rijksuniversiteit
groningen

22-10-2012

Grid Security

Fokke Dijkstra

Donald Smits Centre for Information Technology

Grid & security

- You and the Grid
  - Organising resources and users in Virtual Organisations (VO)
  - Trust and identity
  - Cryptography and signing using public & private keypairs

Some slides taken from David Groep (Nikhef)

Virtual Organisations & Grid

- What is a Virtual Organisation?
  - People in different organisations seeking to cooperate and share resources across their organisational boundaries
  - E.g. A research collaboration
- Each grid is an infrastructure enabling one or more "virtual organisations" to share and access resources
- Each resource is exposed to the grid through an abstraction that masks heterogeneity, e.g.
  - Multiple diverse computational platforms
  - Multiple data resources
- Resources are usually owned by VO members. Negotiations lead to VOs sharing resources

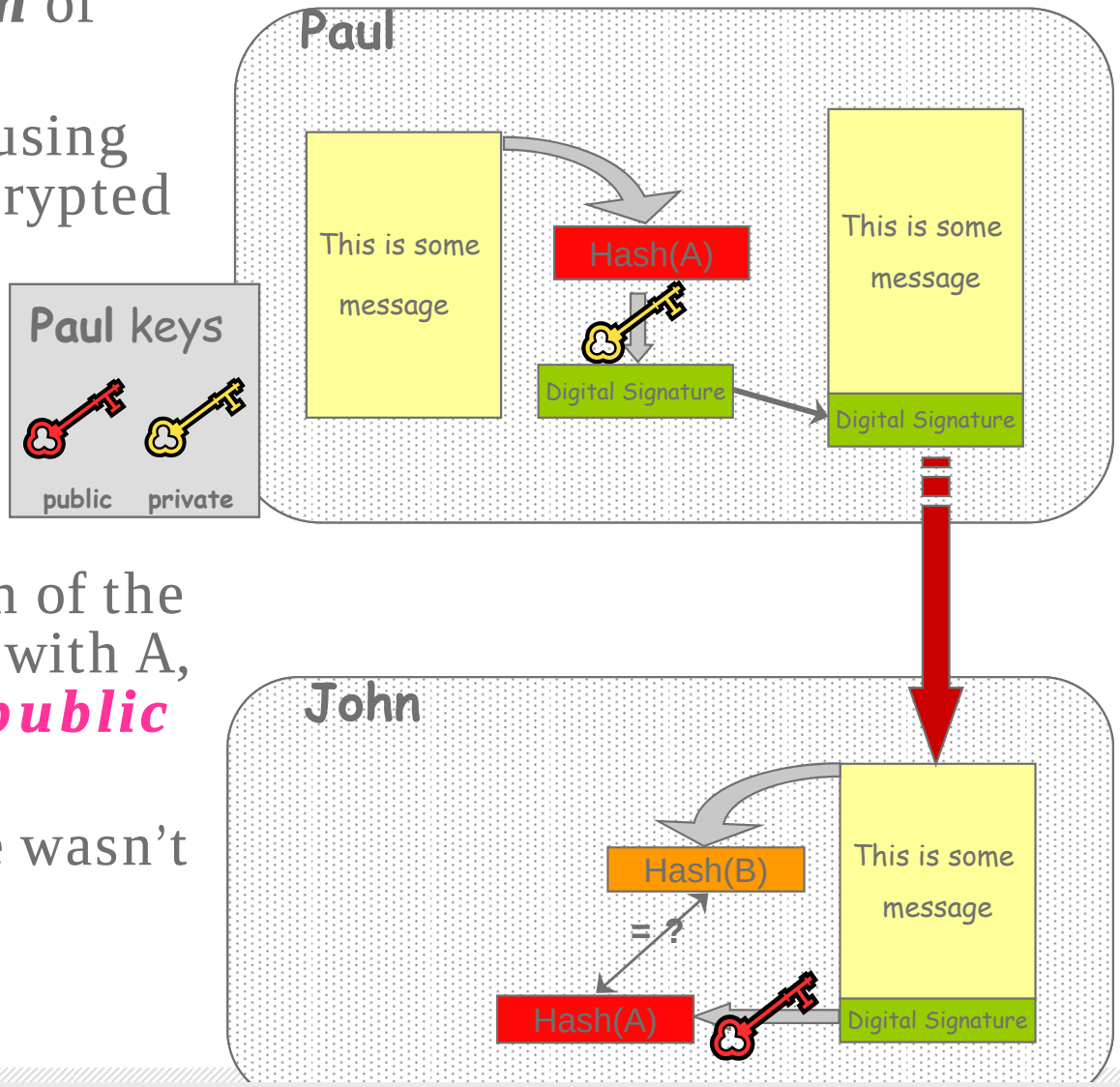
Slide: EGEE presentation

User Identity: Certificates

- Users and resources are typically part of more than one VO,
  - but don't want many passwords
- Users and resource get a *single authentication token* (identity certificate)
  - issued by a party trusted by all ("Certificate Authority"),
  - recognised by many resource providers, users, and VOs
  - in itself does not grant any access, but provides a unique binding between an identifier and the subject
- **This is called your *(identity) certificate***
- **It is a *cryptographically protected statement* by the CA** that you can use to prove your identity **in combination** with a ***private key*** and its ***passphrase***

Digital signatures at work: public & private keys

- **Paul** calculates the ***hash*** of the message
- **Paul** encrypts the hash using his ***private*** key: the encrypted hash is the ***digital signature***.
- **Paul** sends the signed message to **John.**



- **John** calculates the hash of the message and ***verifies*** it with A, decyphered with Paul's ***public*** key.
- If hashes equal: message wasn't modified; **Paul** cannot repudiate it.

