

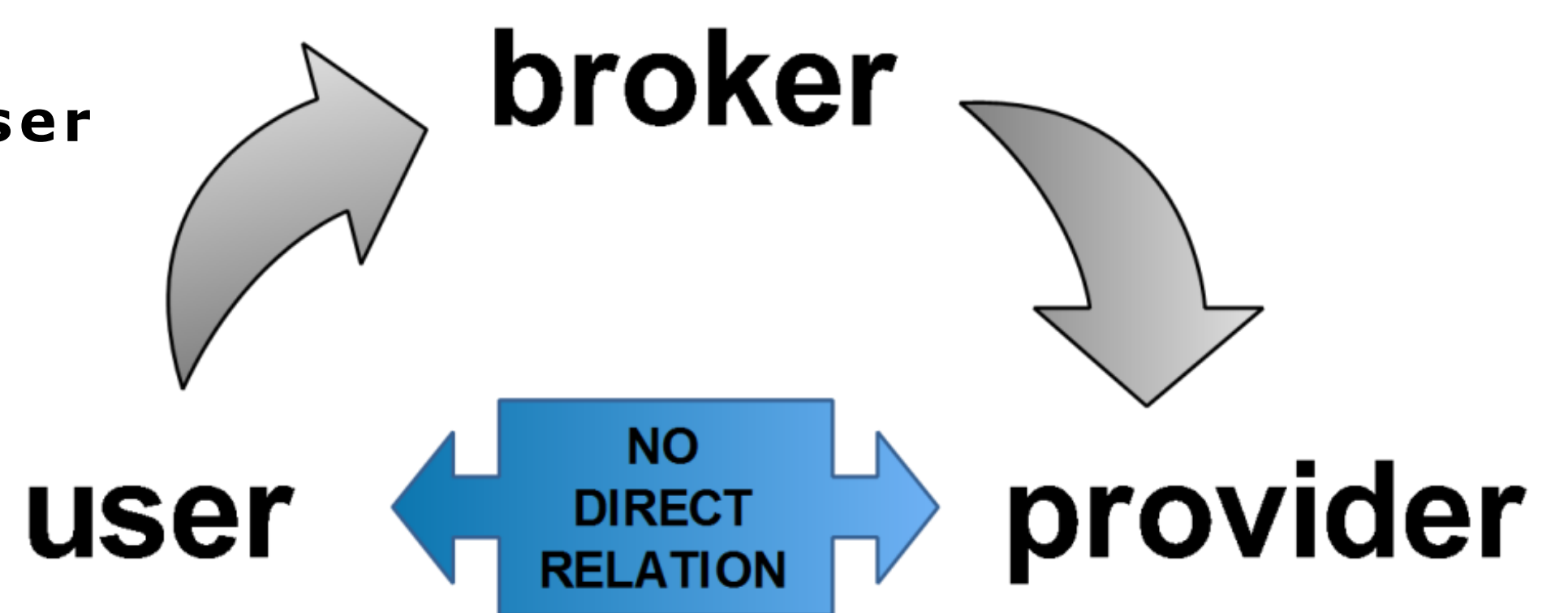
Mediated definite delegation

Certified Grid jobs in ALICE and beyond

Steffen Schreiner, Costin Grigoras, Latchezar Betev, Maarten Litmaath and Johannes Buchmann

