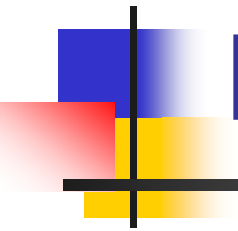


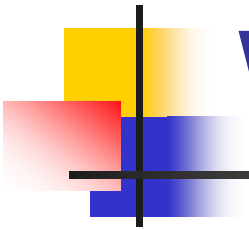
Kerberos and Grids

Daniel Kouřil, Luděk Matyska, Michal Procházka, Tomáš Závodný

Masaryk University & CESNET

email: first.last@cesnet.cz

AFS & Kerberos Best Practices Workshop, SLAC, 2007



What is grid?

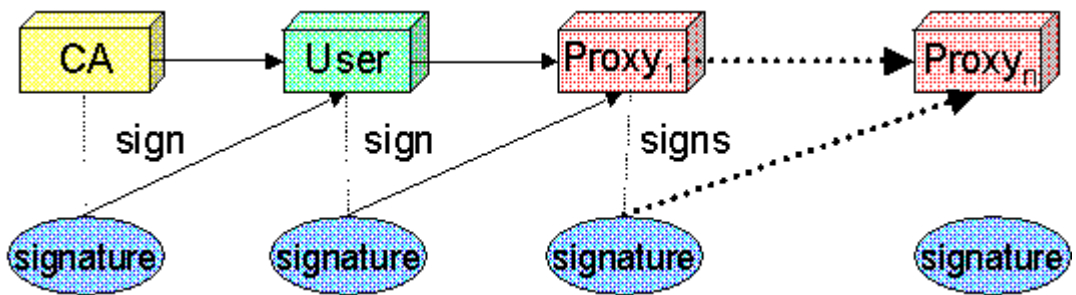
- model of distributed processing of information
  - sharing multiple resources
  - coupling users working on the same projects
  - providing easy access to the infrastructure
- several types of grids nowadays
  - computing grids, data grids, collaborative grids
  - a three-point definition (by Ian Foster):
    - coordinates resources that are not subject to centralized control
    - uses standard and open protocols
    - provides non-trivial quality of service

Authentication model

- Public Key Infrastructure (PKI)
  - Each participant owns a digital certificate (X.509)
- users are uniquely identified by DN from their certificates
  - non-overlapping name spaces
    - guaranteed by the CA policies
- IGTF - a federation of trusted CAs
  - not limited to Grids
  - almost 70 CAs from all the world accredited

X.509 proxy certificate

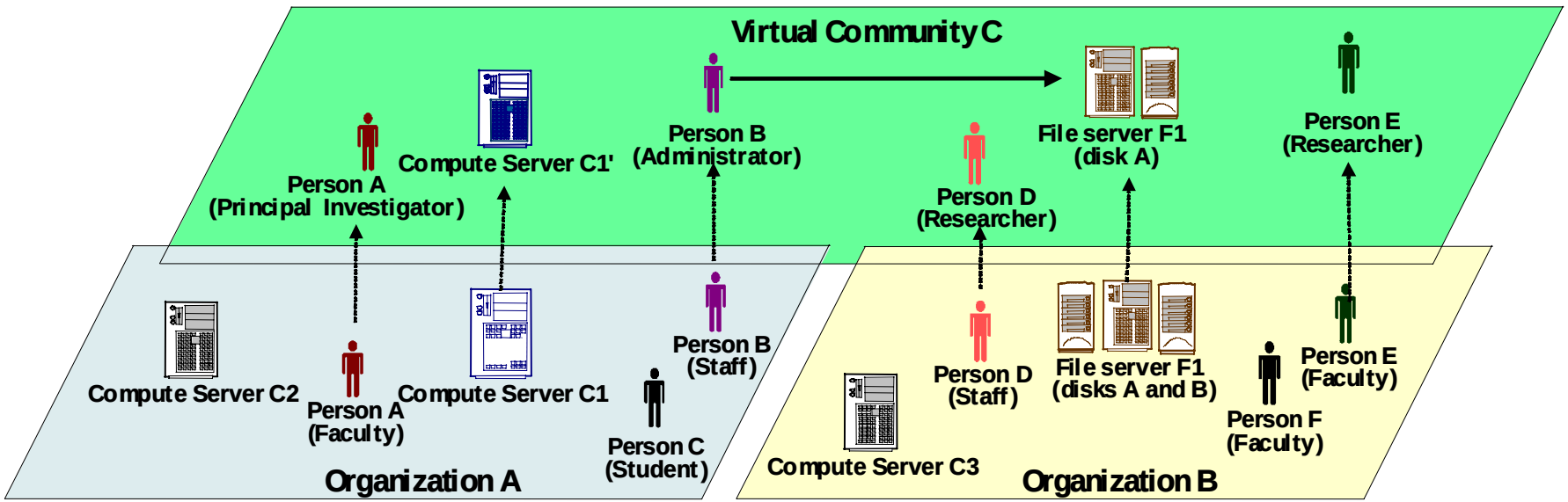
- a new certificate, derived from from normal certificates and another proxy
  - the latest format standardized rfc3820, support in openssl;
- means of SSO and delegation
  - similarly to kerberos tickets
- short time, private key stored less securely
- a significant change of PKI mode
  - proxy is signed by the user, not CA