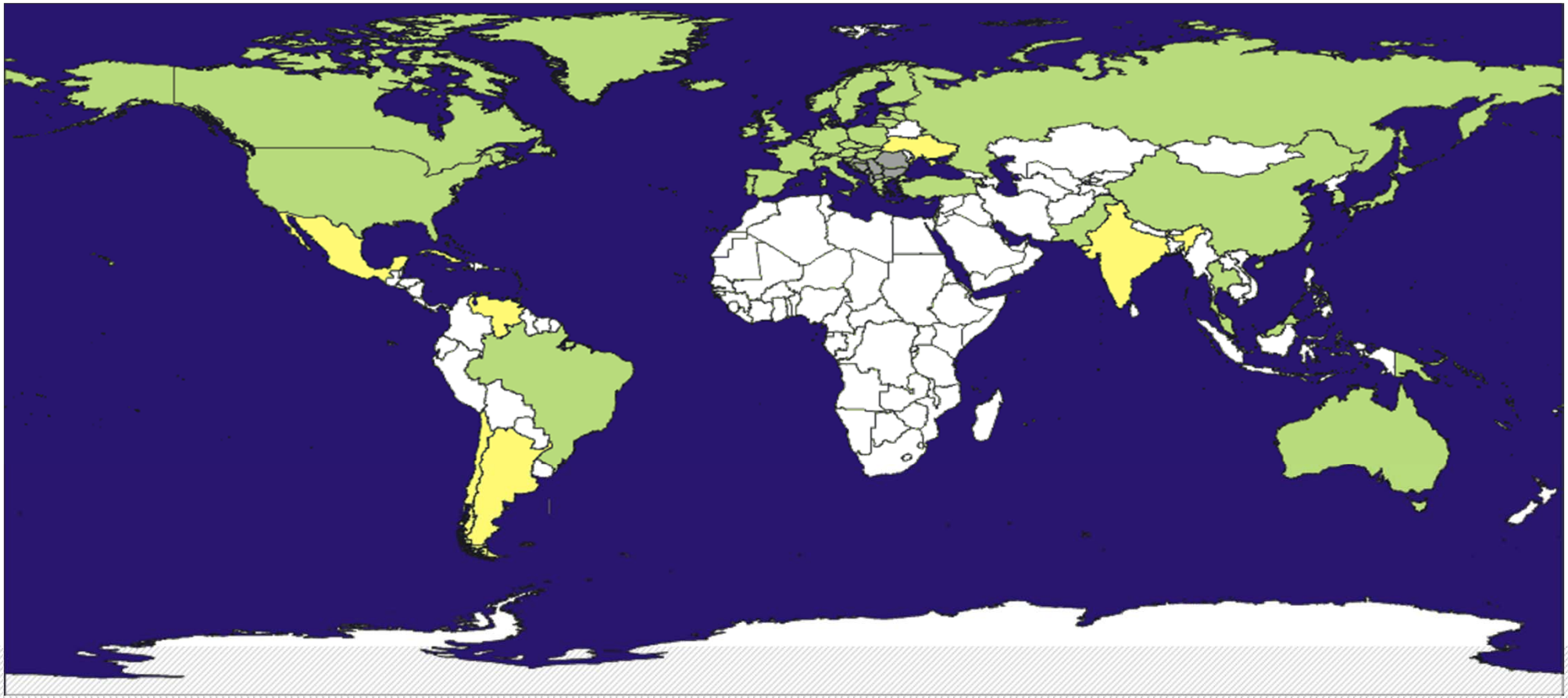
Trusting the signature

- Paul's digital signature is safe if:
  1. Paul's private key is not compromised
  2. John knows Paul's public key
- How can John be sure that Paul's public key is really Paul's public key and not someone else's?
  - A *third party* guarantees the correspondence between public key and owner's identity.
