
# Updates from the EUGridPMA

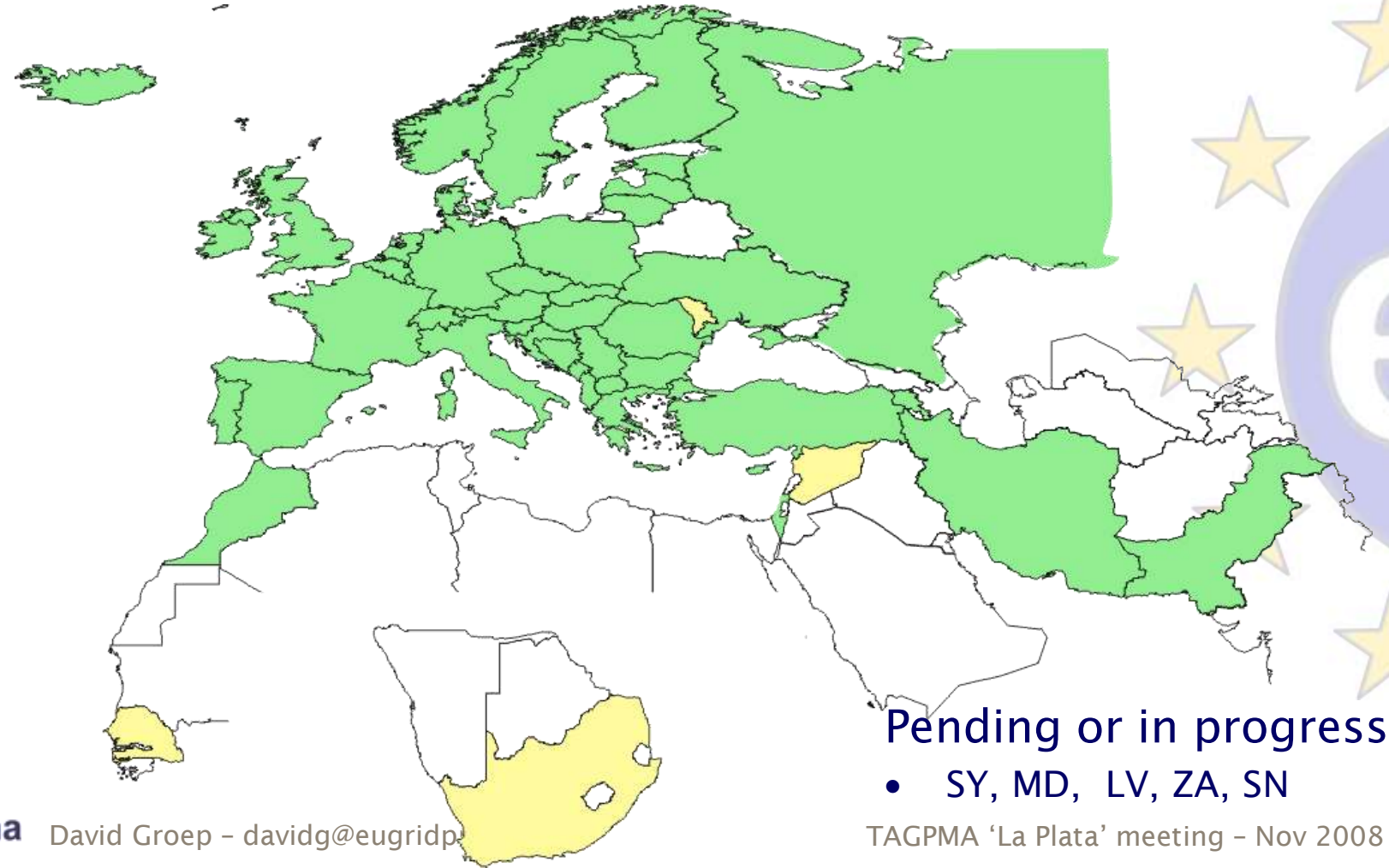
David Groep, Nov 7nd, 2008

# Updates Today

- Towards EMEA coverage
  - Autonomous growth
- Updates
  - AuthZ Operations WG
  - Repository issues