picture from www.globus.org

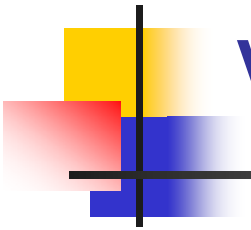
Virtual organization

- additional administrative level
  - connecting users, resources, …
  - spans organizational boundaries
  - e.g. researchers participating in a project

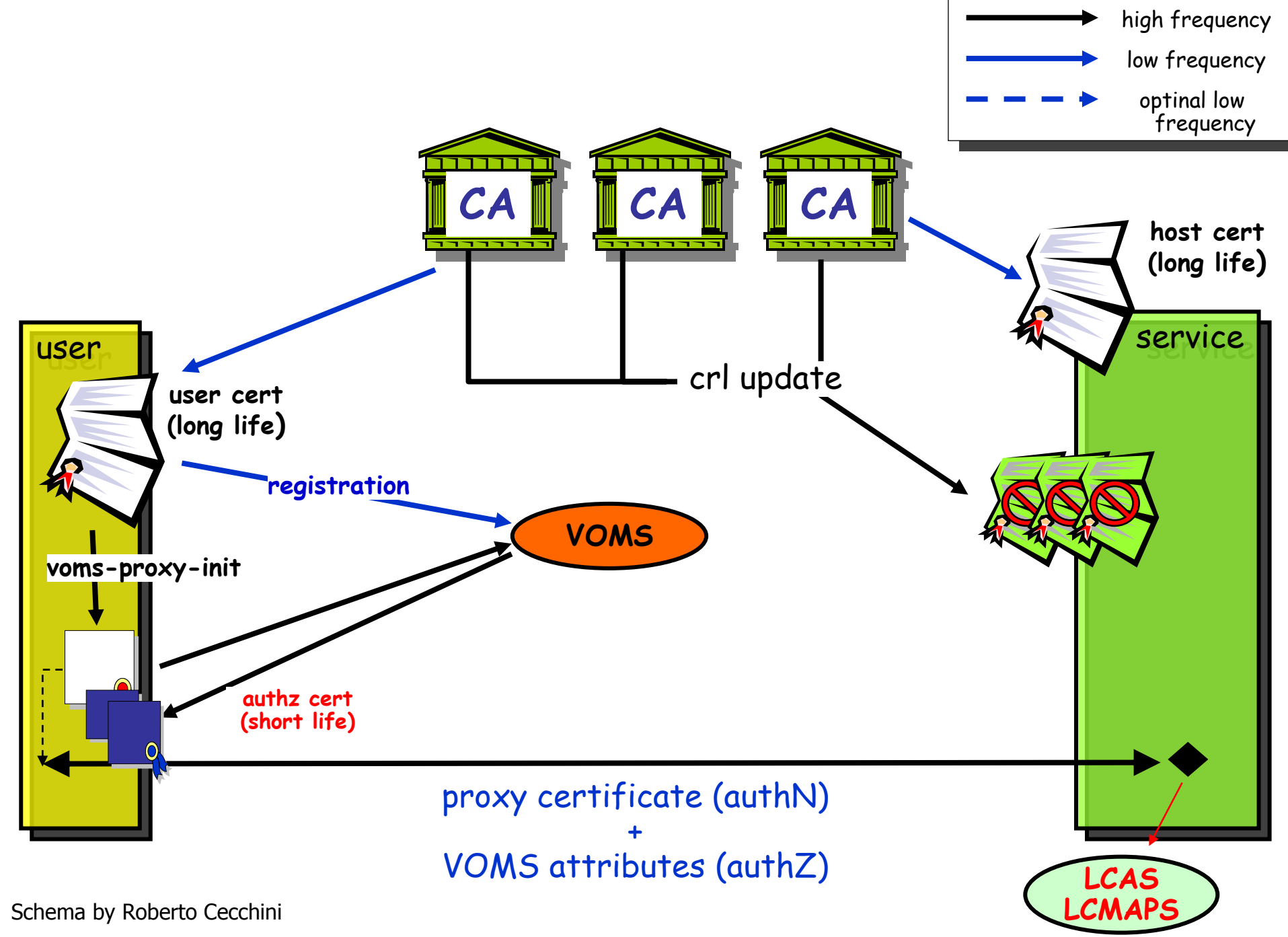


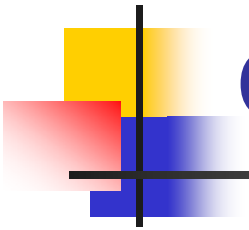
schema from: "The OGSA Architecture, v. 1.0", GFD-I.030 (OGF)

