

Grid Security

Fokke Dijkstra Donald Smits Centre for Information Technology



- > 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)





- > 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



rijksuniversiteit User Identity: Certificates groningen

- > 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

rijksuniversiteit groningen Digital signatures at work: public & private keys

public

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



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





> Paul's digital signature is safe if:

2. John knows Paul's public key

A *third party* guarantees the correspondence between public key and owner's identity.

> How can John be sure that Paul's public key is really

- Both A and B must trust this third party
- This third party signs Paul's public key, which is now called a certificate

22-10-2012

rijksuniversiteit groningen Trusting the signature

1. Paul's private key is not compromised



All research grid infrastructures share
 the same base set of trusted third parties ('CAs')

AP|EU|TAG

> There is typically one in each country





rijksuniversiteit How to get a certificate

- Identity checked with local organisation (e.g. RUG)
- Some magic still needed to get private key from browser to Grid user interface machine

	77		
🍪 TCS eScience Portal - Index -	Mozilla Firefox		<u>- 🗆 ×</u>
<u>File Edit View History Book</u>	marks <u>T</u> ools <u>H</u> elp		
🔇 💽 - C 🗙 🏠	terena.org https://tcs-escience-portal.terena.org/	☆ - Google	P
* TCS eScience Portal - Index			-
	TCS escience Portal		
Contificator			
Certificates			
Request new*	This service allows you to get or deactive a personal certificate.		
My certificates*	To use this service, you will need to log in.		
Revoke*			
CA Certificate			
Help	Login >		
About NREN About Postal			
Privacy Notice	P +0		
	FAQ		
Help	There do no theread 9		
Language 🕁	+ riow does it work?		
Login	+ How long are the certificates valid?		
	+ Why do I have to login?		
	+ Does Confusa store my private data?		
	+ What is this "Confusa" I see everywhere?		
	•		



- > 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





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

😣 😑 🐵 🛛 VOMS Admin > om	negac - Mozilla Firefox				
ile Edit View History B	300kmarks Tools Help				
VOMS Admin > omegac	The same all 0.4.2 hours for many free starfs to feature action	Con (1) Man Consile			
			~ m		
Most Visited + ESmart B	Bookmarks 👻 👹 Getting Started 🔊 NU.nl 👻 🔊 Tweakers.net 👻 🔊 RUG-CIT - Nagios N 👻		(-		
	Voms admin for VO: omegac	Current user: CN=Fokke Dijkstra	ſ		
	Home Browse VO Configuration Info Request membership	Other VOs on this server			
	Welcome to the second s				
	Welcome to the registration page for the omegac VO.				
	To access the VO resources, you must agree to the VO's Acceptable Usage Policy (AUP) rules. Please fill out all fields in the form below and click on the submit button at the bottom of the page.				
	After you submit this request, you will receive an email with instructions on how to proceed.	After you submit this request, you will receive an email with instructions on how to proceed.			
	Your request will not be forwarded to the VO managers until you confirm that you have a va	Tour request will not be forwarded to the VO managers until you confirm that you have a valid email address by following those instructions.			
	By submitting this information you areas that it may be distributed to and stored by V/O and site admini	By submitting this information you agree that it may be distributed to and stored by VO and site administrators. You also agree that action may be taken to			
	or purnicular this intermation you give that it may be assumed to this society of you and see assume confirm the information you provide is correct, that it may be used for the purpose of controlling access in relation to this activity.	to VO resources and that it may be used to contact you			
	Your certificate subject (DN):				
	/DC=org/DC=egee-ne/O=Training Services/OU=users/CN=Fokke Dijkstra				
	The CA that issued your certificate:	v Tutorial CA 1			
	Your name:	k lutonal CA 1			
	Your surname:				
	Your Institution:				
	Your phone number:				
	Your address:				
	Your email address:				
	by registering with the virtual organization (the vol) as a GRID user you shall be dee these conditions of use:	emed to accept			
	 You shall only use the GRID to perform work, or transmit or store data consistent w goals and policies of the VO of which you are a member and in compliance with these use. 	vith the stated conditions of			
	2. You shall not use the GRID for any unlawful purpose and not (attempt to) breach or any GRID administrative or security controls. You shall respect copyright and confident agreements and protect your GRID credentials (e.g. private keys, passwords), sensitive	r circumvent ⁱ tiality e data and files.			
	 You shall immediately report any known or suspected security breach or misuse of t GRID credentials to the incident reporting locations specified by the VO and to the rele Issuing authorities. 	the GRID or evant credential			
	 Use of the GRID is at your own risk. There is no guarantee that the GRID will be availine or that it will suit any purpose. 	ailable at any			



- 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



- 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



- > (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.