Introducing SVOPME, A Scalable Virtual Organization Privileges Management Environment (Grid Site's Perspective)

Tech-X Corporation
Fermi National Accelerator Laboratory

Contacts:
Nanbor Wang nanbor@txcorp.com
Gabriele Garzoglio garzogli@fnal.gov

What are VO Privileges?

Virtual Organizations:

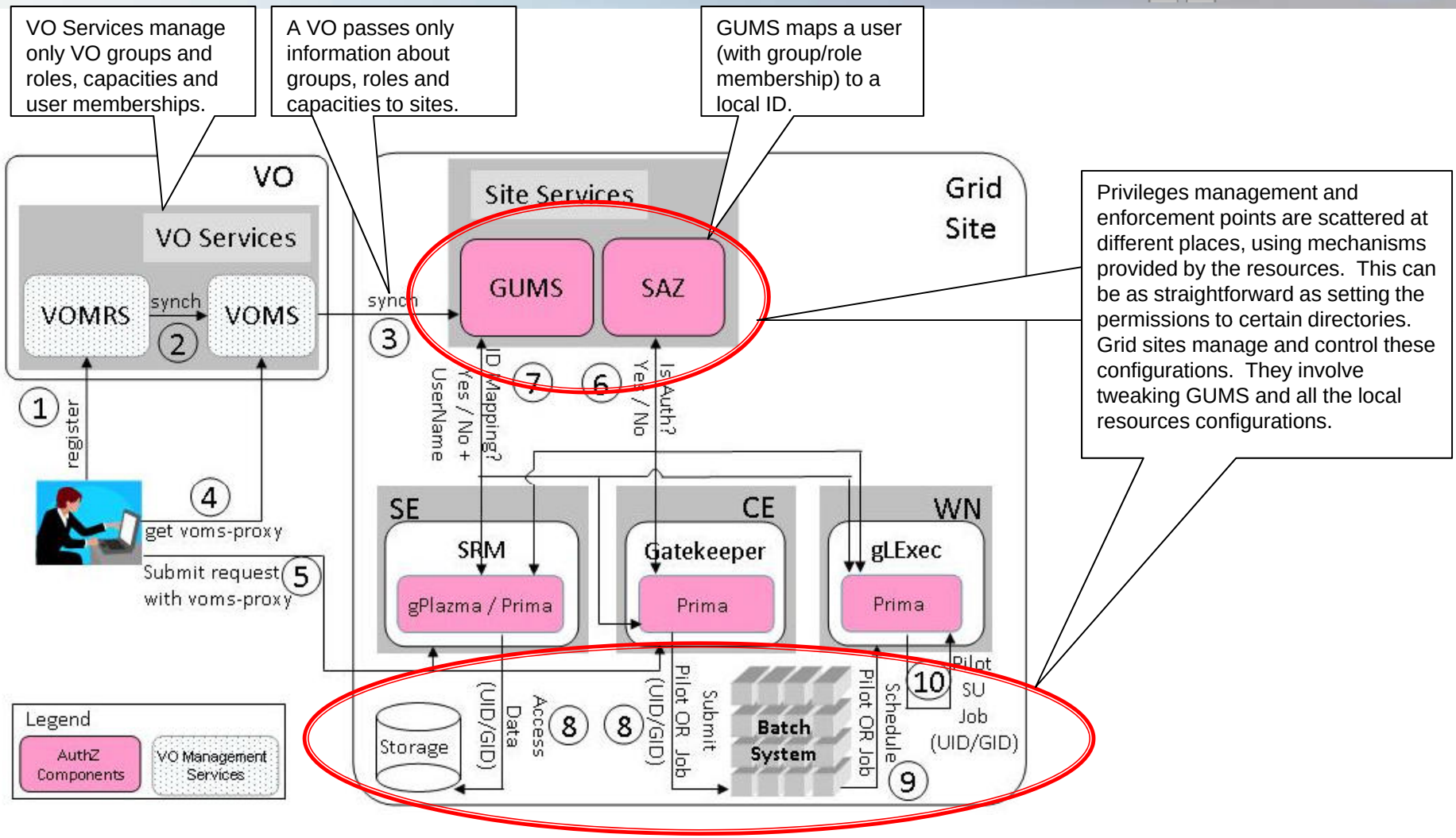
- VOs use shared resources
- VOs need to define resource usage policies for different users within the VOs
  - Example 1: Production team members submit jobs with higher priority
  - Example 2: Software team members can write to disk area for software installations but others can't
- However, VOs do not manage/configure Grid sites

