Proxy Restrictions

Ákos Frohner, Joni Hahkala, Andrew McNab, Gergely Debreczeni

CERN – JRA1 All Hands meeting, 2007-10-25

www.eu-egee.org

Information Society and Media

Rationale

delegated proxy might be stolen

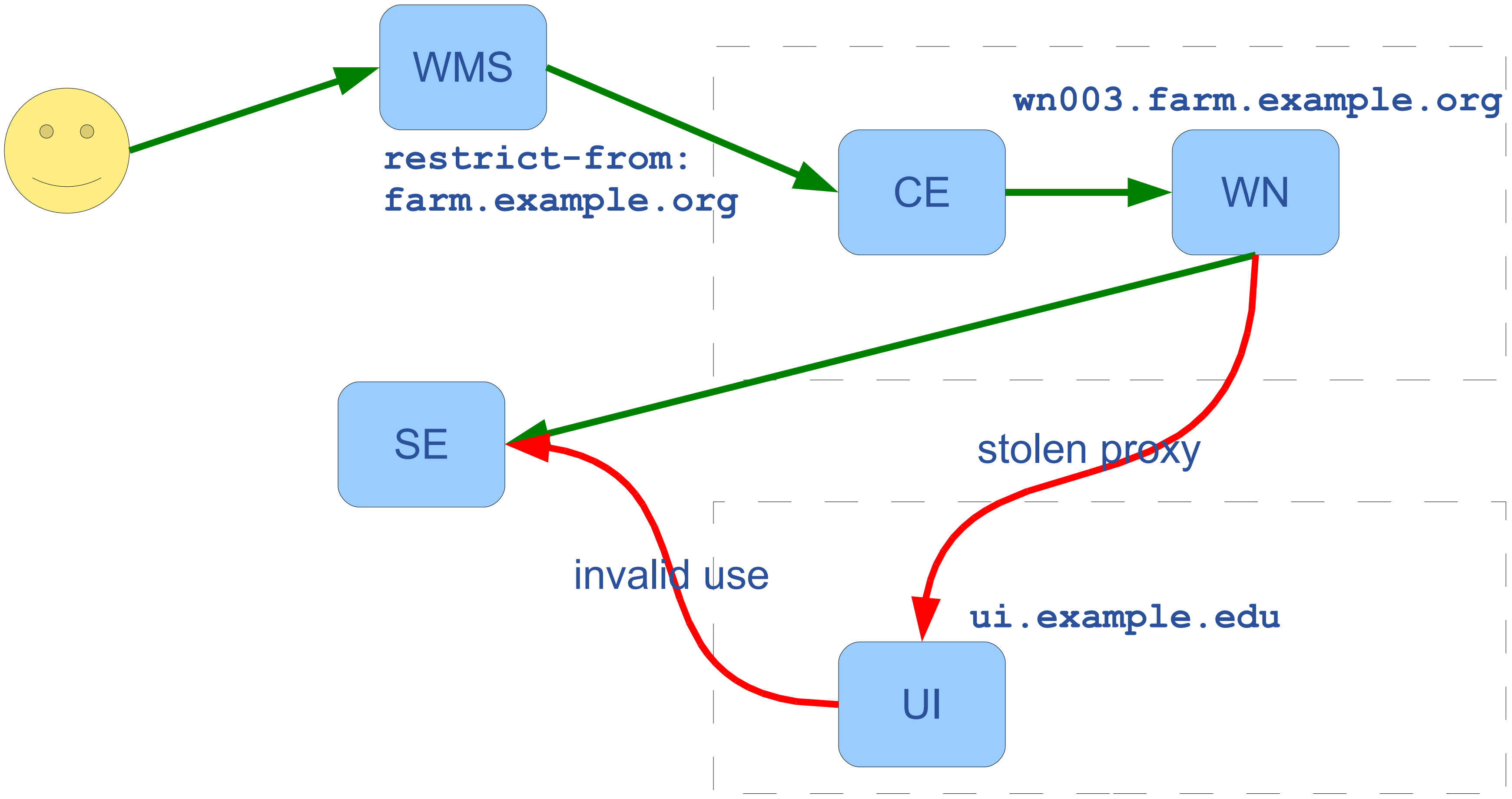
... limiting the damage:

- 'limited' proxy – cannot be used for job submission

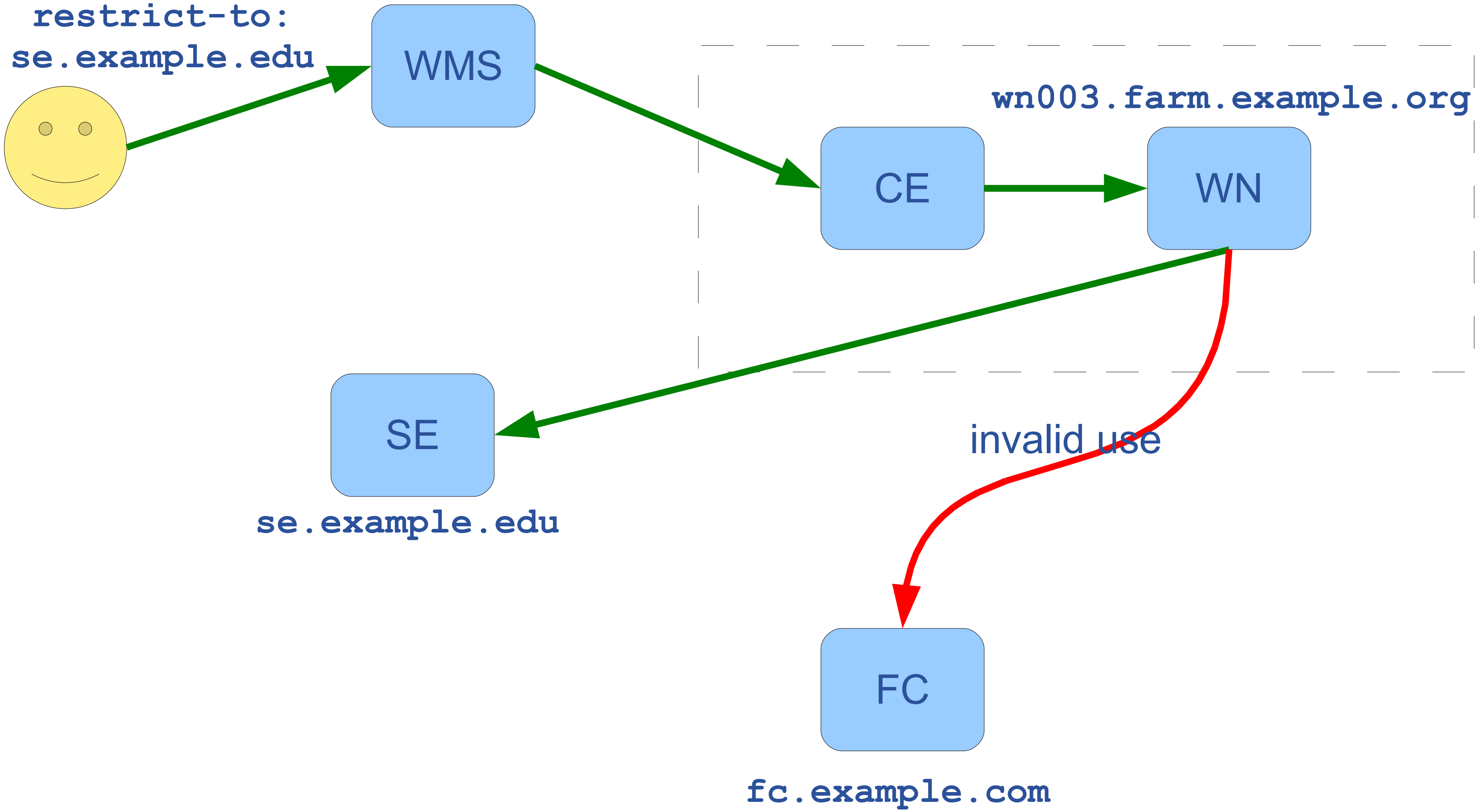
New:

- restrict-from: can only be used from a given site
- restrict-to: can only be used to a given site
- delegation trace for auditing

