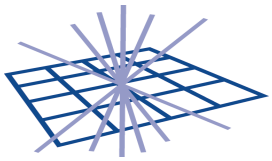
WLCG
Authentication & Authorisation

LHCOPN/LHCONE
Rome, 29 April 2014

David Kelsey

STFC/RAL



GridPP
UK Computing for Particle Physics

Overview

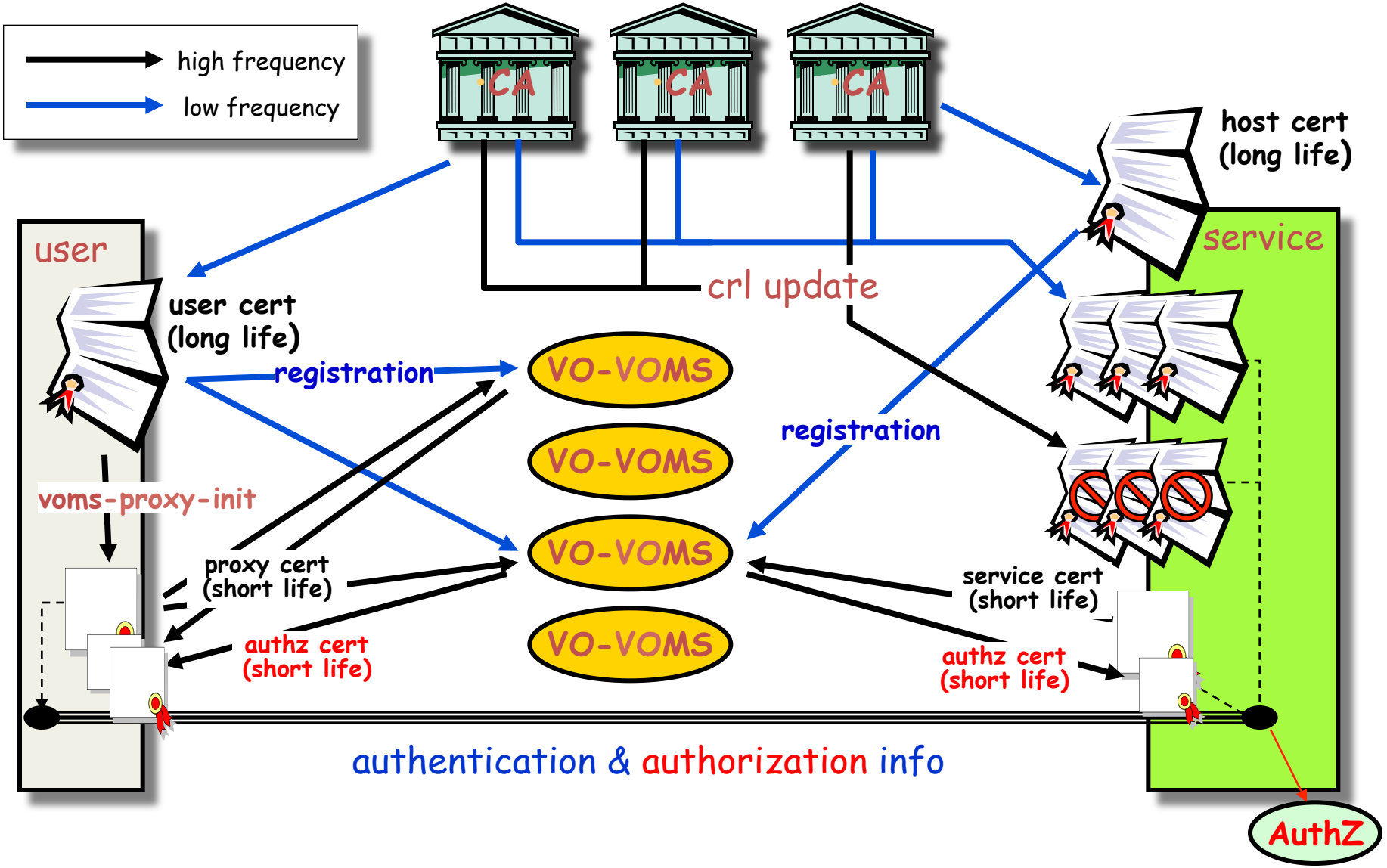
- The WLCG security model
- IGTF
- Other AAI developments
- Validating Certificates
- Example work flow

The Grid Security Model

- User obtains X.509 IGTF certificate once per year
  - Or short-lived cert produced dynamically
  - can be used in many Grids and in many Virtual Organisations (VO)
- Authorisation is controlled by the VO
  - User registers once per year with VO (in VOMS)
  - Attribute certificate confirms VO membership
  - And grants roles and group membership
- User single sign-on by use of Short-lived Proxy Certificates
- Delegation to services (to act on users behalf)