  - Both A and B must trust this third party
  - This third party signs Paul's public key, which is now called a certificate

Trusted third parties

IGTF International Grid Trust Federation AP|EU|TAG

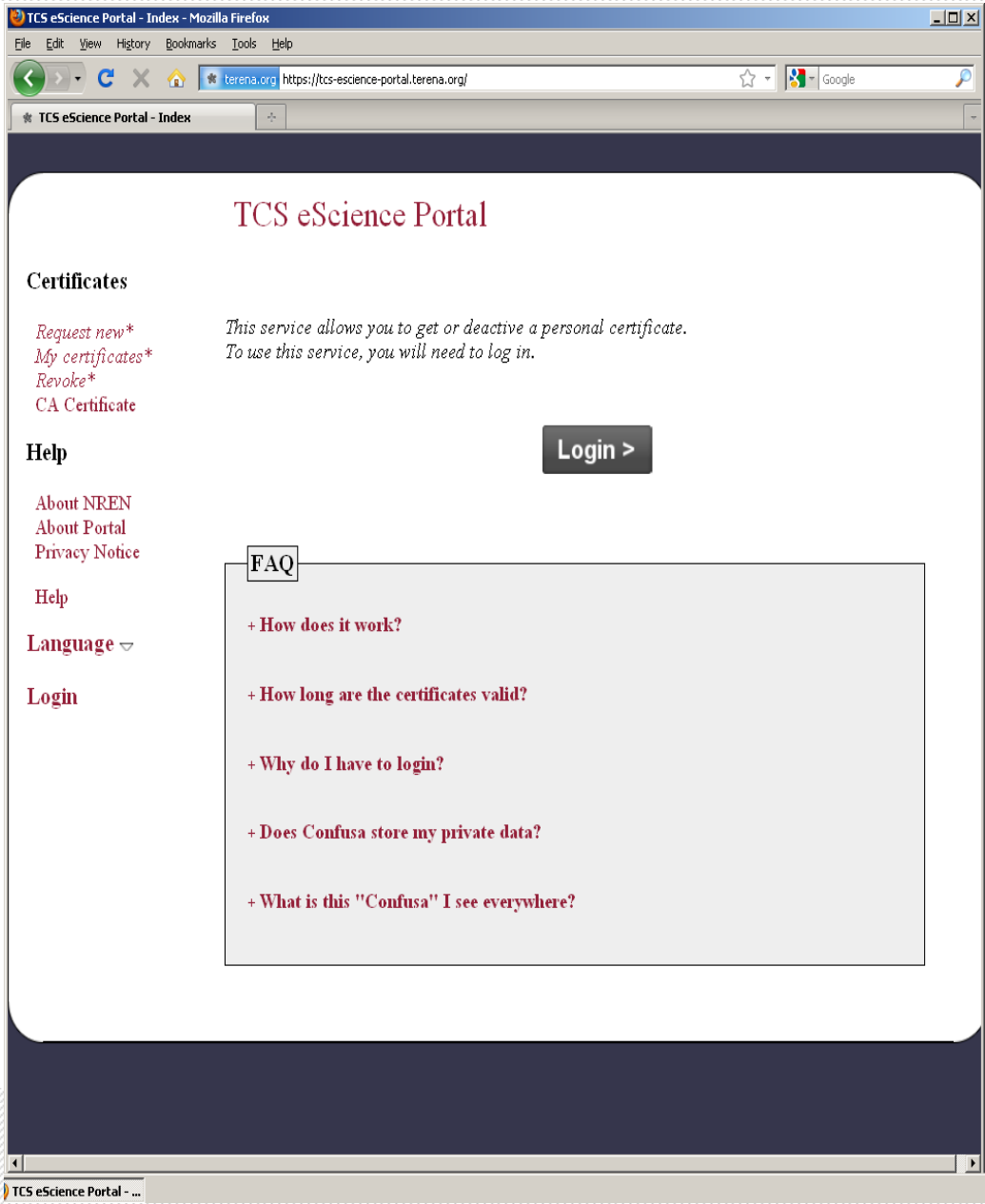
- All research grid infrastructures share the same base set of trusted third parties (‘CAs’)
- There is typically one in each country