Challenge of delegation

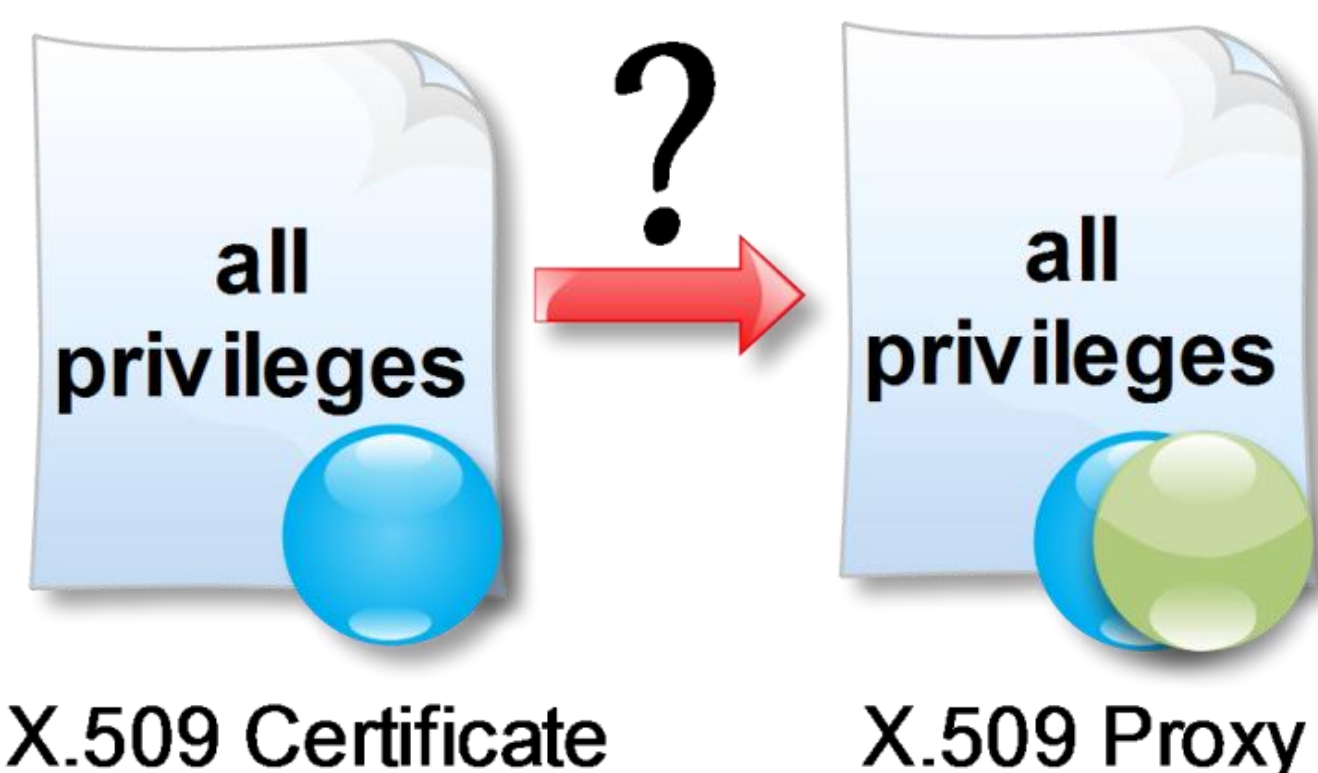
- Allow some provider¹ to do a job **in the name of a user**
- But let a **broker**² decide which provider it will be
- Prove that the **user wants this job** to be done
- Prove that this provider may do **nothing else**
- Prove that **nobody else** may do anything else



¹ e.g. Worker Node

² e.g. Central Grid management system

Problems with X.509 proxy certificates



- Provide **no correlation** with an actual delegation (*several jobs*)
- Can have an **arbitrary period of validity** (*weeks, months, ...*)
- **Allow for misuse** by any owner (*no trusted transfer/propagation*)
- Provide **no theft protection** (copy and use it)
- Might lead to identity theft
- Additional services and callbacks necessary (e.g. for renewal)