- Services and Hosts also authenticated via X.509 certificates

AuthN and AuthZ



Many thanks to David Groep
– slides shown on 2 April 14

eResearchers Requirements

the IGTF model of interoperable global trust and with a view towards FIM4R

AAI Workshop

Presenter: David Groep, Nikhef

IGTF
Interoperable Global Trust Federation
AP | EU | TAG

eugridpma

NIKHEF
SURF SARA

egi
e-infrastructure

IGTF – *Interoperable Global Trust Federation*

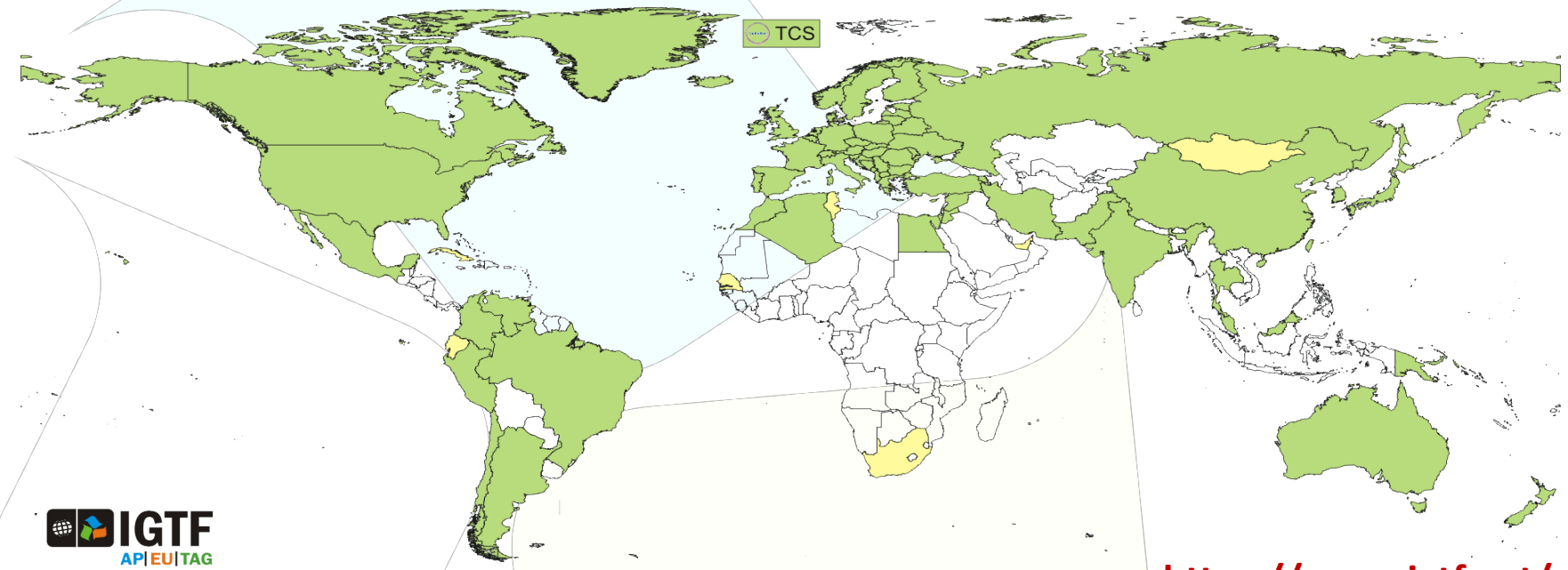
supporting distributed IT infrastructures for research

- IGTF brings together
  - e-Infrastructure resource providers, user communities and identity authorities

  to agree on
  - global, shared minimum requirements and assurance levels
  - inspired and coordinated by the needs of relying parties

- Trust is technology-agnostic
  - focus on global, coordinated identity across communities and across service providers for *cooperative services*
  - define 'best practices' for assurance levels, attribute authority operations, credential management, auditing and reviewing

Coverage: users and providers



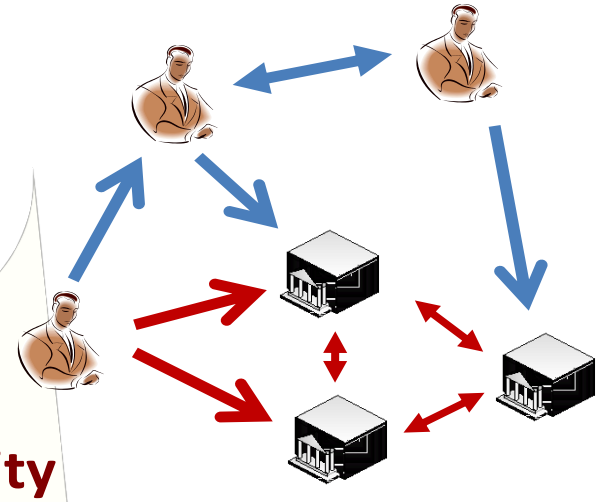
https://www.igtf.net/

- ~100 000 users and resources
- 89 national and regional identity authorities: R&E and commercial
- >1000 different user communities: small and large, national and global
- Major relying parties: EGI, PRACE, XSEDE, Open Science Grid, HPCI, wLCG, OGF, …

