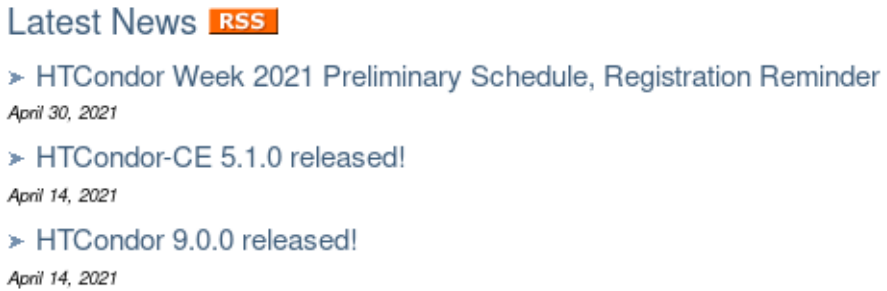
OSG/GlideinWMS Token Auth Update

Brian Bockelman, Brian Lin, Mats Rynge

HTCondor Software Suite (HTCSS)

- SciTokens/WLCG tokens supported since HTCondor-CE 4 and HTCondor 8.9
- HTCondor-CE 5 and HTCondor 9.0 released in April
  - Improvements to the credential → user mapping interface
  - Includes example mapping configurations
  - Documentation https://htcondor.github.io/htcondor-ce/v5/configuration/authentication/#scitokens



HTCondor-CE Configuration

- CE administrators can now place their own SciToken/WLCG token issuer → local user mappings in a dedicated directory, `/etc/condor-ce/mapfiles.d/`
- Downstream packagers can include default mappings in `/usr/share/condor-ce/mapfiles.d/`
- Administrators can map all tokens from a VO to a single user:
  `SCITOKENS /^https:\/\/scitokens\.org\/osg-connect,/ osgpilotuser`
- In addition to also mapping based on the token's subject (e.g., "testing"):
  `SCITOKENS /^https:\/\/scitokens\.org\/osg-connect,testing$/ osgtestuser`