VO Management Service (VOMS)



- An attribute service to maintain VOs
  - push model
  - assigns roles and group memberships to users
- Attribute certificates
  - binding user id with her attributes in a VO
  - limited lifetime
    - no revocation mechanism for VOMS attribute certs
  - Full Qualified Attribute Names (FQANs)
    - single-line representation of the attributes
    - /VOCE/Users/Role=Administrator
  - IETF RFC 3281


high frequency
low frequency
optinal low frequency
CA
CA
CA
host cert
(long life)
service
user
crl update
user cert
(long life)
registration
VOMS
voms-proxy-init
authz cert
(short life)
proxy certificate (authN)
+
VOMS attributes (authZ)
LCAS
LCMAPS
Schema by Roberto Cecchini



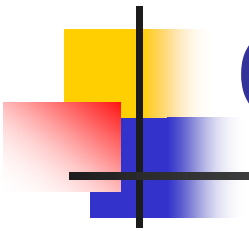
on-line credential services

- on-line credential repository (OCR) - MyProxy
  - storage maintaining users‘ credentials
  - user can obtain them when and where needed
  - more secure private key storage than users‘ systems
  - supports many authN mechanisms (password, Kerberos, OTP, ...)
- on-line certification authority
  - sign certificates to „known“ users on demand
  - short-time certificates, based on the original credential lifetime
  - kCA, Heimdal KDC, MyProxy

Kerberos & Grid

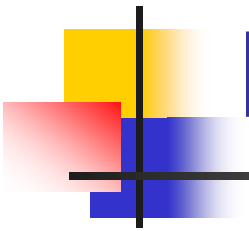
- Our users want to access Grid systems
  - have or not a PKI certificate
  - „multi-mechanism“ SSO
- Our resources are available from a grid
  - resources use Kerberos or
  - resources can be made understand PKI
- Leverage existing authZ infrastructure?
  - VOMS is widely used

