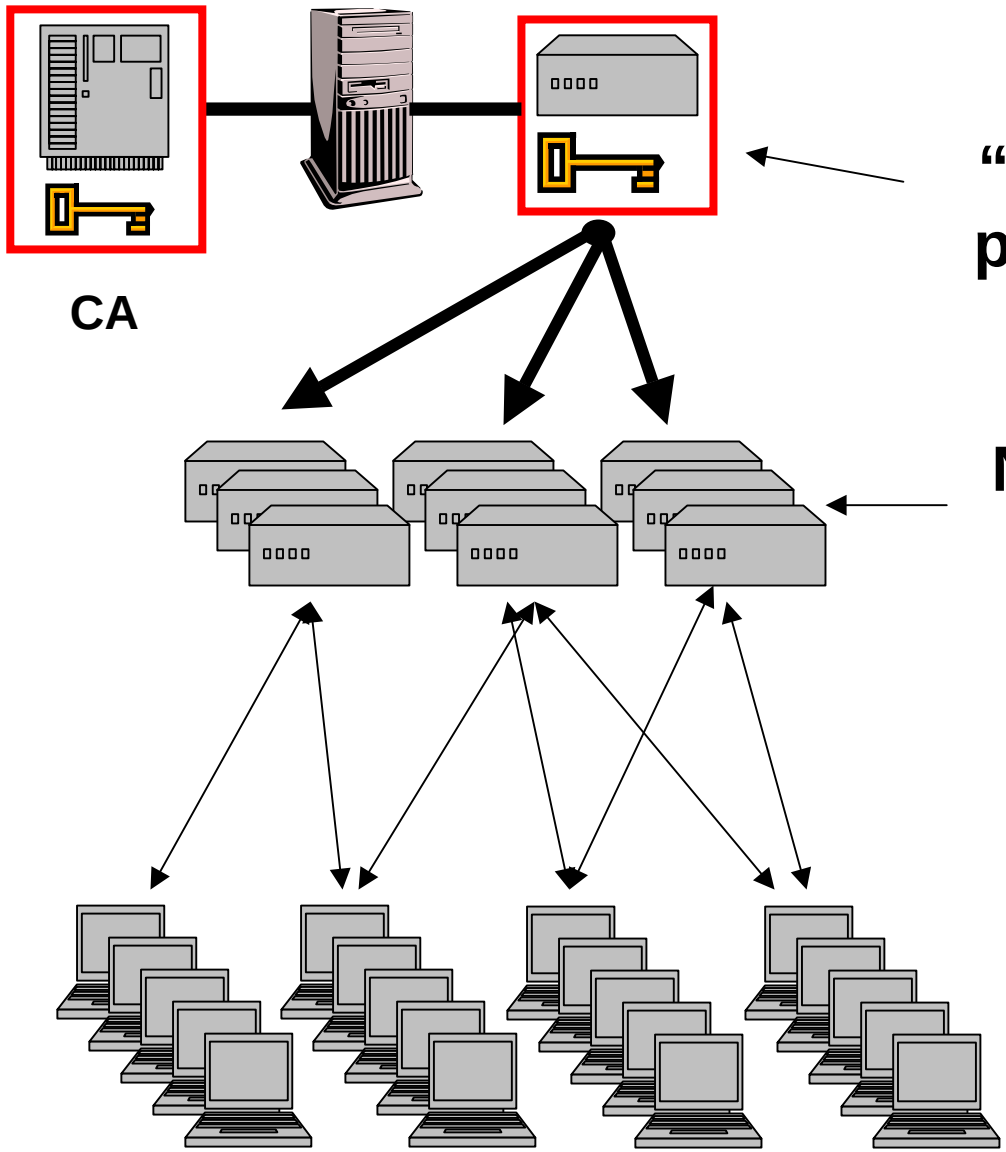
CORESTREET
REAL TIME CREDENTIALS

Distributed OCSP (D-OCSP)



Principle:
Separate security functions from networking.