# Geographical coverage of the EUGridPMA

- 23 of 25 EU member states (all except LU, MT)
- \+ AM, CH, HR, IL, IR, IS, MA, ME, MK, NO, PK, RO, RS, RU, TR, UA, *SEE-GRID* + CA, CERN (int), DoEGrids(US)*



Pending or in progress

- SY, MD, LV, ZA, SN

# More growth expected

- Pending EUMedGrid countries: DZ, TN, LY, EG
- New initative across the 'silk road' countries
  - Established by Ara Grigoryan and ArmeSFo
  - In collaboration with NATO programme

# ‘AuthZ op. policy WG’

- Extending best practices to AA operations policy
  - operational AuthZ policies today are far less clear
  - but the minimum requirements on running an AA server may be quite similar to running a CA
  - ‘There is no other large group of experts out there waiting to take this on’, and we don’t need a parallel I*TF
  - But: scaling the model is quit different

- Prototype version of a guideline at the Wiki

  ‘This is a draft document of the International Grid Trust Federation describing the minimum requirements for the operation of an Attribute Authority (AA) service. The AA service is run by or on behalf of a Grid Virtual Organisation (VO) and maintains attributes for registered VO users and/or VO services. Attribute assertions are securely delivered on request to members of the VO. They are presented by the user and/or service, together with an X.509 credential for authentication, for the purposes of Authorisation of access to a Grid resource.’

# Developments and discussion

- Repository of “good” and “bad” CP/CPS examples
  - boilerplate text repository
  - On software used
  - Activity ‘owner’: Jens Jensen

- Robot certificate
  - *popularity of robot certs growing rapidly – action needed*
  - pre-requisite for portal policies in EGEE and many NGIs
  - issued on a hardware token – cheap, safe and easy

- Credential repository guidelines
  - Risks, solutions, and the dissemination thereof is lacking
  - Quick-scan of some MyProxy stores reveales ‘interesting’ things
  - Guidelines may help – especially for ‘trusted’ credential stores operated by the NGIs (or other persistent infrastructures)

# More items for discussion

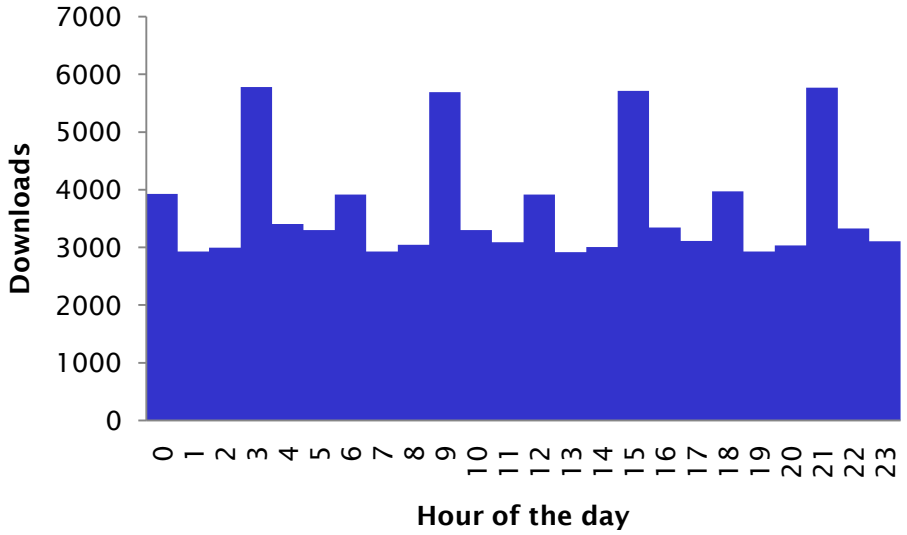
- End-of-life for 1024 bit RSA keys?
  - Might possibly impact performance (although many CAs are already 2048/4096 bits)
  - After a long discussion, figured that this is not our major issue for the moment
- Emergency escalation contact procedure
  - Request all CAs to deposit an emergency contact process with the IGTF RAT and their Chair
- Please implement robot certs as soon as possible
  - *See the presentation later on how to do it*
  - *Hardware tokens, e.g. Aladdin eToken, readily available*
  - *Boiler-plate CP/CPS text available*

