

Grid Middleware Meeting

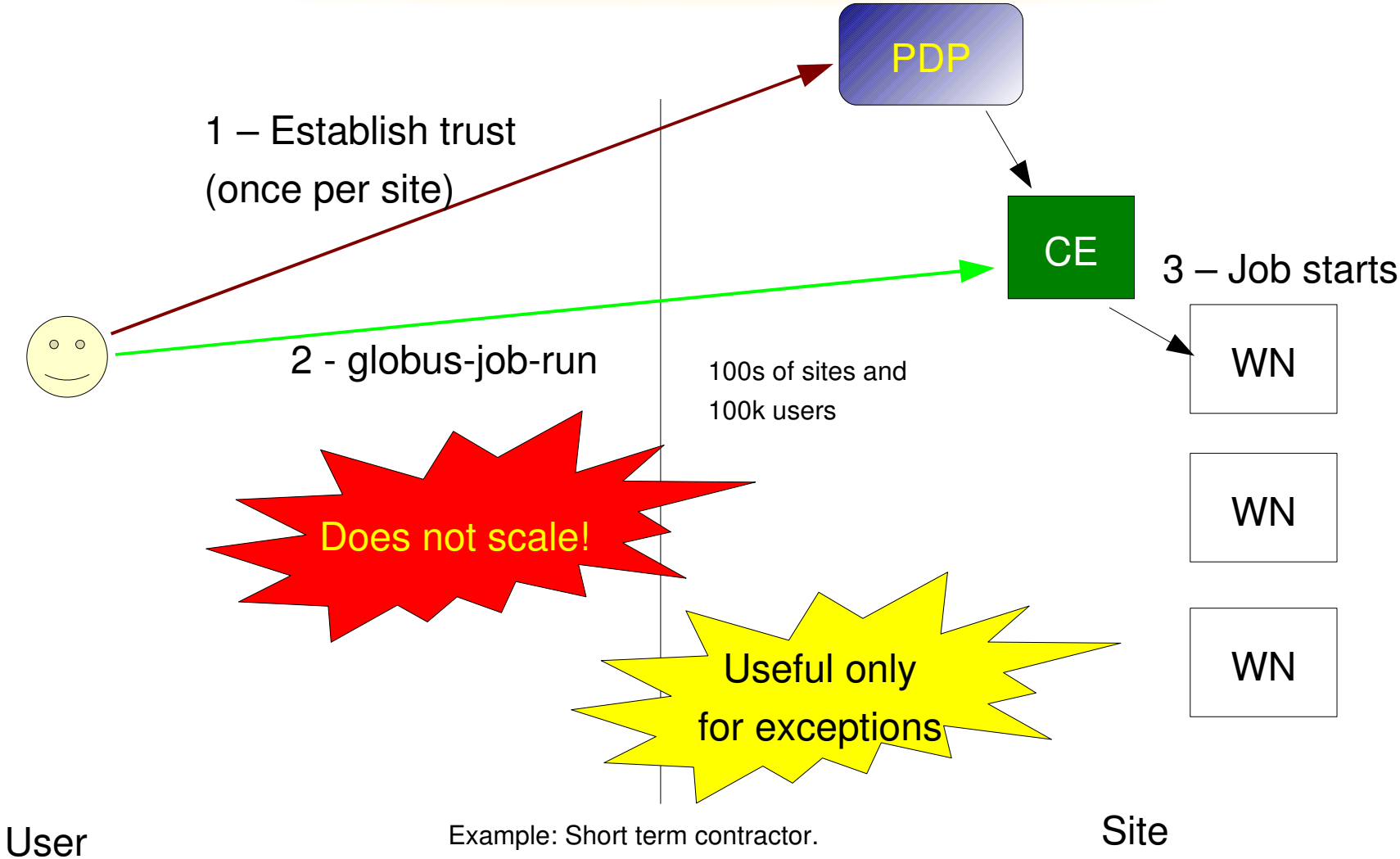
Real life and The Chain of Trust

by Igor Sfiligoi

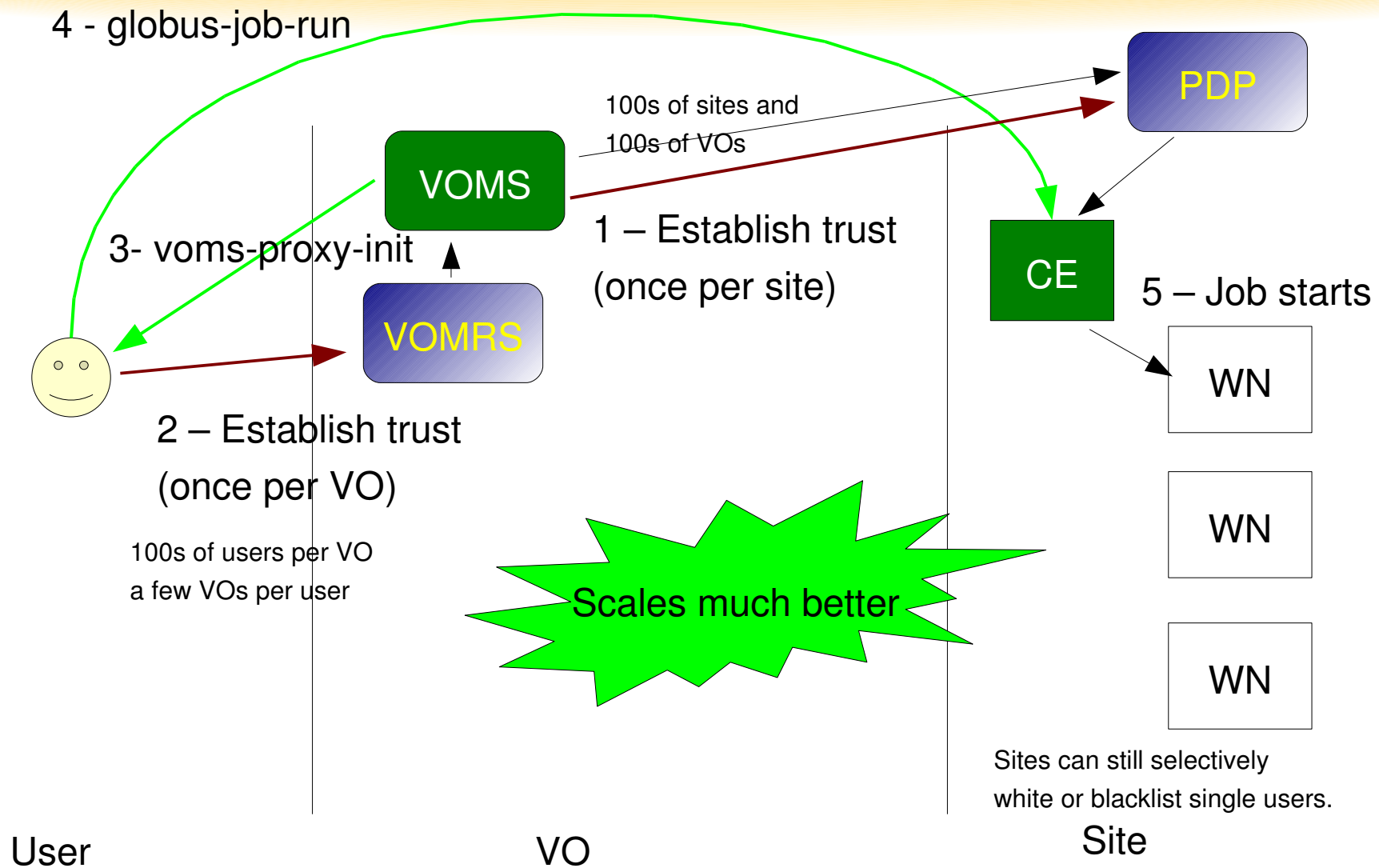
The Grid world

- The Grid is composed of two parties
 - Users (looking for resources)
 - Computing Sites (providing resources)
- The Grid is supposed to be generic
 - No technical restrictions on what is run on the resources, only **usage policies**
- But this implies that Sites trust the Users