Combined log-on

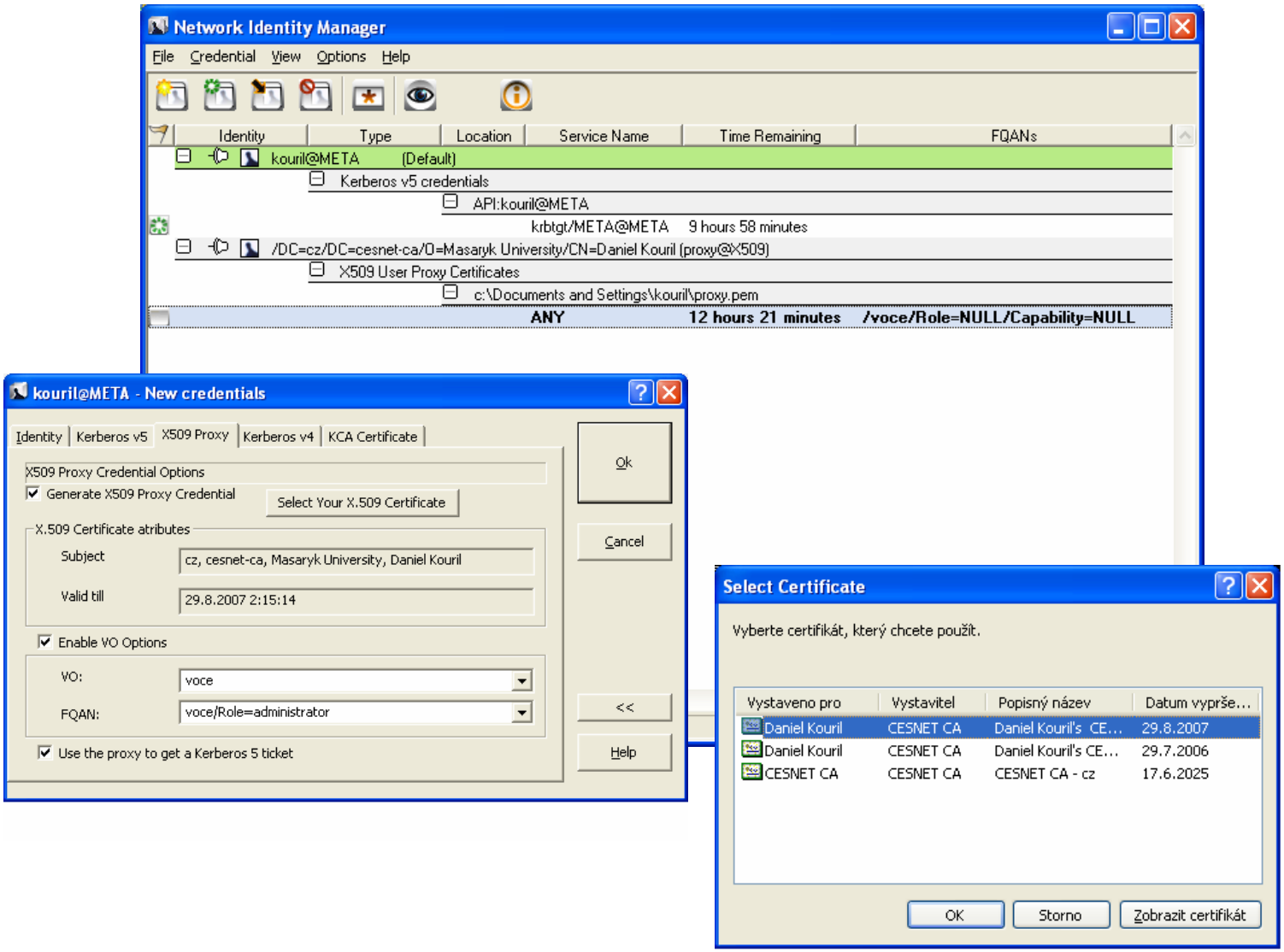


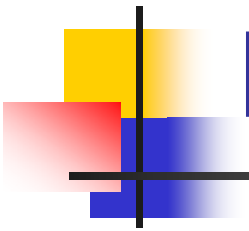
- Targeting at MS Windows
  - Linux users are used to CLI
- Users have or don‘t have certificates
  - A kerberized on-line CA
    - accreditation by the IGTF
    - kCA plugin to NetIdMgr
  - A kerberized on-line credential repository
    - for users who don‘t want maintain their creds
- Simple user‘s login mechanisms
  - ideally integrating Kerberos (local) and PKI
- Applications support

Proxy support in NetIdMgr



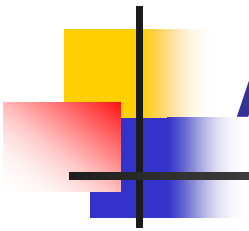
- A plugin to manage proxy certificates
- Implemented as a credential provider
  - tied with Kerberos identity
  - invoked after getting a Kerberos ticket
  - creating all credentials at once (SSO)
- Supports VOMS AC retrieval
- Various PKI data storage locations
  - files, #PKCS11, MS CryptoStore
- Preliminary PKINIT support
  - using Heimdal libraries ported to Win32


Network Identity Manager
File Credential View Options Help
Identity Type Location Service Name Time Remaining FQANs
kouril@META (Default)
Kerberos v5 credentials
API:kouril@META
krbtgt/META@META 9 hours 58 minutes
/DC=cz/DC=cesnet-ca/O=Masaryk University/CN=Daniel Kouril (proxy@X509)
X509 User Proxy Certificates
c:\Documents and Settings\kouril\proxy.pem
ANY 12 hours 21 minutes /voce/Role=NULL/Capability=NULL
kouril@META - New credentials
Identity Kerberos v5 X509 Proxy Kerberos v4 KCA Certificate
X509 Proxy Credential Options
Generate X509 Proxy Credential
Select Your X.509 Certificate
X.509 Certificate atributes
Subject
cz, cesnet-ca, Masaryk University, Daniel Kouril
Valid till
29.8.2007 2:15:14
Enable VO Options
VO:
voce
FQAN:
voce/Role=administrator
Use the proxy to get a Kerberos 5 ticket
Ok
Cancel
<<
Help
Select Certificate
Vyberte certifikát, který chcete použít.
Vystaveno pro Vystavitel Popisný název Datum vyprše...
Daniel Kouril CESNET CA Daniel Kouril's CE... 29.8.2007
Daniel Kouril CESNET CA Daniel Kouril's CE... 29.7.2006
CESNET CA CESNET CA CESNET CA - cz 17.6.2025
OK
Storno
Zobrazit certifikát