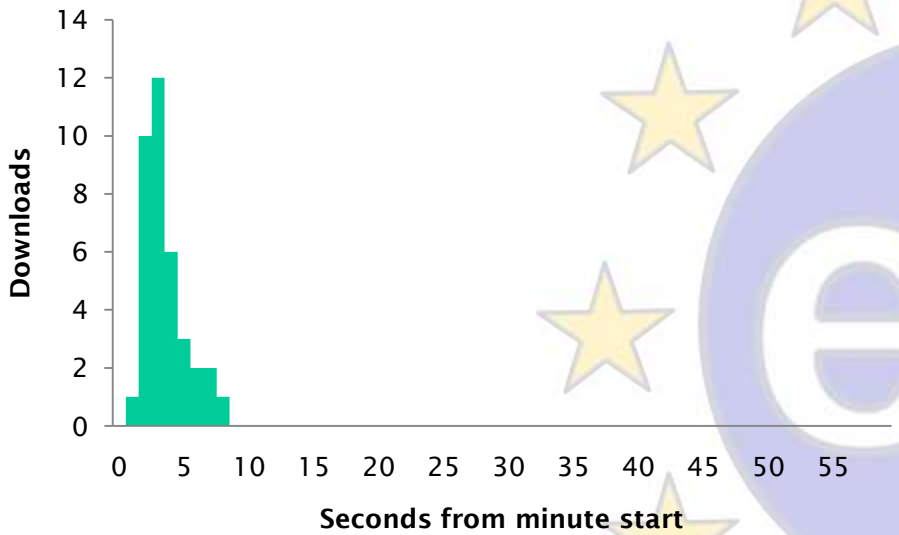
# More items

- Add more OIDs to your end-entity certs
  - At least the OID corresponding to the profile
  - More OIDs from 1SCPs that match
- And more 1SCPs OIDs are being assigned
  - Already there:
    'private key is held on a token'
    'I was F2F identity-vetted'
    'I was vetter through a TTP'
  - New:
    'I am a Robot/automated client',
    'I an a server/host cert'

