OSG Site Coordination Meeting

CRL distribution

Igor Sfiligoi
for the OSG Security Group

Why am I here?

- Some sites are complaining that they have problems downloading the needed CRLs
- Would like to understand how widespread is the problem, and
  - If we need to do something about it
  - Present you a possible solution

Why is this a problem?

- CRLs are the fundamental building block of Grid (x509) security
  - Not the only one, but still...
- CRLs has an expiration date
  - So they need to be renewed often
- If the CRL needed to check the proxy is expired/invalid, the proxy will be rejected
  - Easy to blacklist an entire community!

Why are expired CRLs a problem?

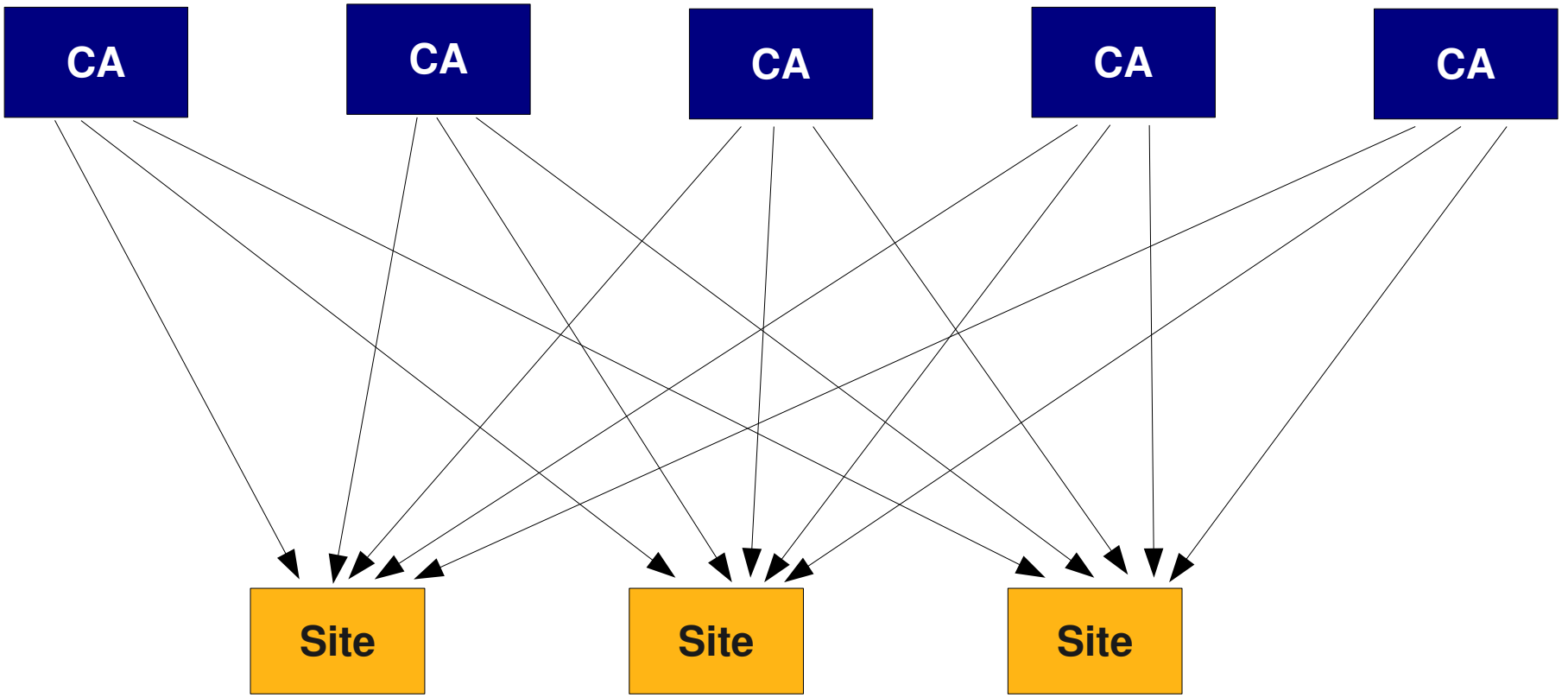
- Job submission to CE fails
- Data transfer to SE fails
- Data transfers from WNs fail
- Other services from WNs fail

Each node has its own copy of CRLs.

Users may well experience problems on a subset of WNs only.

It can get confusing fast!

CRLs renewal today



What can go wrong?

- Network problems at site
- Network problems at CA
- Routing problems between site and CA
- CA overload
- CA operational issues

What can go wrong?