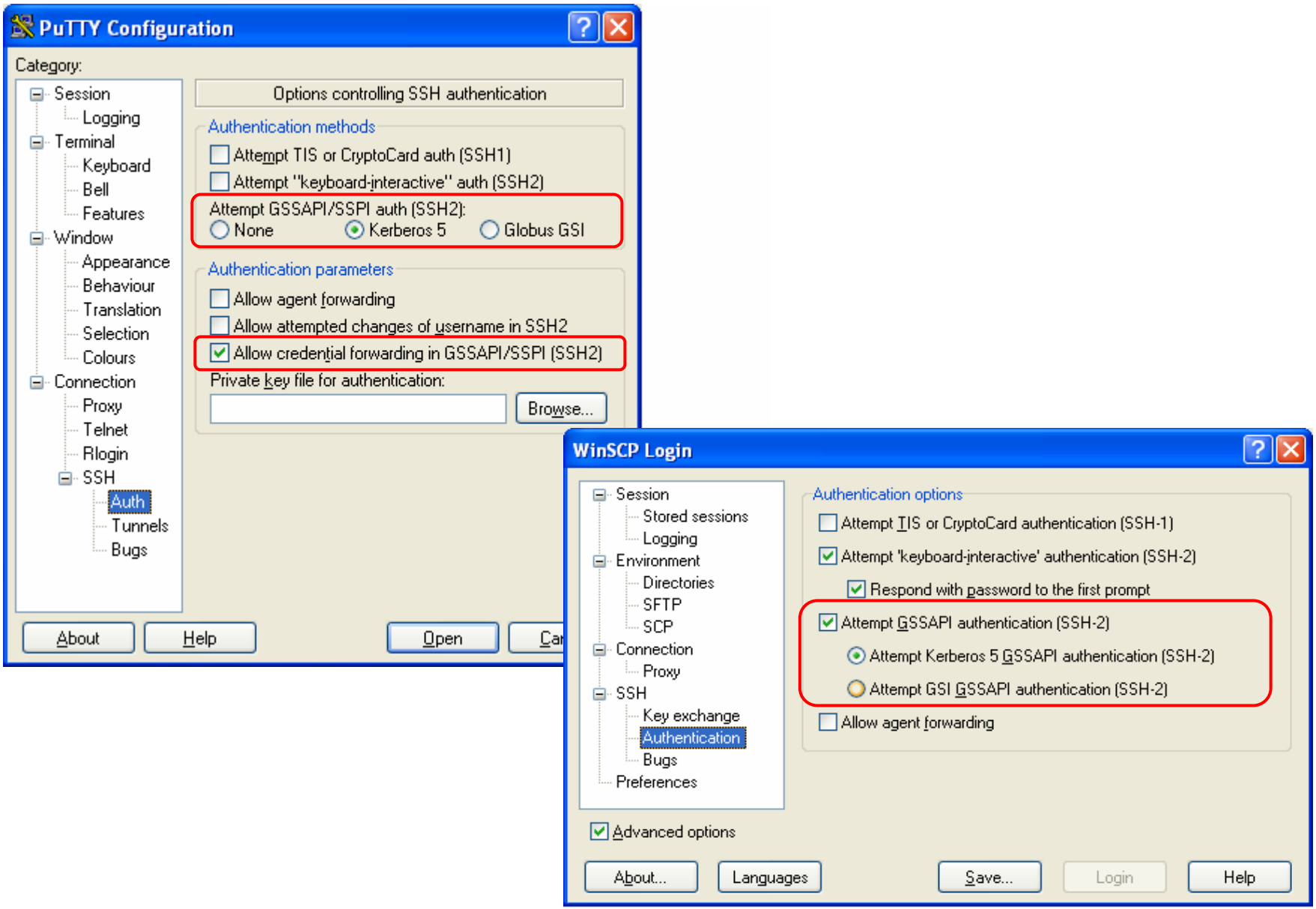
Future work on plugin

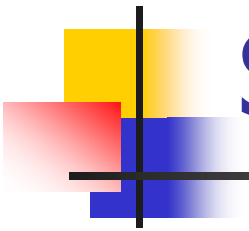
- Implement an identity provider
  - to be useful for broad Grid community
- PKINIT support
  - especially for smart card users
  - to minimize user intervention
- Support proxy retrieval from OCR
  - using a Kerberos ticket or another certificate
- More secure storage of proxies
  - requires adaptation on the applications side, too