# Web Cachability, why?

Downloads clustered in first seconds of the minute

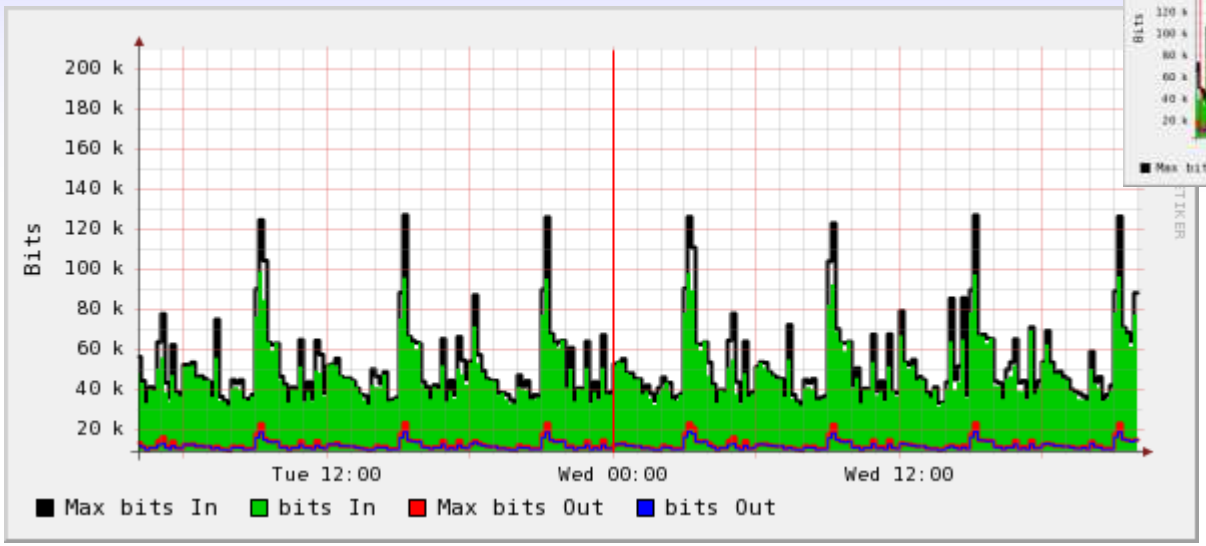


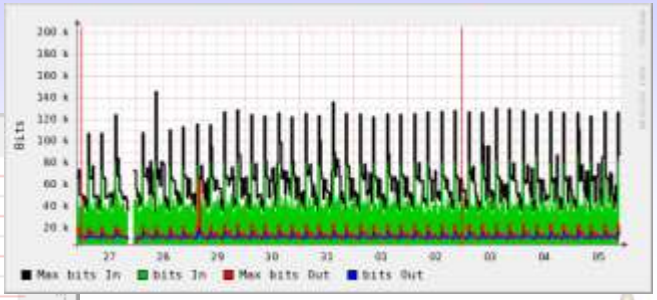




Data: DutchGrid CA

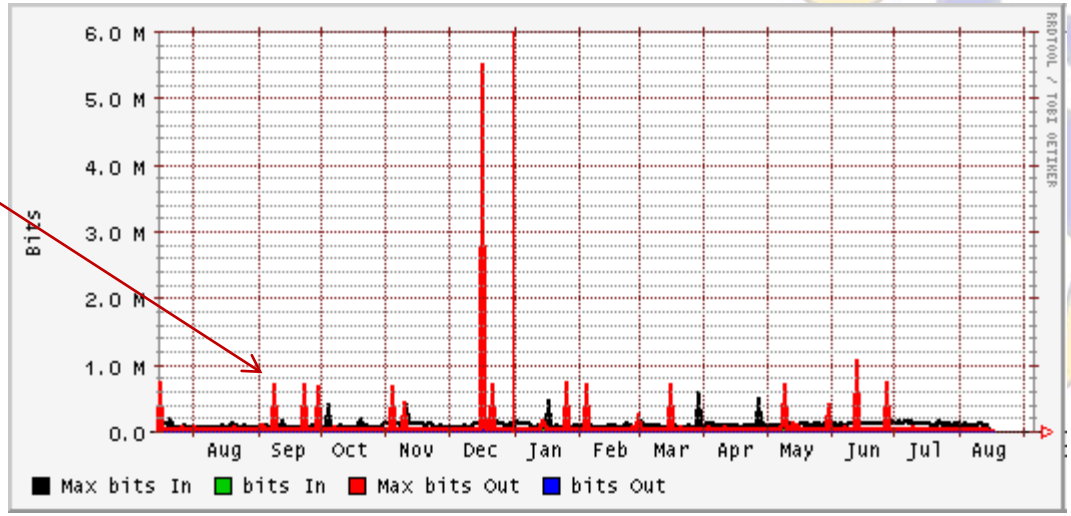
Statistics: 88452 downloads per day per CA
14084 distinct IP addresses
average 4 downloads per day per host