rijksuniversiteit groningen

How to get a certificate

- Through Terena e-Science portal: https://tcs-escience-portal.terena.org/
- Identity checked with local organisation (e.g. RUG)
- Some magic still needed to get private key from browser to Grid user interface machine



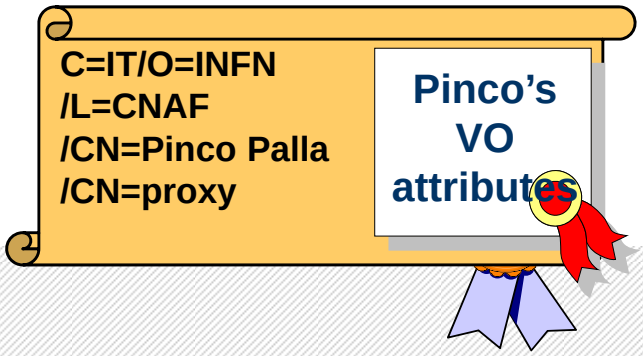
VO affiliation

› Per-VO Authorisations (“visa”)
  - granted to a person or service by a virtual organisation
  - based on the ‘passport’ name
  - acknowledged by the resource owners
  - providers can still ban individual users, and decide which privileges are granted to which VO attributes

In your case, these ‘visa’ are called ***VOMS credentials***

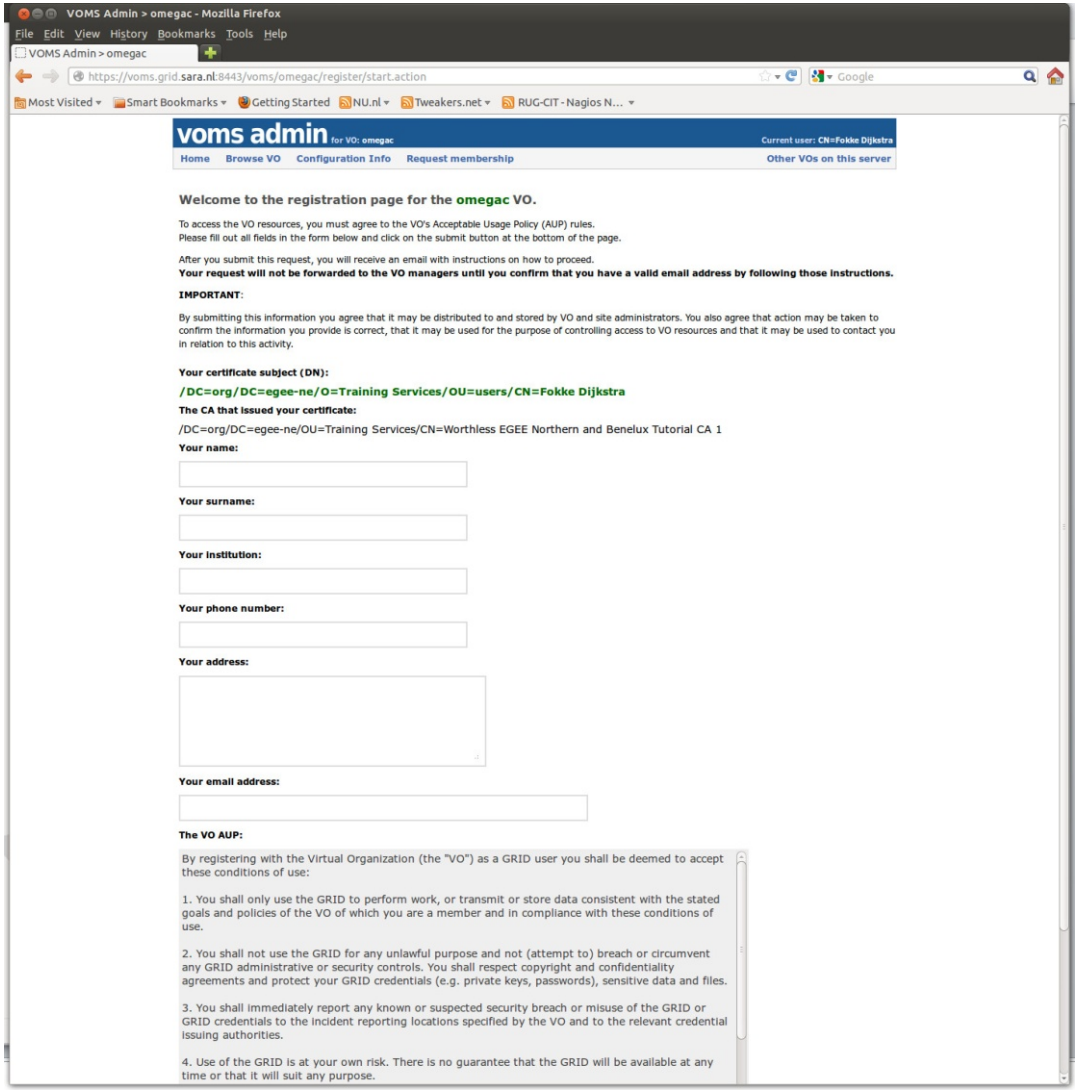
› It is a cryptographically protected statement **by the VO**

› which is bound (by the VO) to your subject name



VOMS server

- Service that takes care of:
  - Member registration
  - Adding VOMS credentials to certificate



Single sign-on and delegation

- To authenticate with your certificate directly you would have to type a passphrase every time
- Also you need a way to send you *VOMS credentials* across
- In the Grid Security Infrastructure today, this is solved by '*proxy certificates*'
  - *a temporary key pair*
  - *in a temporary certificate signed by your 'long term' private key*
  - *valid for a limited time (default: 12 hours)*
  - *and itself not protected by a passphrase*

Getting a VOMS proxy

- VOMS credential consists of a list of attributes that are tied to your proxy certificate
- Groups membership, roles and capabilities may be expressed in a format that binds them together

  <group>/Role=[<role>][/Capability=<capability>]

```
[glite-tutor] /home/giorgio > voms-proxy-init --voms gilda

Your identity: /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
Enter GRID pass phrase: ******

Your proxy is valid until Mon Jan 30 23:35:51 2006
Creating temporary proxy.............................Done

Contacting  voms.ct.infn.it:15001 [/C=IT/O=GILDA/OU=Host/L=INFN
Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.infn.it] "gilda"

Creating proxy ..................................... Done
Your proxy is valid until Mon Jan 30 23:35:51 2006
```

Summary

- (X.509) certificates used in the Grid for users and services
- Used to identify yourself
- Consisting of a private key that you use to sign things
- A public key that others can use to read your messages and that guarantees that you wrote them
- This public key is signed by a trusted 3rd party the Certificate authority
- Short lived proxy certificates without passphrase used for day to day work
- VOMS attributes attached to proxy certificates to show VO membership and other VO related information.