Application support

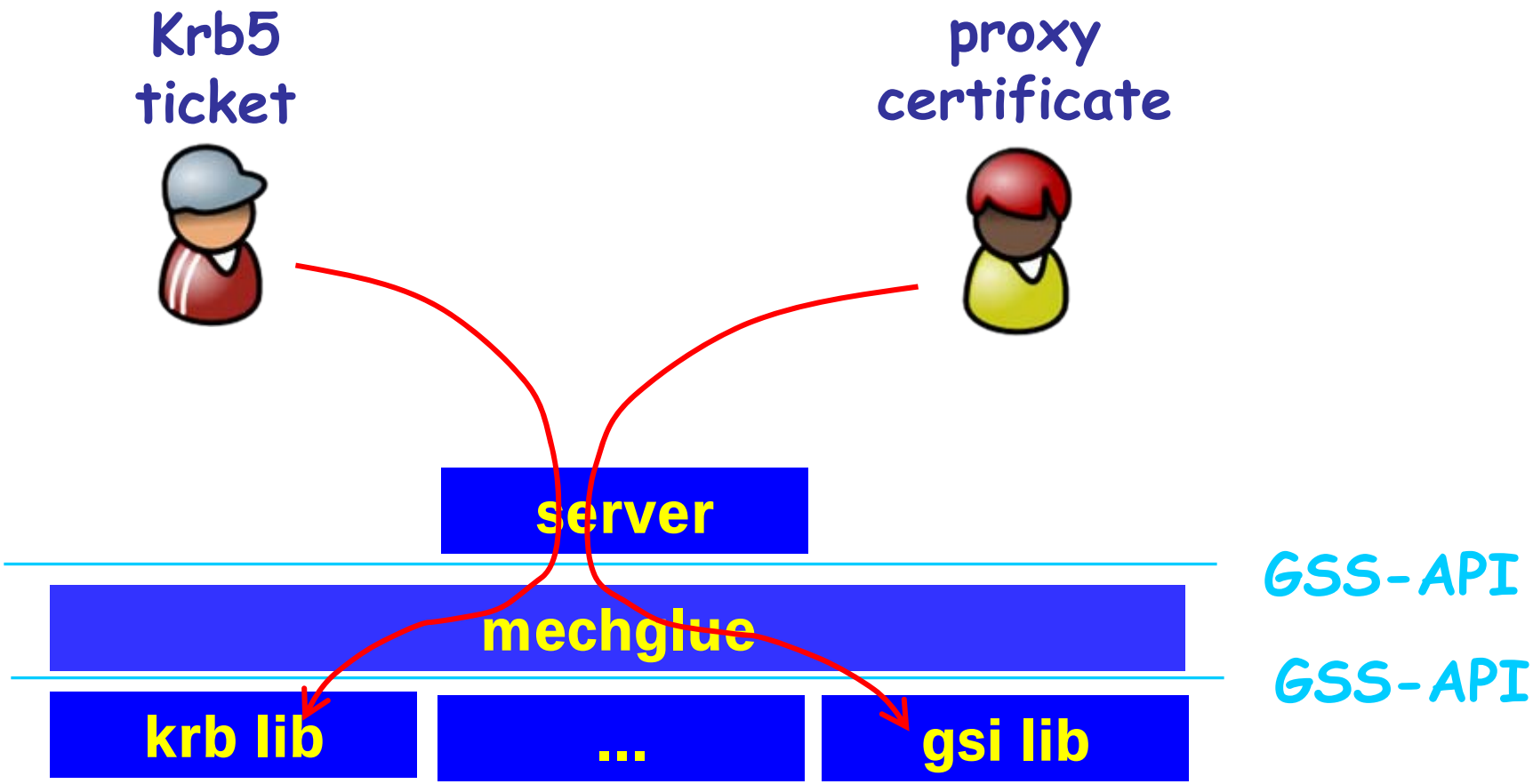
- Grid User Interface machines
  - providing all middleware necessary
  - Accessible using SSH
- Putty & WinSCP supporting Krb & proxy
  - based on GSS-API authentication
    - a third-party patch
  - can be used to support both mechanisms
    - user must choose one
  - binary versions available from meta.cesnet.cz

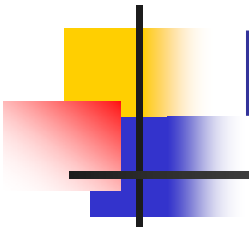

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Proxy
Telnet
Rlogin
SSH
Auth
Tunnels
Bugs
Options controlling SSH authentication
Authentication methods
Attempt TIS or CryptoCard auth (SSH1)
Attempt "keyboard-interactive" auth (SSH2)
Attempt GSSAPI/SSPI auth (SSH2):
None
Kerberos 5
Globus GSI
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH2
Allow credential forwarding in GSSAPI/SSPI (SSH2)
Private key file for authentication:
Browse...
About
Help
Open
WinSCP Login
Session
Stored sessions
Logging
Environment
Directories
SFTP
SCP
Connection
Proxy
SSH
Key exchange
Authentication
Bugs
Preferences
Authentication options
Attempt TIS or CryptoCard authentication (SSH-1)
Attempt 'keyboard-interactive' authentication (SSH-2)
Respond with password to the first prompt
Attempt GSSAPI authentication (SSH-2)
Attempt Kerberos 5 GSSAPI authentication (SSH-2)
Attempt GSI GSSAPI authentication (SSH-2)
Allow agent forwarding
Advanced options
About...
Languages
Save...
Login
Help



Server support

- Clients can use Kerberos or proxies
- Running separate binaries on different ports
  - complex to manage
  - client re-configuration necessary
- Main servers use GSS-API
- Mechglue helps to choose correct GSS-API library
  - a thin layer between an application and several GSS-API libraries

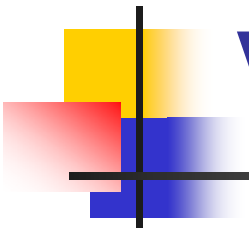

Krb5
ticket
proxy
certificate
server
mechglue
krb lib
...
gsi lib
GSS-API
GSS-API