Distributed OCSP: Security



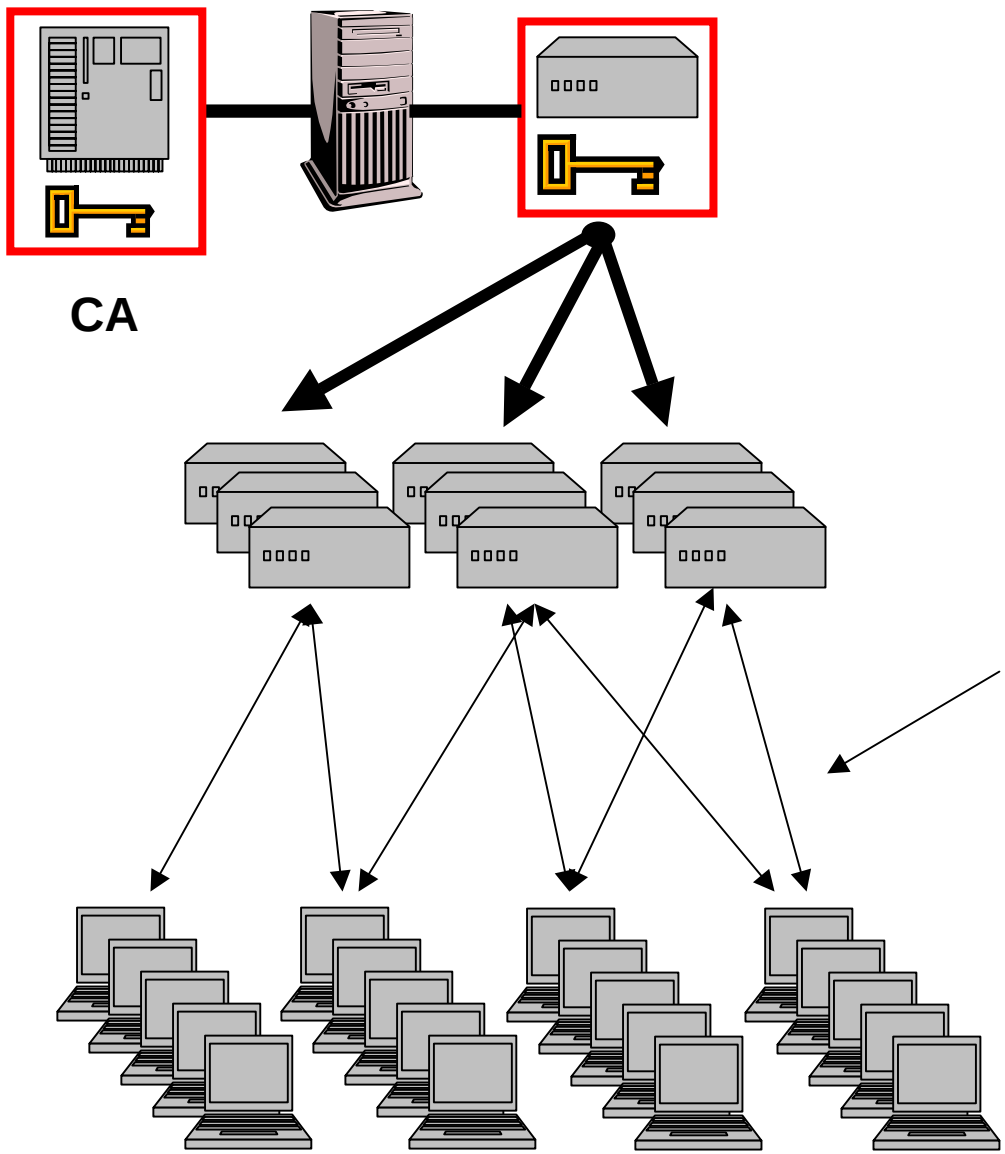
“Off-line” signing key prevents compromise

No keys in online servers; responders cannot “lie”

= requires trust (physical and data security)