Site trusts user



Site trusts VO that trusts user

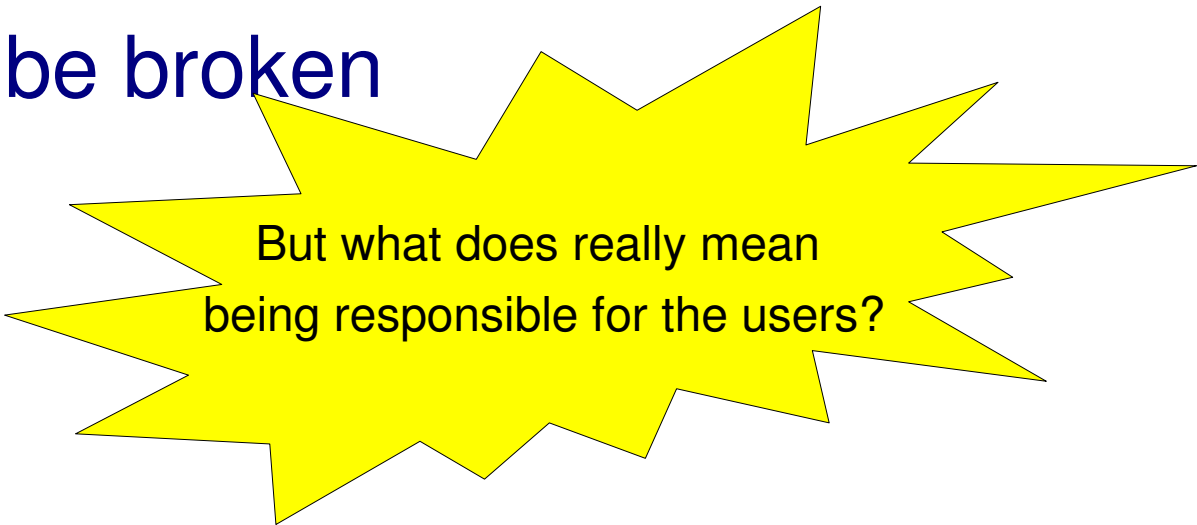


With delegation come responsibilities

- Sites don't trust the users Users directly, anymore
 - They trust them because a higher body guarantees for them!
- All links in the Chain of Trust must behave properly
 - If a single piece of the chain fails, the whole chain is broken!