Grid Sites:

- Grid sites provide resources
- Grid sites don't define VOs' usage policies
- Grid sites enforce and manage user privileges
- Grid sites do not allow others (such as VO admins) to change the site configurations

Site and VO Challenge: Enforcing heterogeneous VO privileges on multiple Grid sites to provide uniform VO Policies across the Grid (ad hoc solution: verbal communication)

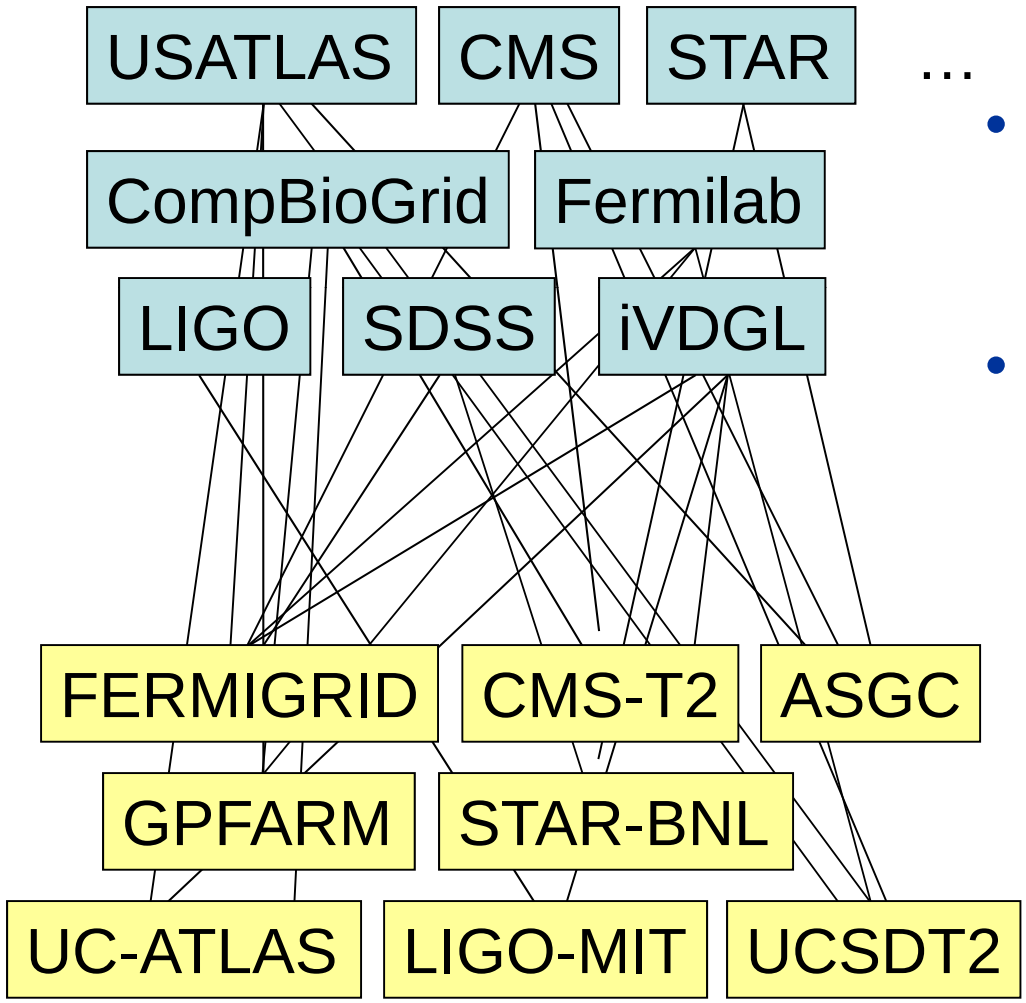
State-of-the-Art
User Privilege Management