Token Auth in the OSG

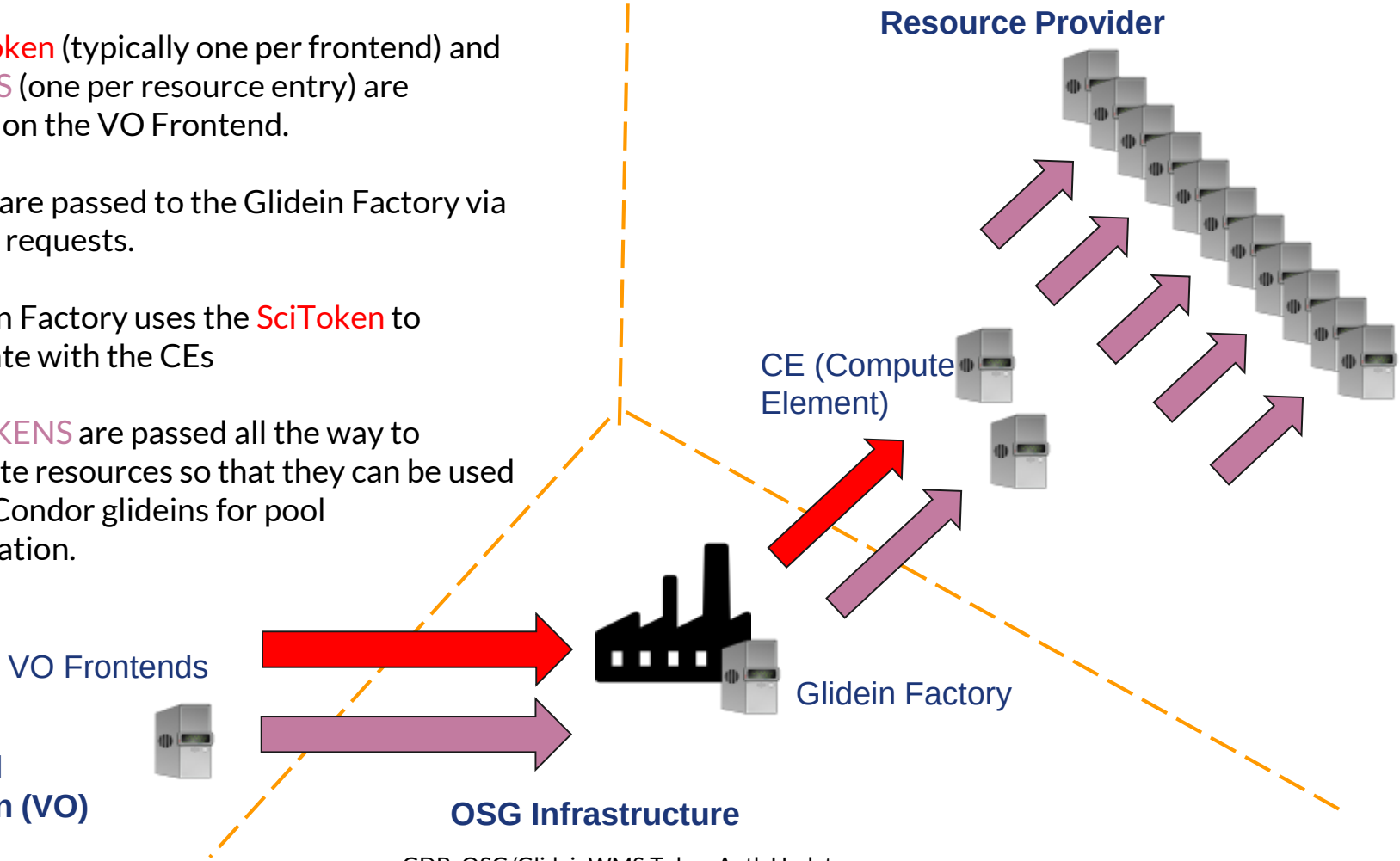
- GlideinWMS 3.7.3 adds support for SciToken/WLCG token pilot submission and pilots reporting back via HTCondor IDTOKENS
  - SciTokens/WLCG tokens are short-lived, asymmetrically encrypted: any CE can authenticate a VO's token using the issuer's public key
  - IDTOKENS are generated per factory entry, revocable, and symmetrically encrypted: only the issuing VO can use/authenticate the token
- In April, we demonstrated end-to-end token-based resource allocations against a production site:
  - Set up OSG and GLOW SciToken issuers
  - GlideinWMS ITB factory updated to 3.7.3
  - GLOW and OSG VO frontends updated and patched (see later slides)