# Network traffic



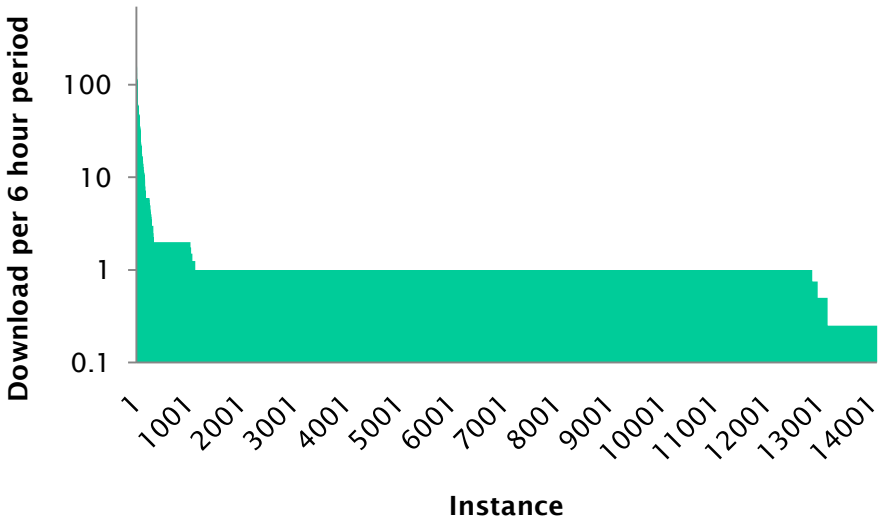



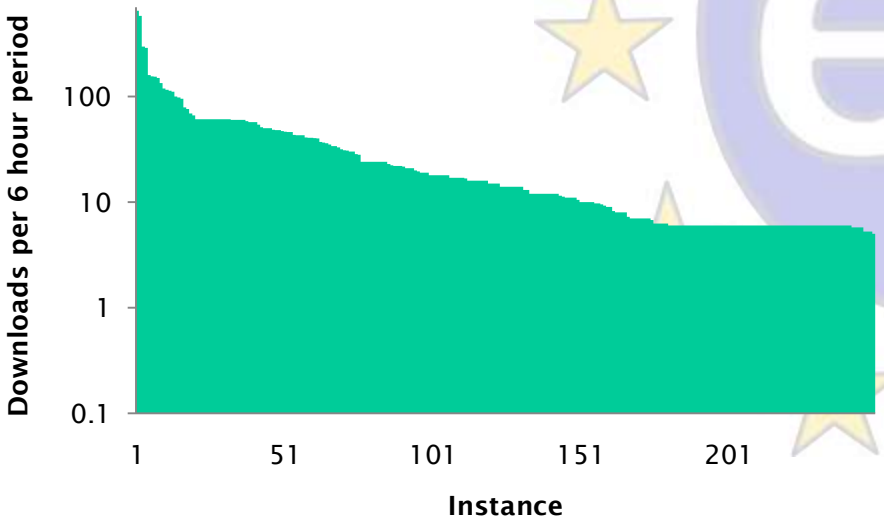
Site cache misconfigurations or new sites



# There Are Caches

- Majority of IPs download individually every 6hours
- But there are at least 300 sites that cache!



# Web Cacheability

- Good

```
$ HEAD -S http://ca.dutchgrid.nl/medium/cacrl.pem
200 OK
Cache-Control: max-age=3600
Connection: close
Date: Wed, 05 Nov 2008 21:31:48 GMT
Accept-Ranges: bytes
Server: Apache
Content-Length: 4728
Content-Type: text/plain
Expires: Wed, 05 Nov 2008 22:31:48 GMT
Last-Modified: Tue, 04 Nov 2008 10:07:05 GMT
Client-Date: Wed, 05 Nov 2008 21:31:48 GMT
Client-Response-Num: 1
```