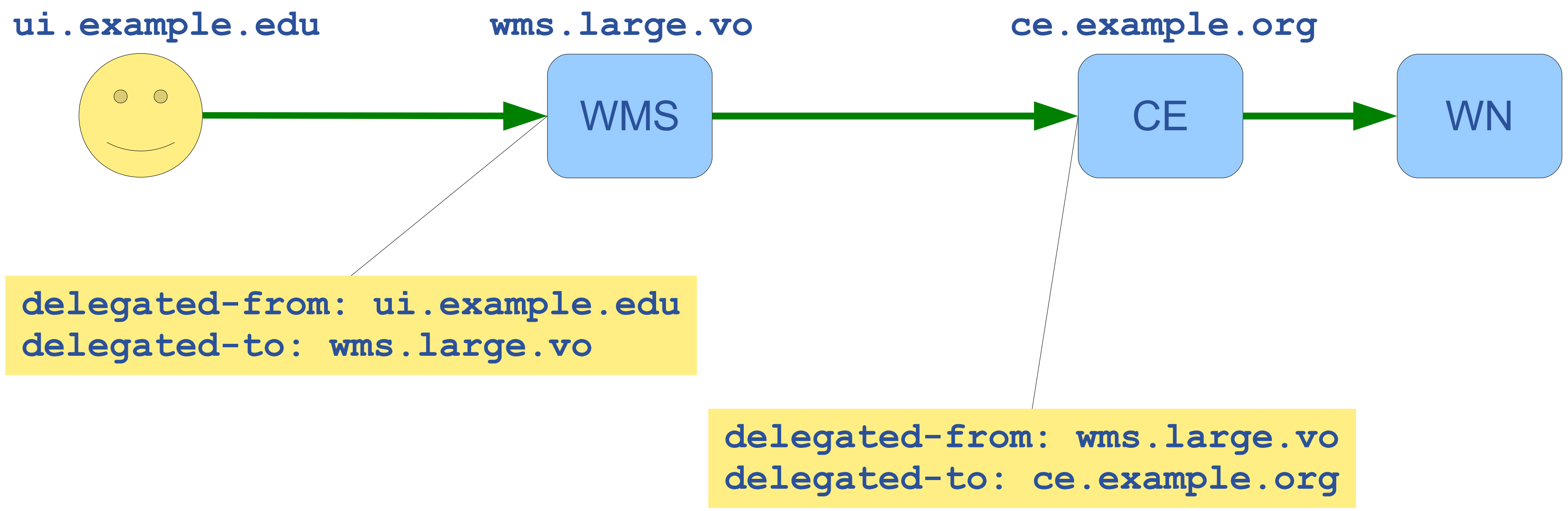
restrict-from



restrict-to


restrict-to:
se.example.edu
WMS
wn003.farm.example.org
CE
WN
SE
se.example.edu
invalid use
FC
fc.example.com

Delegation Trace



delegated-from: ui.example.edu
delegated-to: wms.large.vo

delegated-from: wms.large.vo
delegated-to: ce.example.org

It should be configurable for pseudonymity/anonymity.

Matching Rules

- (partial) DNS name:

```
restrict-from: example.org
restrict-from: .net example.edu
```

- IPv4 address:

```
restrict-from: 10.1.2.3
restrict-from: 10.1.0.0/16
```

- IPv6 address:

```
restrict-from: 2001:db8::a00:20ff:fea7:ccea
restrict-from: 2001:db8::a00:20ff:fea7:ccea/10
```

- OR: restrictions in the same certificate
- AND: restrictions in the chain

LCG Example

CMS CRAB
https://twiki.cern.ch/twiki/bin/view/CMS/CRAB

Users use CRAB to submit CMS jobs, which discovers where the data is located, so it submits the job to a close CE.

The CRAB wrapper could generate a restriction including the SE holding the data and the destination CE as a simple file with proxy restrictions, which could be included in the delegated proxy, when the job is submitted.

Q1/2

What happens, if the proxy is restricted by the CE, however it is used in an SRMcopy operation? The SE must act on behalf of the user, however the SE might not be inside the restricted domain.

- The CE could include the local SE and the user should submit an SRMcopy to pull/push from that service.
- The CE might also include other global services, such as FTS, which make use of delegation.

Q2/2

Shall we use proper ASN.1 structures for the restrictions and trace or a simple string representation is enough?

- In case of an ASN.1 structure we have to allocate our new OID arc.
- In case of a simple string extension we might just use VOMS' include OID: 1.3.6.1.4.1.8005.100.100.2
  This would also simplify the introduction of this idea, as any user can include a simple text file under this OID using the '-include' option of 'voms-proxy-init'

TODO

- **add the proposed extensions to the delegation services:**
  - GridSite (C)
  - gLite delegation (Java)
- **add optional check for these extensions in**
  - trustmanager (Java)
  - gridsite (C)
  - LCAS/LCMAPS (C)
- **provide methods to retrieve the delegation trace for logs**
- **...?**