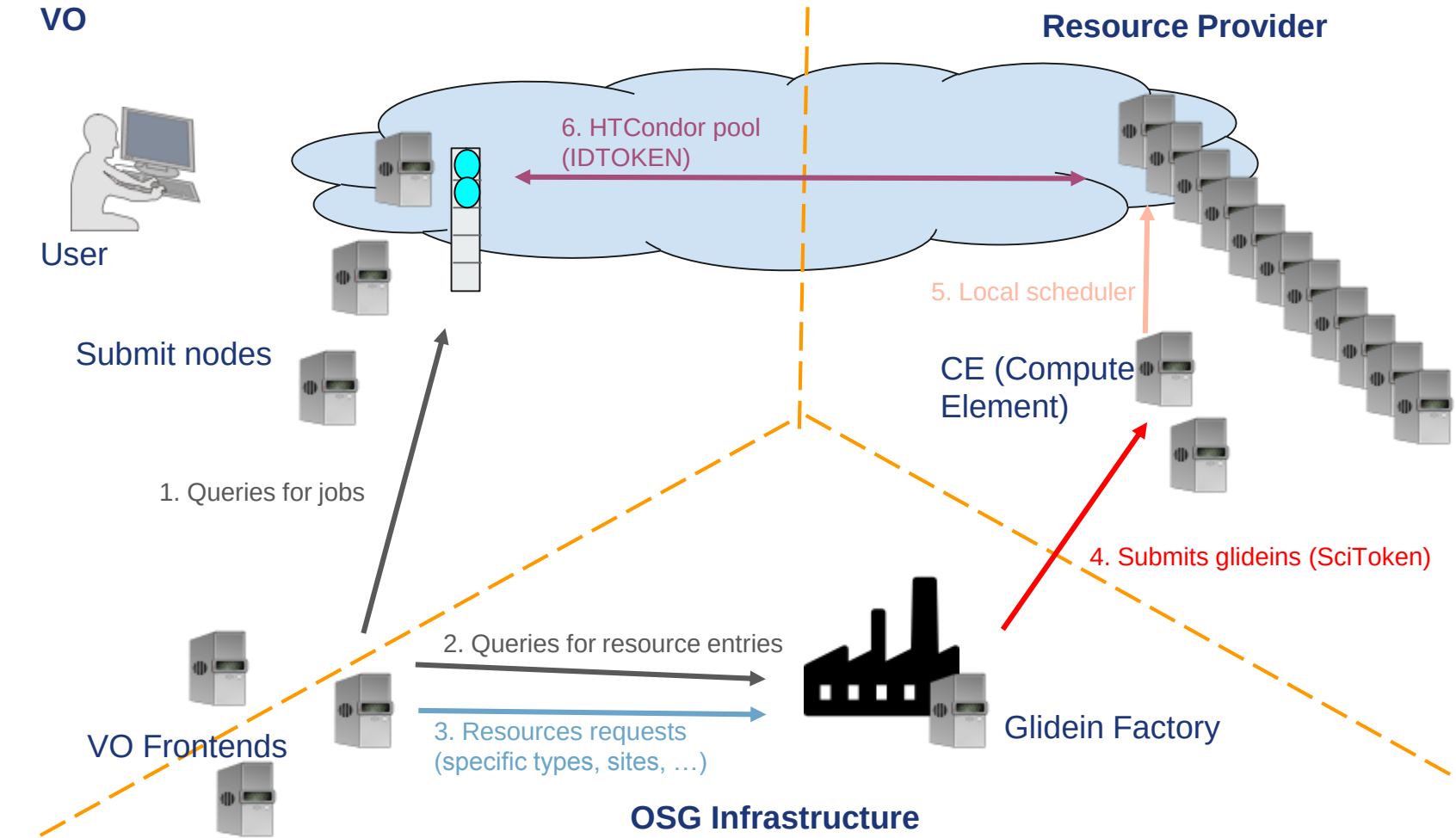
Both SciToken (typically one per frontend) and IDTOKENS (one per resource entry) are generated on the VO Frontend.

All tokens are passed to the Glidein Factory via the glidein requests.