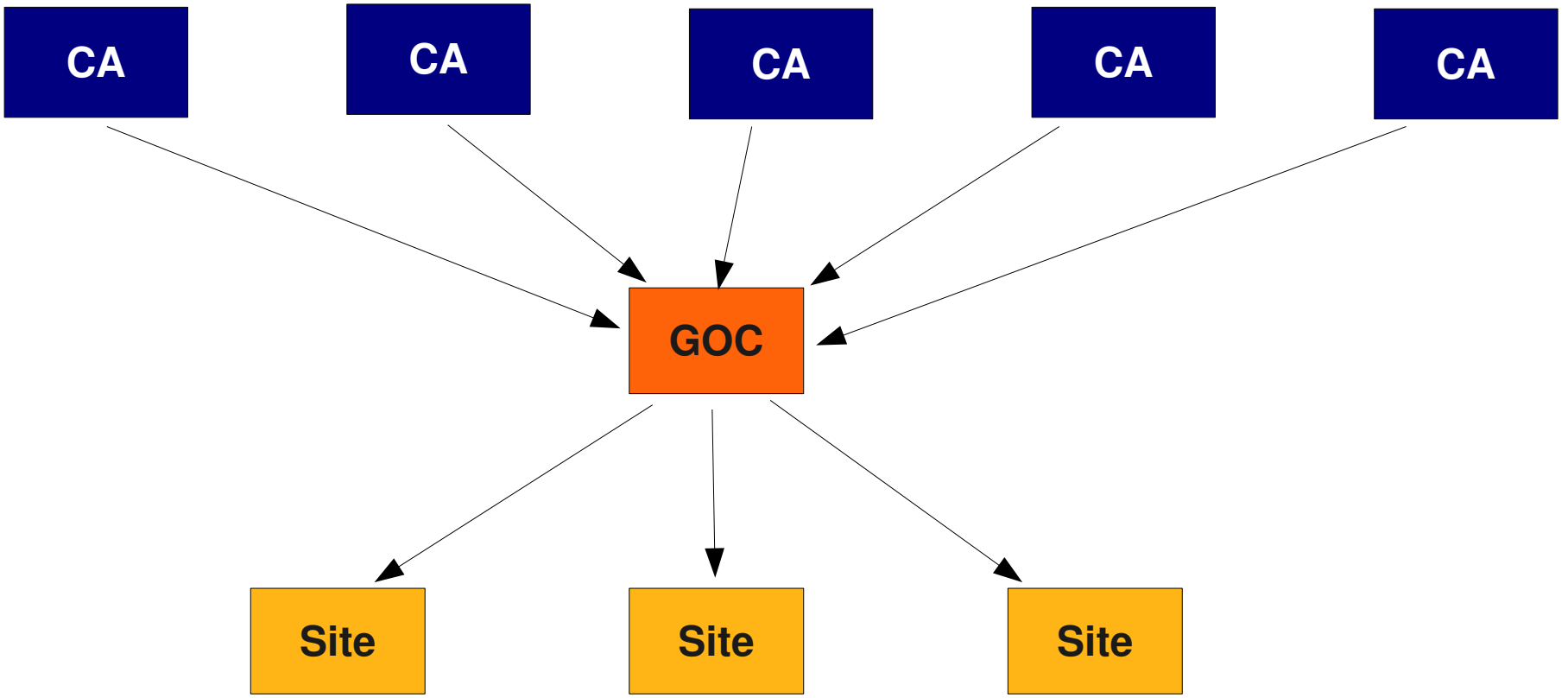
- Network problems at site
- Network problems at CA
- Routing problems between site and CA
- CA overload (comes and goes)
- CA operational issues

Assuming CAs are willing to work with GOC (not with random sites)

Legend:

* Site can debug and fix
* GOC can debug and help fix
* ???????

Possible solution



What can go wrong now?

- Network problems at site
- Network problem at GOC
- Routing problems between site and GOC
- Network problems at CA
- Routing problems between GOC and CA
- CA overload
- CA operational issues
- GOC operational issues

Legend:

* Site can debug and fix
* GOC can debug and help fix
* ?????

Assuming CAs are willing to work with GOC (not with random sites)

GOC now a critical service?

- We understand that GOC could become a single-point-of-failure
- We want to avoid this!
  - The picture was just a simplified version
  - The real solution is expected to fall back to direct download from the CAs if GOC is down

Summary

- Is this really a problem for most of the sites?
  - Or just a minor annoyance you already know how to handle?
- Should we look at the proposed alternative?
  - Has pros and cons
  - It will not come for free to OSG
- Or would smaller changes be enough?
  - Maybe just better emails?