Mechglue and gsi-openssh

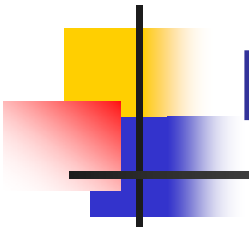
- gsi-openssh
  - patch for OpenSSH maintained by NCSA
  - based on the Simon Wilkinson's patch
  - supports using mechglue
- Can be applied to other services too
  - a CVS server at MU

VOMS in Kerberos

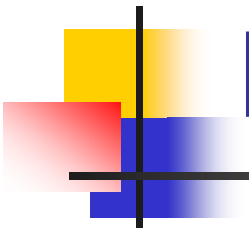


1. retain VO information for „foreign“ users comming to a Kerberos domain
   - to set priorities on jobs etc.
2. leverage a widely used authZ solution
   - VOMS is becoming the key AuthZ corner-stone in Grids

Embedding VOMS attributes in tickets

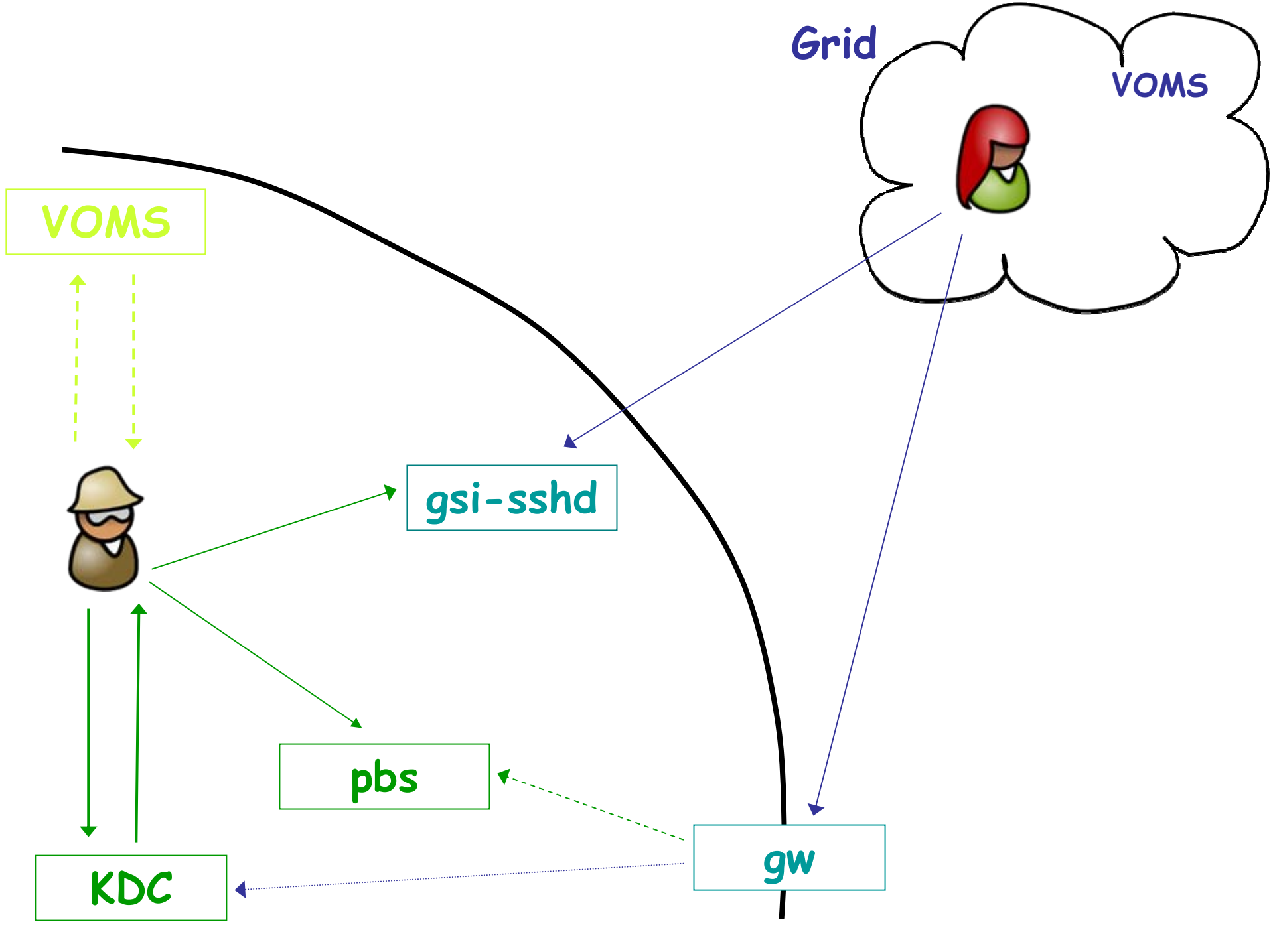


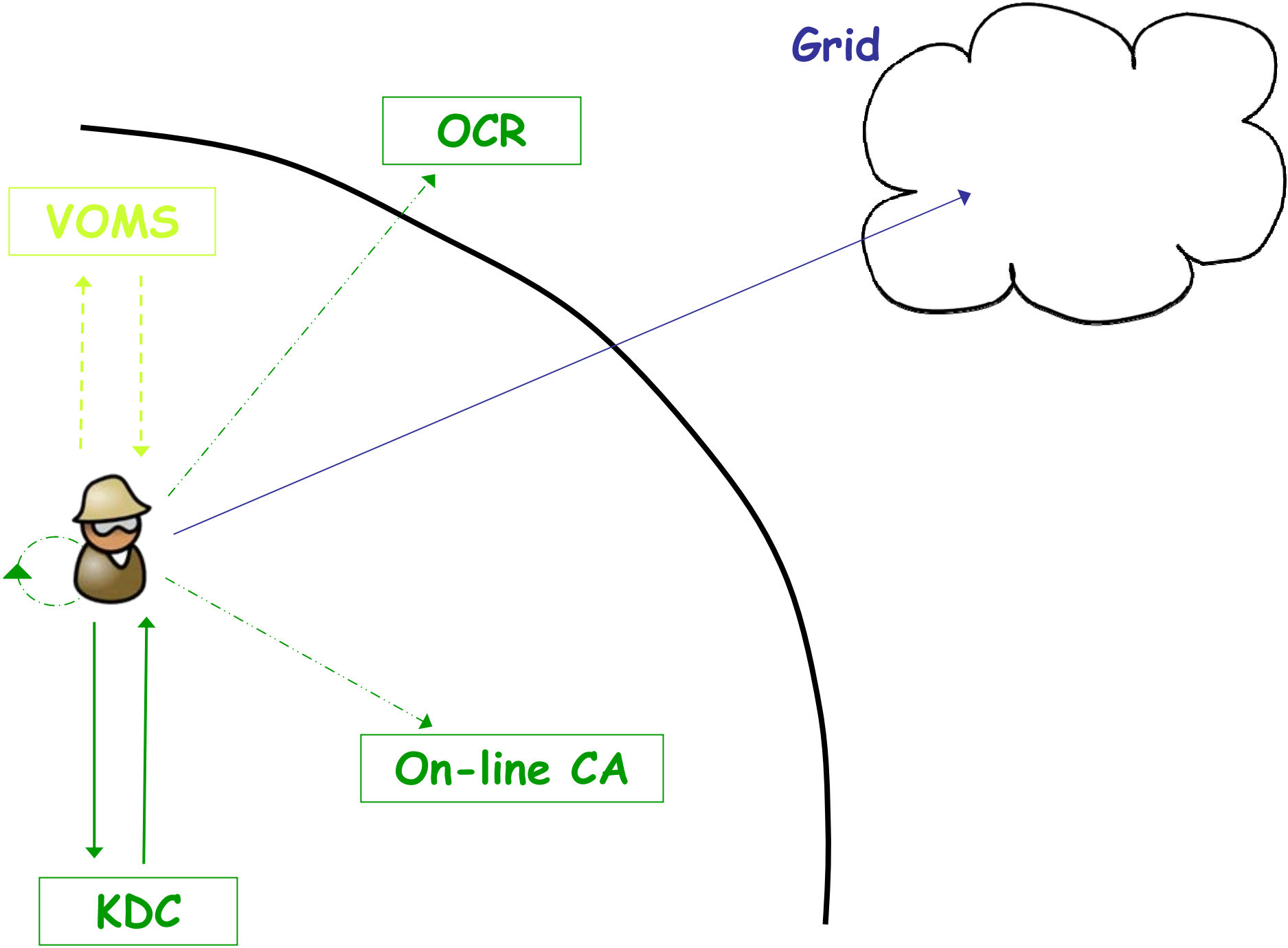
- The clients use only ticket for local authentication
  - tickets contain the authorization data field
- Clients (can) present their VOMS attributes to the KDC
  - PKINIT
  - the KDC can put the VOMS certificate into TGT and all derived tickets
  - end service can search the authorization field upon verifying the ticket
- Similar to MS PAC
  - attribute service isn't co-allocated with the KDC



Prototype implementation

- Support in the Heimdal KDC
  - it supports proxy certificates (only RFC-compliant though)
- A simple server using the authorization field
  - experimenting with gsi-ssh and its session hooks (to be independent on the application)
- The client part remains unchanged


Grid
VOMS
VOMS
gsi-sshd
pbs
gw
KDC


Grid
OCR
VOMS
On-line CA
KDC