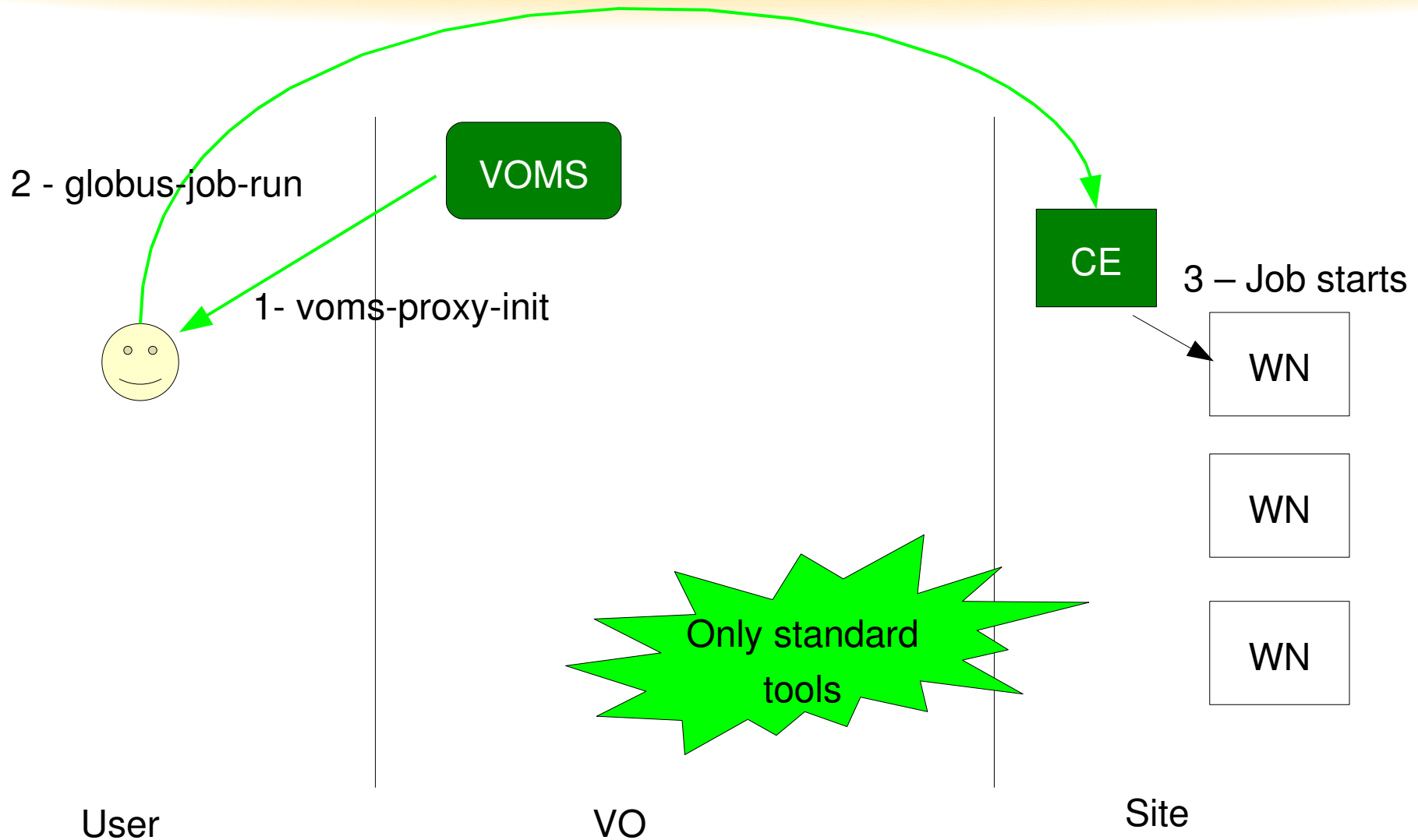
VOs need to be responsible

- VOs guarantee for their users
- If a VO is notified that a user misbehaved
 - **The VO needs to take action against the user**
- If a VO fails to correct the problem, the trust relationship will be broken