A new model of mediated definite delegation

$U = \{ u : \text{user able to delegate tasks} \}$

$P = \{ p : \text{delegable interaction /privilege} \}$

$E = \{ e : \text{entity, as e.g. a Grid job or file} \}$

$A = \{ a : \text{agent, able to execute tasks on behalf of users} \}$

$\mathbb{T} = \{ t : \text{period of validity} \}$

$B = \{ b : \text{request broker} \}$

$\mathbb{D} = \{ d : \text{unmediated delegation} \}$

$C = \{ c : \text{derivative, verifiable transformation of } d \}$

$D = \{ d : \text{mediated delegation} \}$

Unmediated delegation

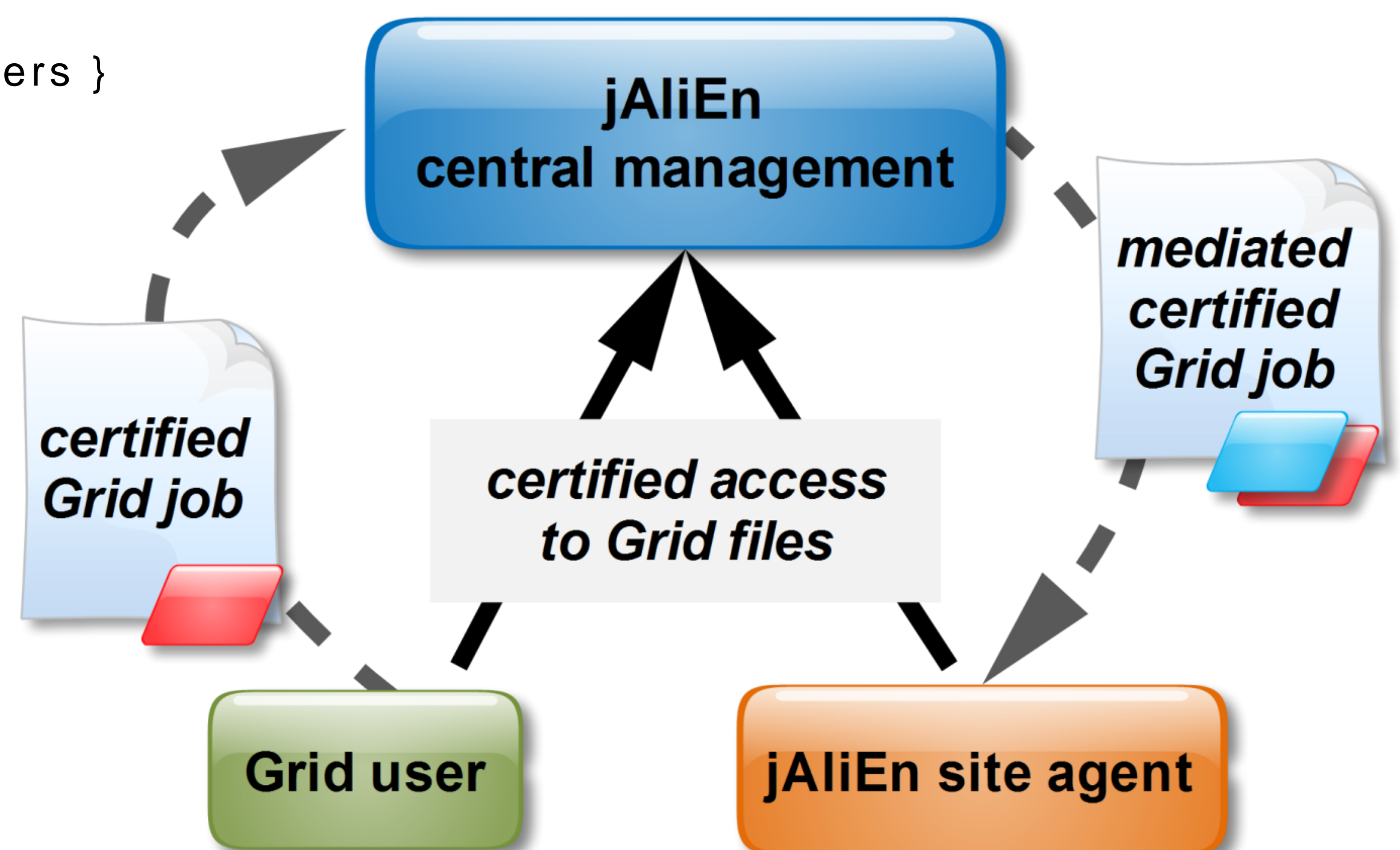
$$\phi : U \times P \times E \times B \times \mathbb{T} \rightarrow \mathbb{D}$$

Mediated delegation

$$\psi : \mathbb{D} \times \mathcal{P}(C) \times A \times \mathbb{T} \rightarrow D$$

Relayed unmediated delegation

$$\delta : \mathbb{D} \times \mathcal{P}(C) \times B \times \mathbb{T} \rightarrow \mathbb{D}$$

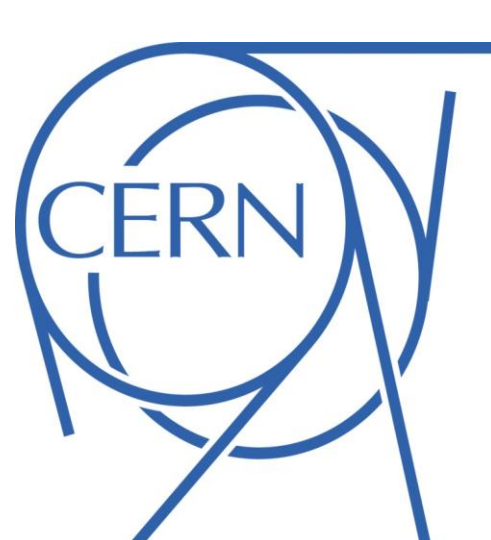


jAliEn - Certified grid jobs and files

- A Grid job is **digitally signed** by the user and all brokers
- Digitally signed Grid file Catalogue entries
- Allows **full authentication** of Grid jobs on a site
- Site is allowed to **do only what a job specifies**
- User is **protected from identity theft**
- **Misuse can be identified** and resulting data removed
- Provides **non-repudiation** if software is trustable



<http://jAliEn.cern.ch>



CHEP 2012
New York University's Skirball Center and Kimmel Center
New York
May 21st – 25th 2012