The Glidein Factory uses the SciToken to authenticate with the CEs

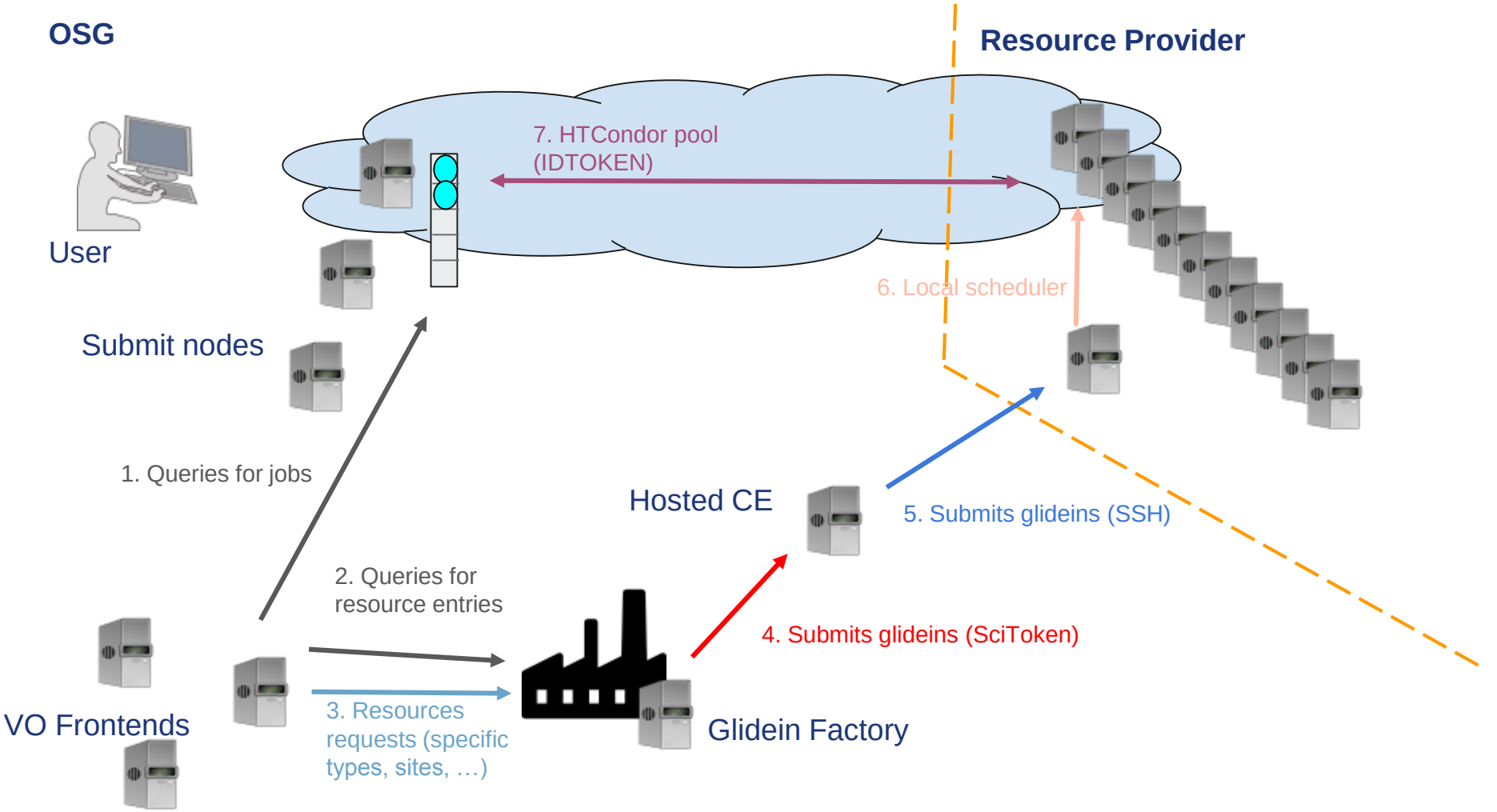
The IDTOKENS are passed all the way to the compute resources so that they can be used by the HTCondor glideins for pool communication.




VO
Resource Provider
User
6. HTCondor pool
(IDTOKEN)
5. Local scheduler
Submit nodes
CE (Compute
Element)
1. Queries for jobs
4. Submits glideins (SciToken)
2. Queries for resource entries
3. Resources requests
(specific types, sites, …)
VO Frontends
Glidein Factory
OSG Infrastructure

OSG Hosted CEs

- OSG Operations manages ~40 CEs that submit pilots to remote sites over SSH
- Hosted CEs are deployed on multiple Kubernetes clusters via SLATE
- OSG Software demonstrated Hosted CEs working with SciTokens-based pilots
- We’re aiming for 50% Hosted CEs accepting SciTokens-based pilots by June


OSG
Resource Provider
User
7. HTCondor pool
(IDTOKEN)
6. Local scheduler
Submit nodes
1. Queries for jobs
Hosted CE
5. Submits glideins (SSH)
2. Queries for
resource entries
4. Submits glideins (SciToken)
VO Frontends
3. Resources
requests (specific
types, sites, …)
Glidein Factory

Next Steps

- WLCG CE & Factory Token Hackathon June 3-4: https://indico.cern.ch/event/1032742/
- Plan token → user mapping strategies
  - Many VOs have multiple X.509 proxies → different users based on storage access rights
  - Tokens allow us to separate pilot/storage credentials. Do we still need different pilot users?
- Open issues
  - SciToken/WLCG token pilots still require an X.509 proxy (fix targeted for GlideinWMS 3.7.5)
  - Various minor fixes for GlideinWMS frontends (targeted for GlideinWMS 3.7.5)
  - HTCondor-CE SciToken/WLCG token submission failure does not fallback to GSI
  - Update accounting tools to retrieve VO data from token-based jobs

Questions?

This material is based upon work supported by the National Science Foundation under Grant Nos. 1836650 and 2030508. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.