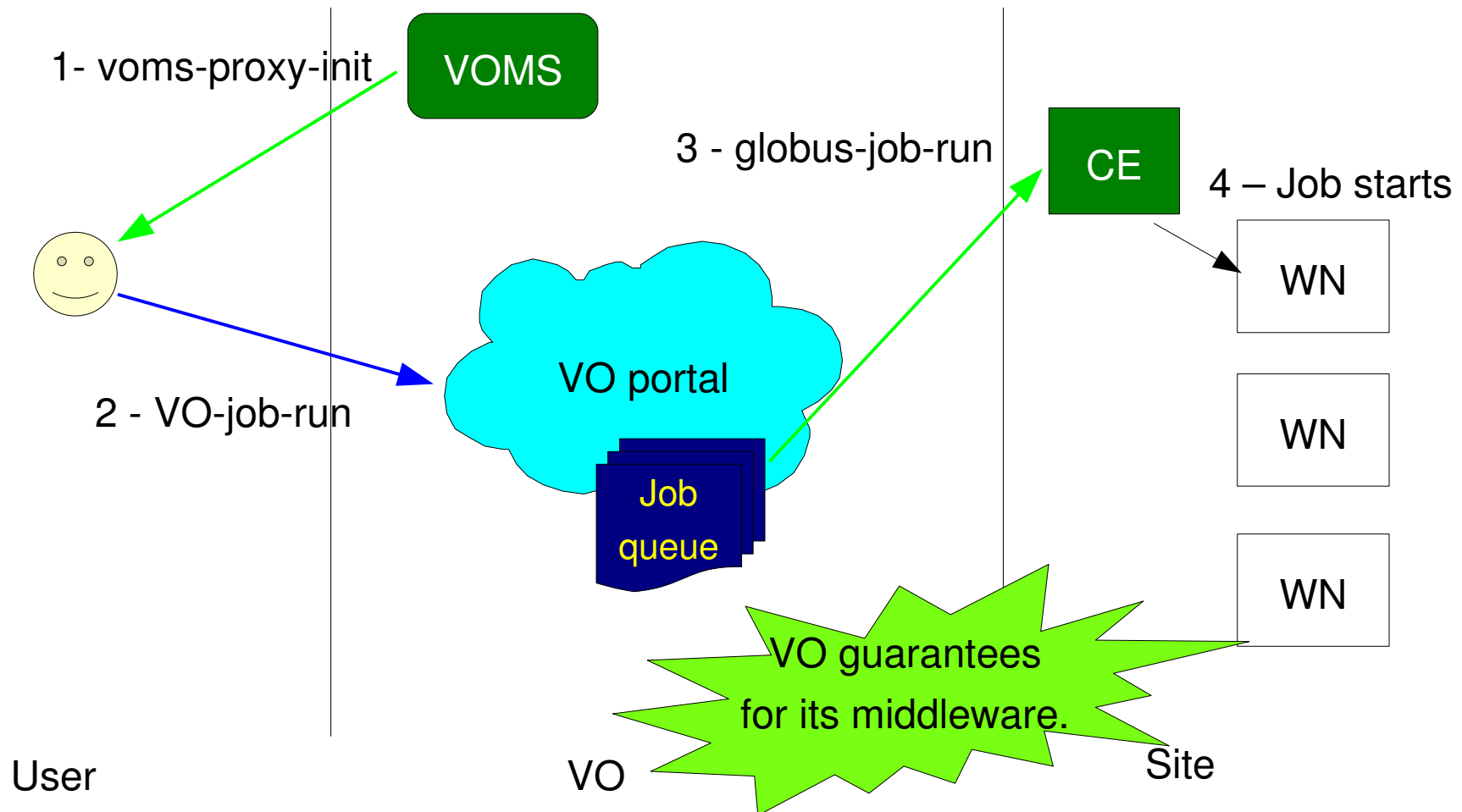


But what does really mean
being responsible for the users?