IGTF is a coordinating body, and not a legal entity in itself – although its members may be

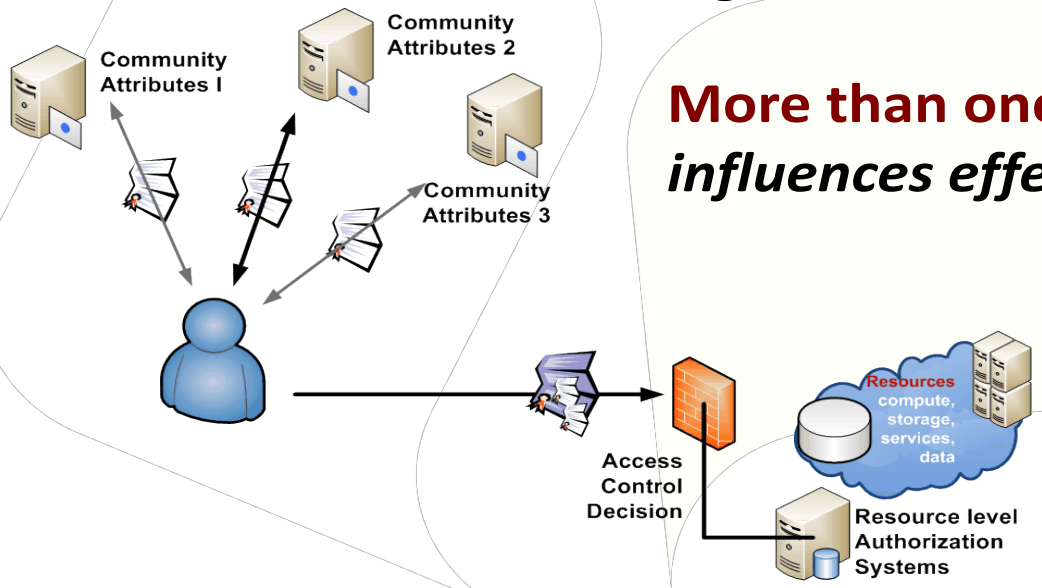
Community characteristics

More than one administrative organisation



More than one service provider
participates in a single transaction

More than one user
in a single transaction



More than one authority
influences effective policy

Single interoperating instance
at a global level

Other AAI developments

- Improving ease of use
  - Do not duplicate identity vetting procedures
  - Hide certificate management from users
    - Note WLCG middleware will continue to use X.509
- TERENA Certificate Service, CILogon (USA)
  - The ability to issue long-lived certificates to users following authentication using national federated identity credential (no additional ID vetting)
- FIM4R/REFEDS/eduGAIN/TERENA/Geant - AAI for Research
  - Defining Researchers requirements for single-signon using national federated identity and merging VO AuthZ attributes
- IGTF – new IOTA profile
  - Profile with lower levels of assurance on ID vetting
  - Assuming ID vetting is done by VO (as is the case for LHC expts)

Some AuthN technical details

- Mutual Authentication of clients and services
  - Using SSL
- User issues and signs a short-lived (~1 day) proxy cert
  - Same DN with /proxy added
  - Signed by users long-lived credential
- Whole signing path up to self-signed root must be checked for validity
  - Including dates, signatures, policy or name-space signing constraints
  - Must also check all Certificate Revocation Lists (CRL) or OCSP (online status)
- Self-signed root CA is distributed out of band by trusted IGTF/ WLCG procedures and stored in Trusted-CA directory
- As a general principle
  - private keys never cross the network (generated and used locally)
  - Even if encrypted

Job submission workflow (example)

- User submits analysis work to the experiment job management system (e.g. ATLAS PANDA) (with mutual AuthN and AuthZ)
  - May use MyProxy credential store
- Independently, the experiment system submits pilot jobs to WLCG sites
  - Authenticated as the ATLAS Pilot System (and AuthZ)
  - This identity gets mapped to local Unix credentials of the pilot system (run on worker node via local batch system)
- Users analysis payload is pulled by pilot job to WLCG worker node
- Using gLexec on worker node, the Unix account is switched to that mapped from the identity of the end user (pilot job identity needs privs)
- Job output written back to submission portal
  - Authenticated as submission system (or as end user?)

Final words

- Haven't said much about AuthZ but that is just as important
- Building trust takes lots of effort and time
- The IGTF federation is well established and works
- Workflows usually involve several admin domains, several identities (users, service operators, …)
- The (WLCG) security team would be happy to discuss AuthN and AuthZ architectures

Questions?