OCSP

EDG discussion

Dublin December 2003

What “supports” OCSP now?

- Openssl 0.9.7 or later – see http://www.openssl.org/docs/apps/ocsp.html
  - Supports client and at least some basic server functionality
  - We have tested client side, not server side
- Globus –
  - GT 3.2 (discovered accidentally) in alpha testing, supports openssl 0.9.7.
  - Will a separate GSI release or back rev Globus be made available? Unknown
- Netscape/Mozilla browsers
  - Can support a designated OCSP responder, or search for OCSP responder in AIA attribute
  - We have tested this a little
- Microsoft Internet Explorer – NOT!
  - 3rd party plugins
- Servers
  - Apache would presumably depend on underlying version of openssl – unknown
  - Commercial web servers (eg IIS) – unlikely
- Java
  - new Java security classes support it; will try this internally on our CA (which is Java-based)

Creating an OCSP service – issues

- Globus support
  - Avoiding the problems of current CRL support
  - Co-existence with CRL's and other validation

OCSP implementation issues

- OCSP service discovery
  - DNS SRV? Maybe indirectly, since OCSP < URL, not a port; establish a convention
  - AIA extension in End Entity certs(see RFC 3280, section 4.2.2.1)
  - But our demonstration shows a different technique
- Configured servers
  - Site/project/local OCSP responders (see later)
- Web service/OGSA wrapper
- Configurations
- Design the service to avoid
  - The software engineering problem of current CRL use
  - The problems network services always have with reliability
  - Define defaults that make sense
  - Add a configuration file; consider /etc/nsswitch.conf for example Which OCSP server to use Local/URL to a specific server/AIA

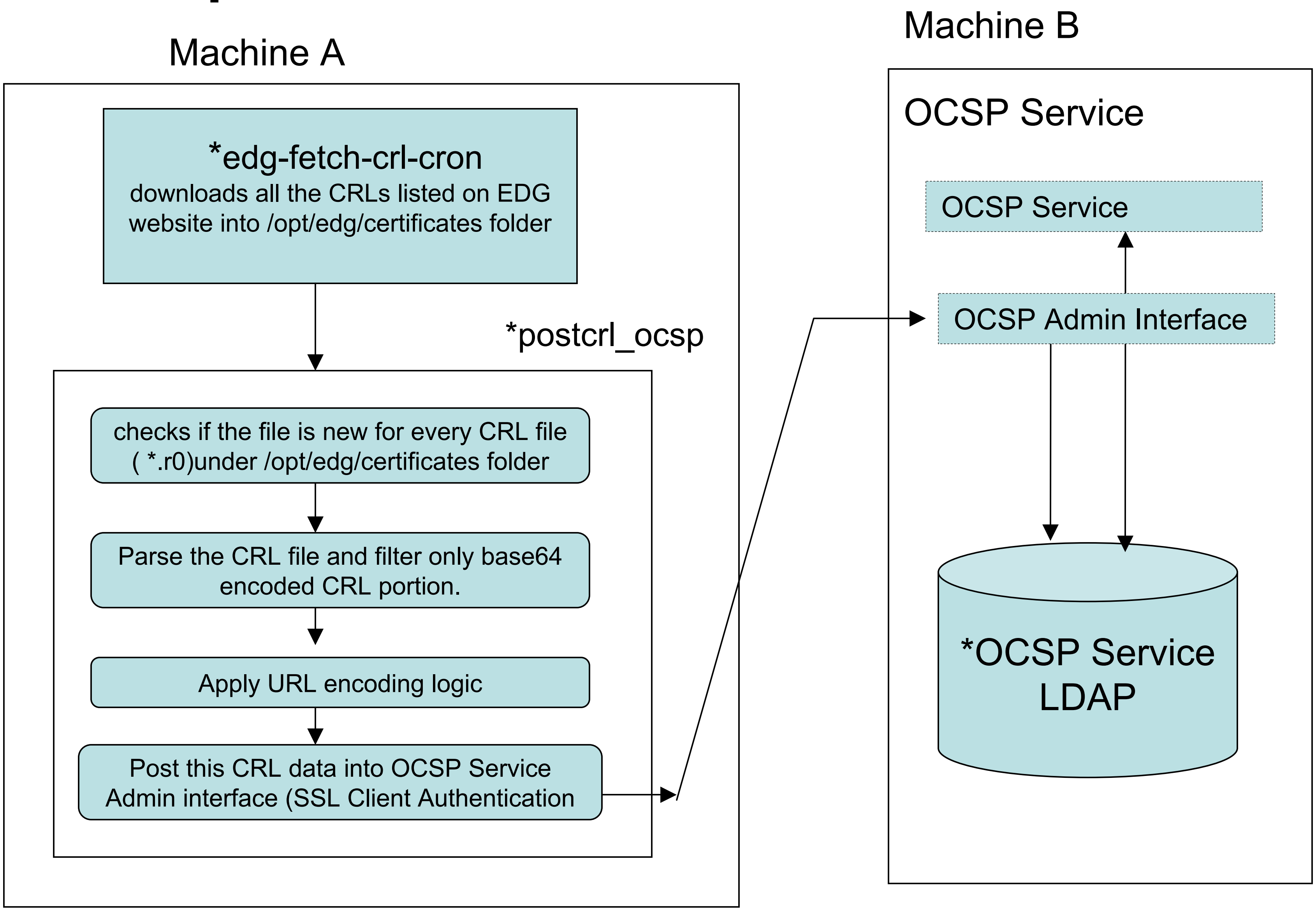
OCSP Implementation (2)

- Define defaults that make sense
- Add a configuration file; consider /etc/nsswitch.conf for example
  - Which OCSP server to use
  - Local/URL to a specific server/AIA extension in cert
- What validation service to use
  - CRL/OCSP/other?
- How to deal with failure
  - ignore/log/authentication failure
- How to deal with OCSP “unknown” response (same as failure?)

OCSP Implementation (3)

- Caching
  - Probably more of a grid service problem than a client problem?
  - Cache lifetimes / negative vs positive results
- Chaining / referrals
  - Mentioned in discussion with another party –
  - OCSP server back end issue?
- OCSP server issues
  - Trusted service
  - Site/project/local OCSP responders
    - Local – cache?
    - Site/project OCSP responders
      - » Opportunity here is to hide all the update & management Issues on a few machines; other grid services must know About these responders.
    - Packaging info for OCSP responders
      - » See ESnet demo
    - Push vs Pull
      - » ESnet demo shows both, but isn't responder "pull" more practical?

Experimental OCSP service



Machine A

*edg-fetch-crl-cron
downloads all the CRLs listed on EDG website into /opt/edg/certificates folder

*postcrl_ocsp

checks if the file is new for every CRL file (*.r0)under /opt/edg/certificates folder

Parse the CRL file and filter only base64 encoded CRL portion.

Apply URL encoding logic

Post this CRL data into OCSP Service Admin interface (SSL Client Authentication

Machine B

OCSP Service

OCSP Service

OCSP Admin Interface

*OCSP Service LDAP

* edg-fetch-crl-cron & postcrl_ocsp are cron job runs every night

*All the CA certificates listed on http://marianne.in2p3.fr/datagrid/ca/ca-table-ca.html has been installed with OCSP Service