CoreStreet
REAL TIME CREDENTIALS

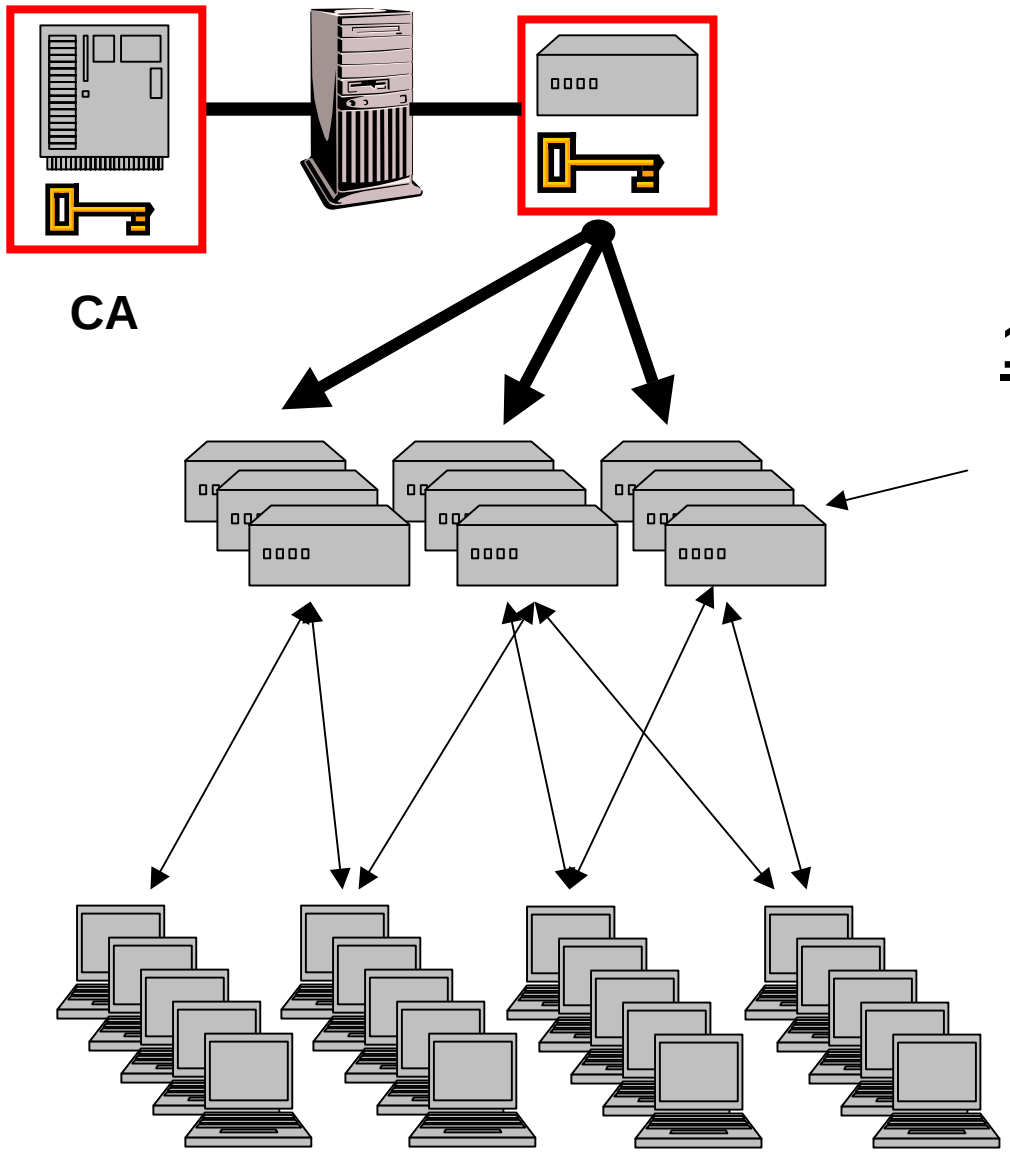
Distributed OCSP: Scalability



Low client bandwidth:

- **1-3 kB per response**

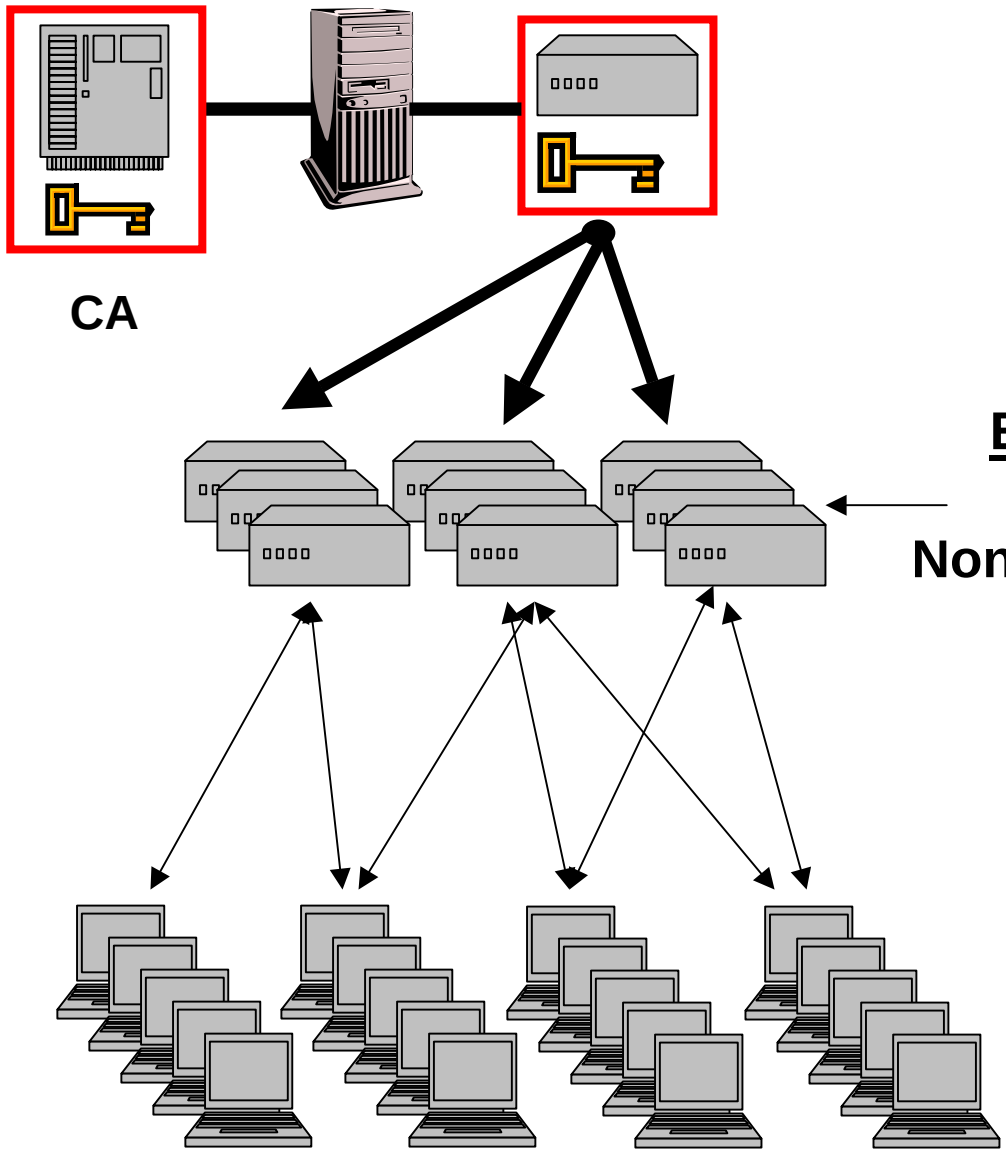
Distributed OCSP: Performance



1000 requests/sec each:

- No RSA at runtime
- Simple table look-ups
- 10-100 ms per request

Distributed OCSP: Deployment



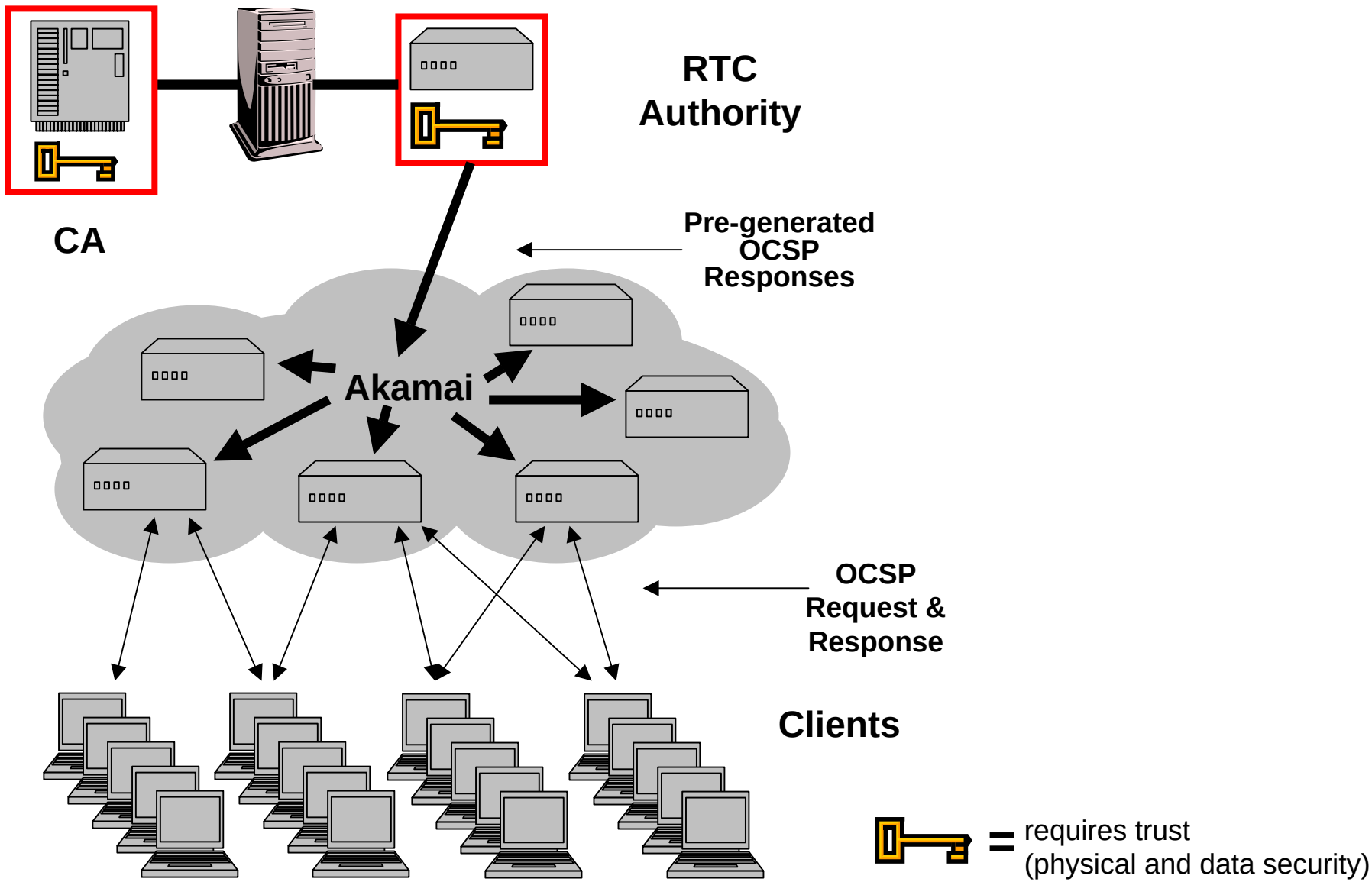
Each responder requires* :

Server: $3k

Non-secure hosting: $3-5k / year

*** (or run on any existing server)**

Distributed OCSP, Managed



CoreStreet
REAL TIME CREDENTIALS

Questions …