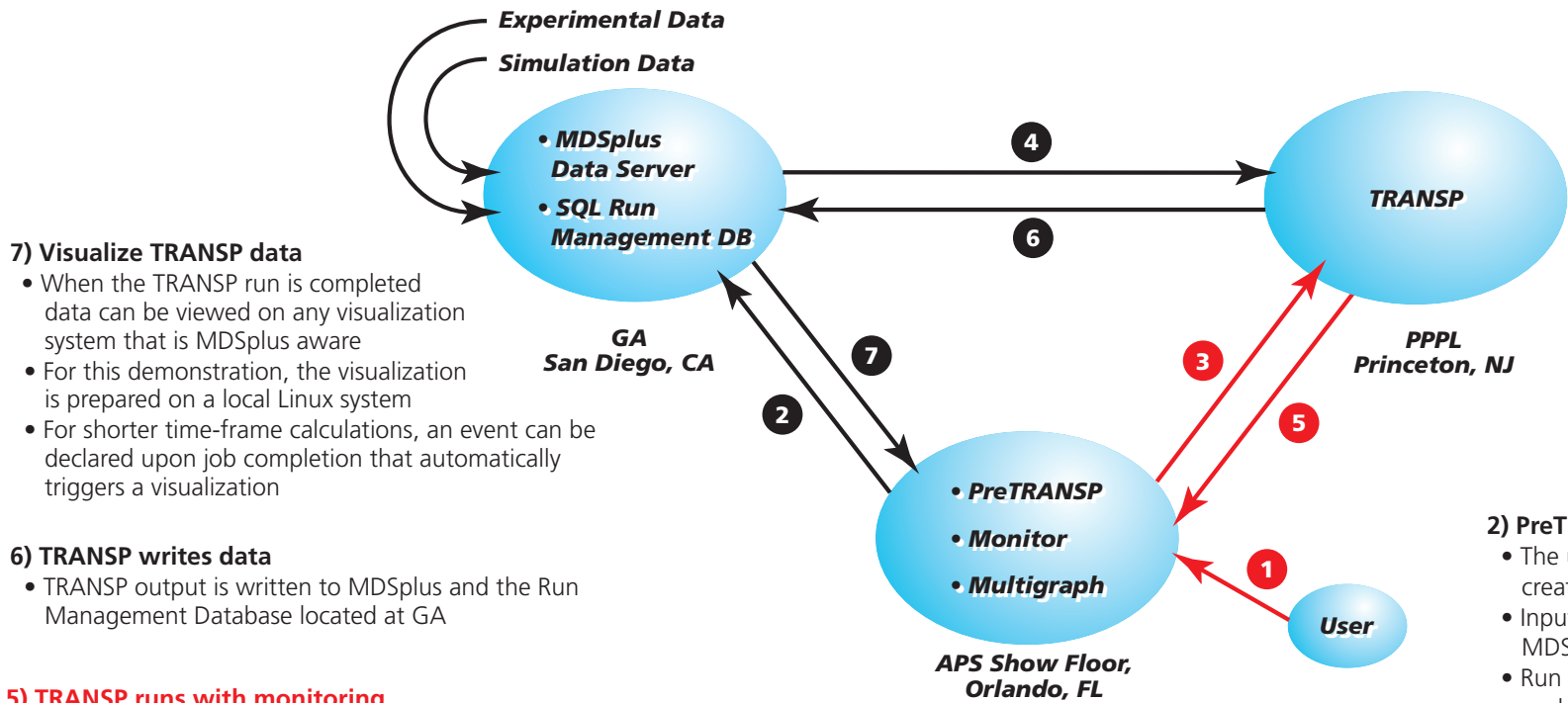


# THE NATIONAL FUSION COLLABORATORY: Building a National FusionGrid

The demonstration represents the first components of production FusionGrid

Any code and MDSplus data repository can be FusionGrid enabled. Future plans include additional codes and data archives to be added.



### 7) Visualize TRANSP data

- When the TRANSP run is completed data can be viewed on any visualization system that is MDSplus aware
- For this demonstration, the visualization is prepared on a local Linux system
- For shorter time-frame calculations, an event can be declared upon job completion that automatically triggers a visualization

### 6) TRANSP writes data

- TRANSP output is written to MDSplus and the Run Management Database located at GA

### 5) TRANSP runs with monitoring

- TRANSP runs on PPPL Linux cluster
- Monitoring software allows the user to track the status of their run

### 1) User Authentication

- Person has previously joined the collaboratory by obtaining a credential from the DOE Science Grid Certificate Authority which is an X.509 identity certificate
- User logs onto the FusionGrid using the credential
- Logging onto the Grid uses the Globus GSI single sign-on capability
- Creates a short term proxy certificate that persists through your Grid session

### 2) PreTRANSP prepares input data

- The user runs a GUI that assists them in creating inputs to the TRANSP code
- Inputs for a TRANSP run are written into MDSplus at GA
- Run management database at GA is updated to indicate run is being prepared
- Data access contingent on authentication & authorization of original user

### 3) Authorize & Start TRANSP

- Transparently to the user, the TRANSP job is started remotely using Globus GRAM
- Globus GSI transparently verifies that the user is who the credential says it is
- Globus GRAM calls Akenti to check the authorization policy for the user
- If authorized, the TRANSP run is queued for execution

### 4) TRANSP reads input

- TRANSP reads input data from MDSplus and Run Management Database located at GA
- Data access contingent on authentication & authorization of original user



#### Key Words:

**Akenti** ([www.itg.lbl.gov/Akenti/](http://www.itg.lbl.gov/Akenti/)) is a security model and architecture that provides scalable security services in a highly distributed network environment. Akenti has been developed by a team at the Lawrence Berkeley National Lab.

**Globus** ([www.globus.org](http://www.globus.org)) is a set of software tools that enables flexible, secure, and coordinated resource sharing among dynamic collections of individuals, institutions & resources. Globus has been developed by a team led by the Argonne National Lab.

**MDSplus** ([www.mdsplus.org](http://www.mdsplus.org)) provides a set of tools for acquiring and managing data from fusion experiments and codes. MDSplus was developed by a team led by the MIT Plasma Science and Fusion Center