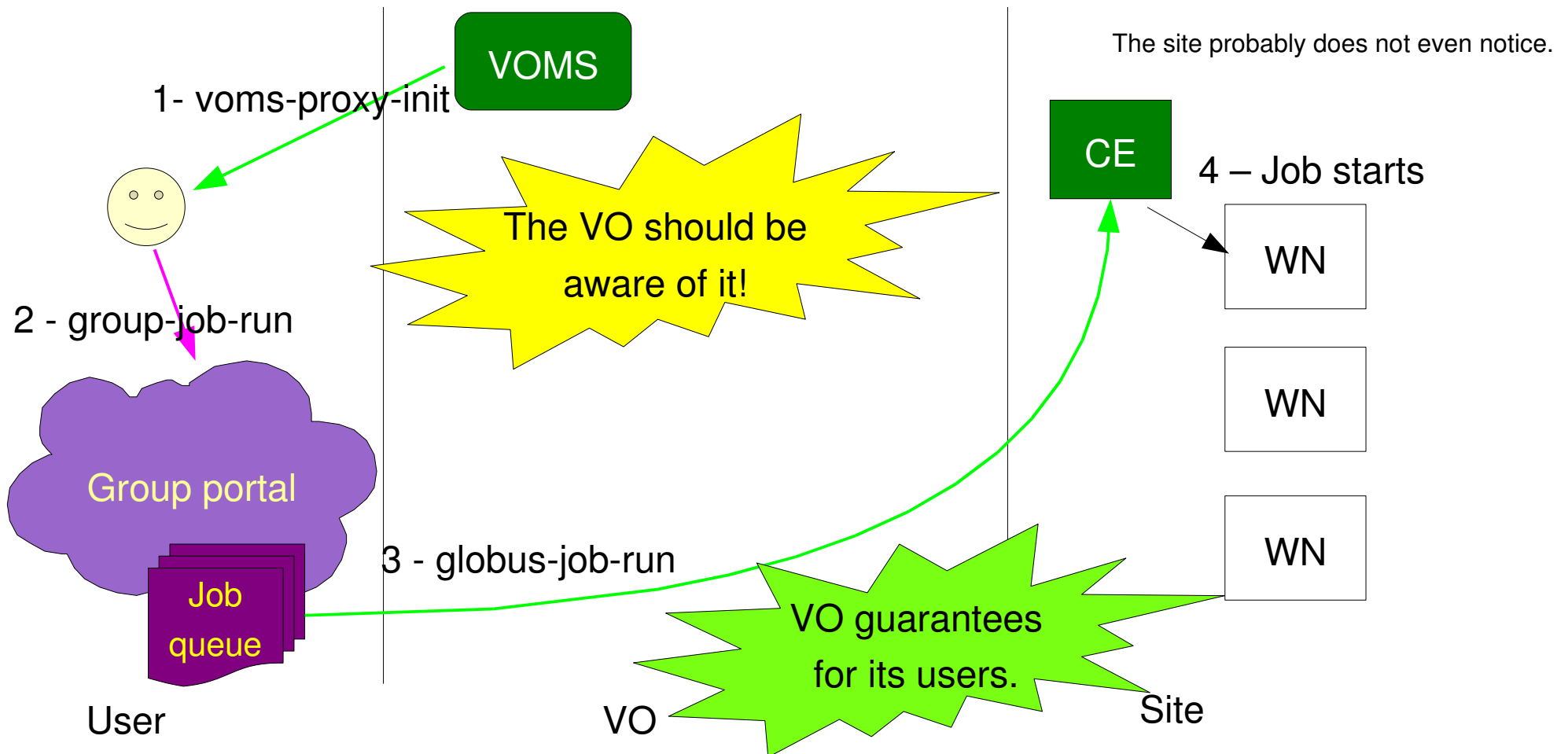
The simple scenario



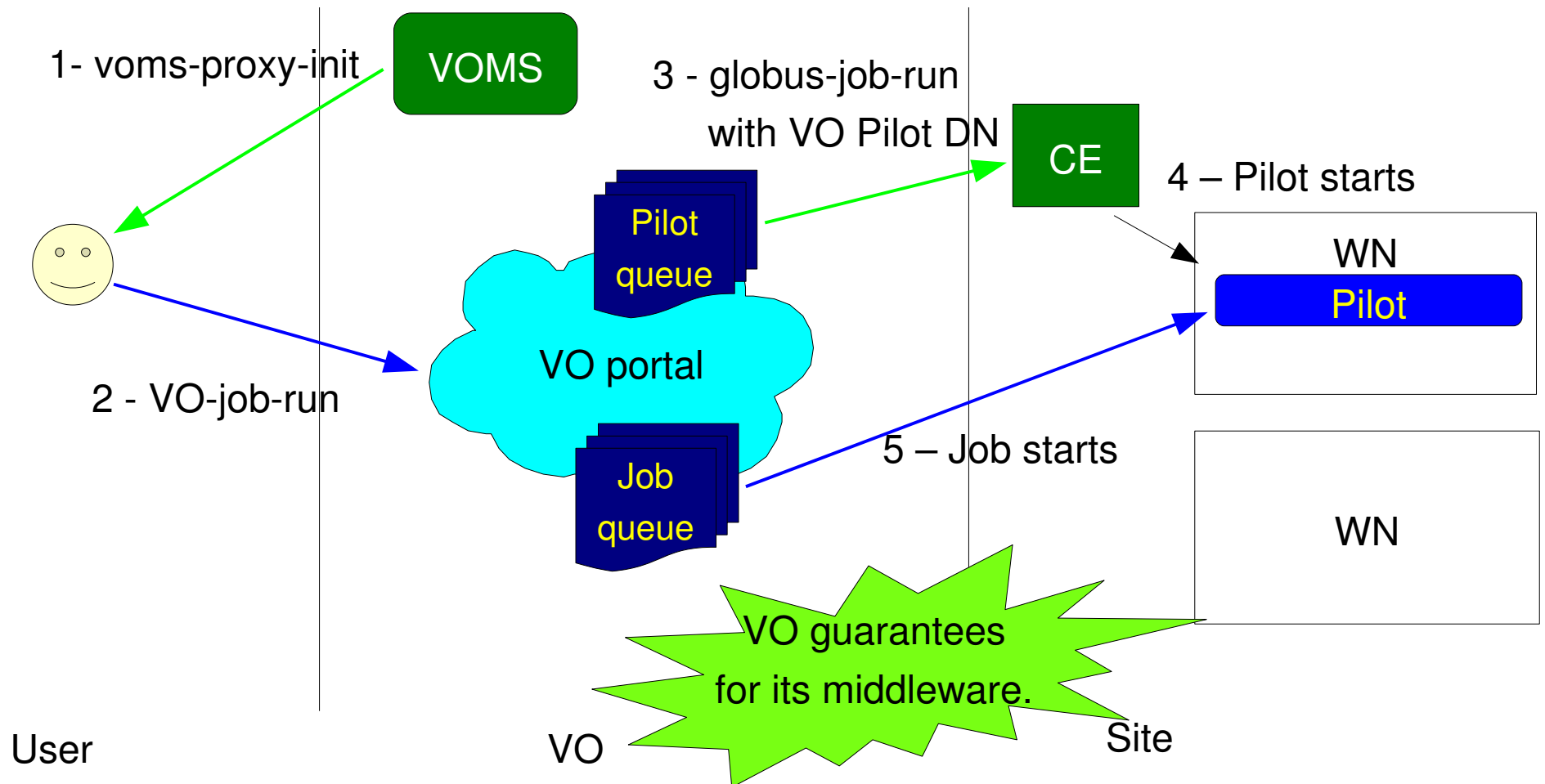
A simple VO portal



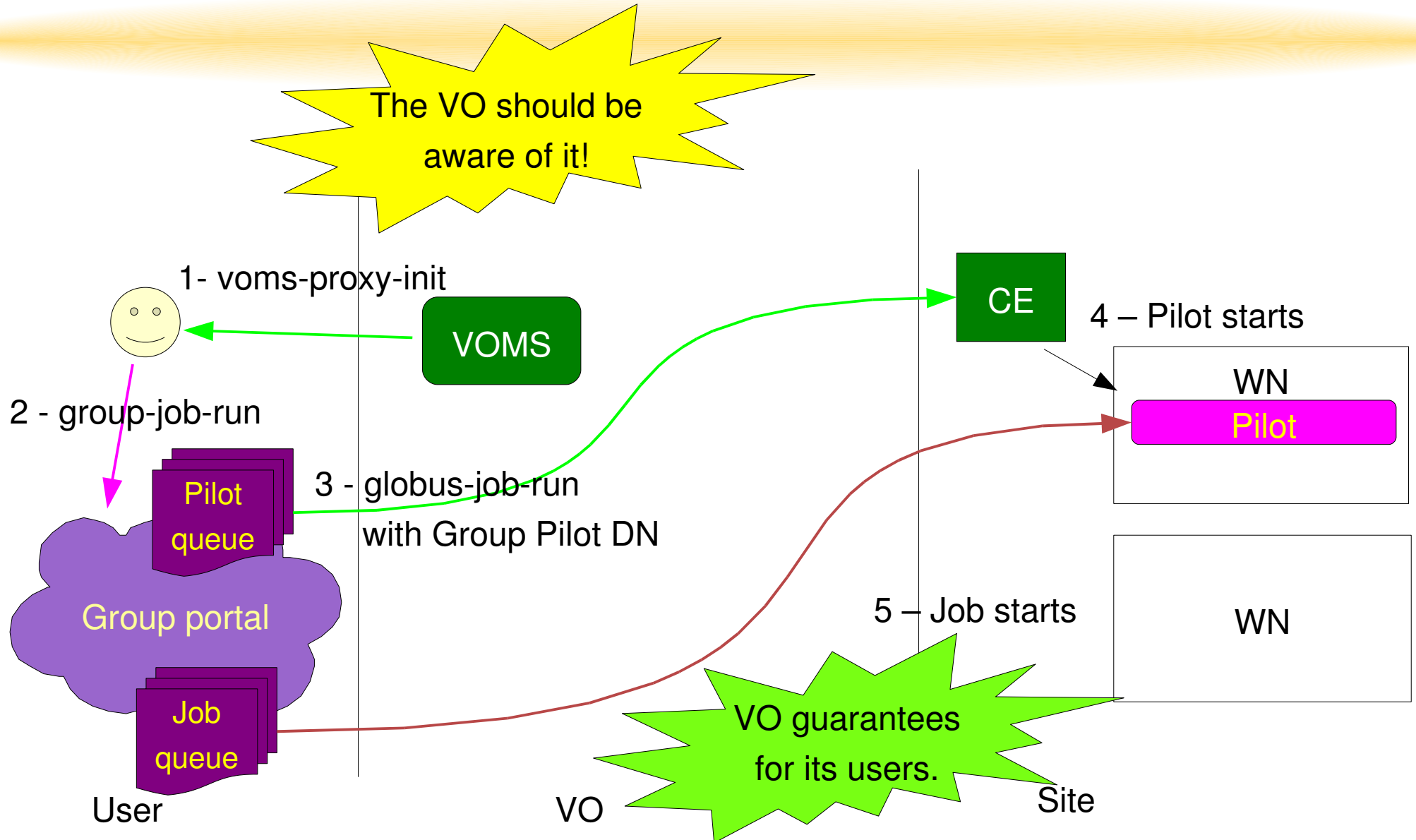
A user provided infrastructure



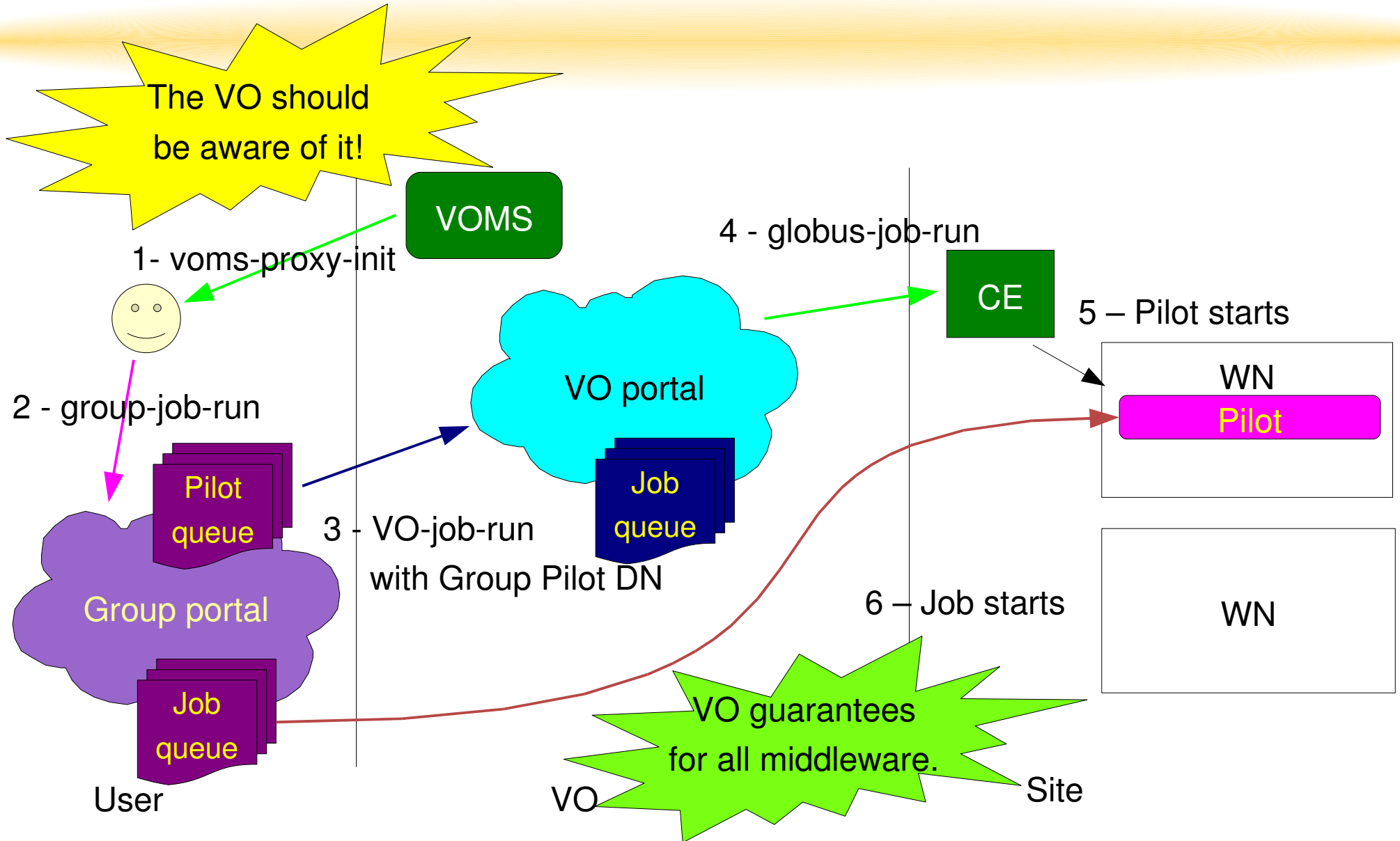
A pilot VO portal



A pilot group portal



Mix and match – an example



VO responsibilities

- VOs are responsible for
 - The users
 - The VO middleware
- If users set-up their own middleware, the VO is indirectly responsible for that, too
 - since it guarantees for the users

VO Middleware can help

- The VO must monitor both
 - user jobs, and
 - user work practices
- The VO Middleware is the ideal place to do it
 - But only if users use it!
 - No control when users submit directly to the sites

Can sites help?

- Today, sites know very little of what is going on in the VOs
 - VOs on their own when things go wrong
- Ideally, the site should distinguish between the various scenarios
 - To help identify the source of the problem
 - To disable the offending jobs without affecting legitimate ones

A complex problem

- In the standard Push model:
 - Single out compromised submit machines
 - Distinguish between VO portals and user machines
 - Detect improper user portals
- In the pilot world:
 - Distinguish a pilot job from a regular job
 - Enforce pilots talk to the local security infrastructure
 - Distinguish official pilots from user pilots

Conclusions

- The Chain Of Trust is getting longer and thus more complex
- VOs are responsible for their users
 - And any infrastructure they put in place
- The Grid Middleware is needed to verify the trust is not abused
 - What we have today is not enough!