# Web Cacheability

- Reasonable, but relies on remote site cache setup

```
$ HEAD http://ca.grid-support.ac.uk/cgi-bin/importCRLpem
200 OK
Connection: close
Date: Wed, 05 Nov 2008 21:15:02 GMT
Accept-Ranges: bytes
ETag: "164011-6b3a-1c7652c0"
Server: Apache/2.0.46 (Red Hat)
Content-Length: 27450
Content-Type: text/plain; charset=UTF-8
Last-Modified: Wed, 09 Jan 2008 13:31:31 GMT
Client-Date: Wed, 05 Nov 2008 21:15:02 GMT
Client-Peer: 130.246.143.144:80
Client-Response-Num: 1
```

# Web Cacheability

- Update your CRL URL, but answer is reasonable

```
$ HEAD http://www.dutchgrid.nl/ca/medium/cacrl.pem
HTTP/1.1 301 Moved Permanently
Date: Mon, 03 Nov 2008 08:59:13 GMT
Server: Apache
Location: http://ca.dutchgrid.nl/medium/cacrl.pem
Content-Length: 247
Content-Type: text/html; charset=iso-8859-1
```

- Update your CRL URL, answer wastes the cache

```
$ HEAD http://www.lip.pt/ca/lip-crl.pem
HTTP/1.1 302 Found
Date: Mon, 03 Nov 2008 09:04:08 GMT
Server: Apache/2.2.6 (Fedora)
Location: http://ca.lip.pt/lip-crl.pem
Content-Length: 287
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

# Web Cacheability

- Uncacheable

```
$ HEAD 'http://crls.services.cnrs.fr/get.fcgi?ca=CNRS-Projets&cmd=getpem.crl'
200 OK
Connection: close
Date: Wed, 05 Nov 2008 21:17:05 GMT
Server: Apache/2.2.8 (Fedora) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8b
Content-Length: 593
Content-Type: octet/stream
Client-Date: Wed, 05 Nov 2008 21:35:44 GMT
Client-Peer: 195.220.197.22:80
Client-Response-Num: 1
Content-Disposition: attachement; filename="CNRS-Projets.crl"
```

(no Last-Modified nor Expires header)

# Web Cacheability

- Just plain weird

```
$ HEAD http://www.cs.tcd.ie/Grid-Ireland/gi-ca/1e43b9cc.r0
200 OK
Cache-Control: max-age=259200
Connection: close
Date: Mon, 03 Nov 2008 09:05:40 GMT
Accept-Ranges: bytes
Server: Apache
Content-Length: 4505
Content-Type: text/plain
Expires: Thu, 06 Nov 2008 09:05:40 GMT
Last-Modified: Tue, 28 Oct 2008 15:42:44 GMT
Client-Date: Mon, 03 Nov 2008 09:05:40 GMT
Client-Peer: 134.226.32.57:80
Client-Response-Num: 1
```

# Web Caching configuration (apache)

- Apache 2.x configuration - within your (virtual) host section

```
<FilesMatch "cacrl.(pem|der|cer)$">
   ExpiresActive On
   ExpiresDefault "access plus 1 hours"
   Options -Includes
</FilesMatch>

<FilesMatch "cacert.(pem|der|cer)$">
  ExpiresActive On
  ExpiresDefault "access plus 1 days"
  Options -Includes
</FilesMatch>
```

# IGTF Release Process and Web

- Release Process
  - Releases moved to (preferably) Monday or Tuesday
  - More documentation of the process still needed
  - More checks are now built into the process (Debian!)

  End use: **https://dist.eugridpma.info/distribution**
  **https://www.apgridpma.org/distribution**

- Monitoring and alarms
  - Nagios: **http://signet-ca.ijs.si/nagios/** (guest/guest)
  - PMA Distribution Warnings by email 4 times/day
  - *It helps, but reaction to the warnings is down again …*

# Changes to the Classic AP

- See special presentation …


Some dates for you to remember and schedule

- 26-28 Jan 2009: 15th, CyGrid, Nicosia, CY
- 11-13 May 2009: 16th, SWITCH, Zurich, CH
- 14-16 Sept 2009: 17th, DFN, Berlin, DE