The OSG Authorization Infrastructure

Motivations of SVOPME

Address scalability

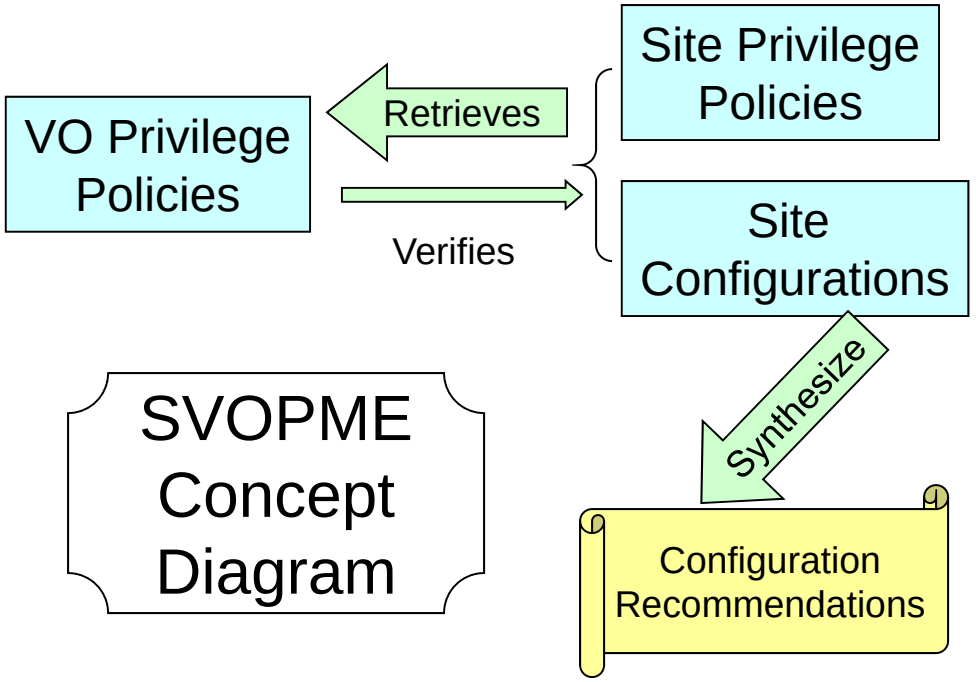


- **With the growth in Grid usage, both the numbers of VOs and Grid-sites increase**
- **Propagating privilege policies by verbal communication between VO and Grid site admins no longer scales**
- **SVOPME fills the gap by**
  - Providing the tools and infrastructure to help
    - VOs express their policies
    - Sites support VOs
  - Reuse proven administrative solutions – we adopt common system configuration patterns currently in use in major grid sites

SVOPME Helps Grid Sites Maintain Privilege Policies Defined by VOs

SVOPME

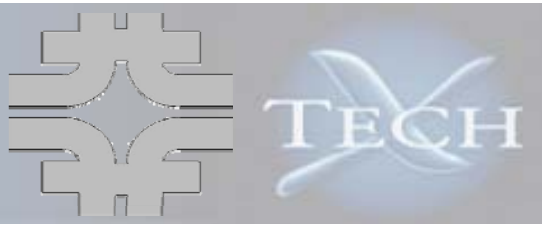
- Aims to replace the verbal interaction with automated workflows
- Pre-defines a set of policy types – new types can be added easily
- Provides tools for VOs to define, package, and publish privilege policies
- Synthesizes effective site policies automatically
- Documents policies in XACML format, no ambiguity
- Allows programmatic verification of policies
- Verifies site policies against those of VOs'



SVOPME Concept Diagram

- Provides recommendations to site configurations for better VO supports

Advantages of SVOPME



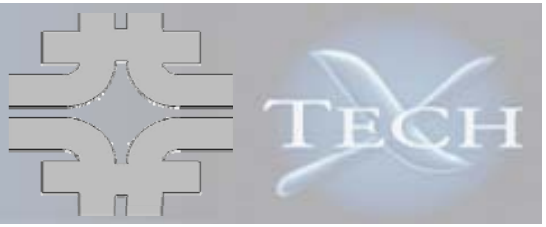
VOs

- No need to run ad-hoc jobs to figure out what policies are enforced and what not
- Provides templates to define commonly used policies
- Automates most of the communication with Sites that support the VO
- Provides the basis for the negotiation of privileges at sites that provide opportunistic access
- Use a web interface at sites to verify policy compliance.

Sites

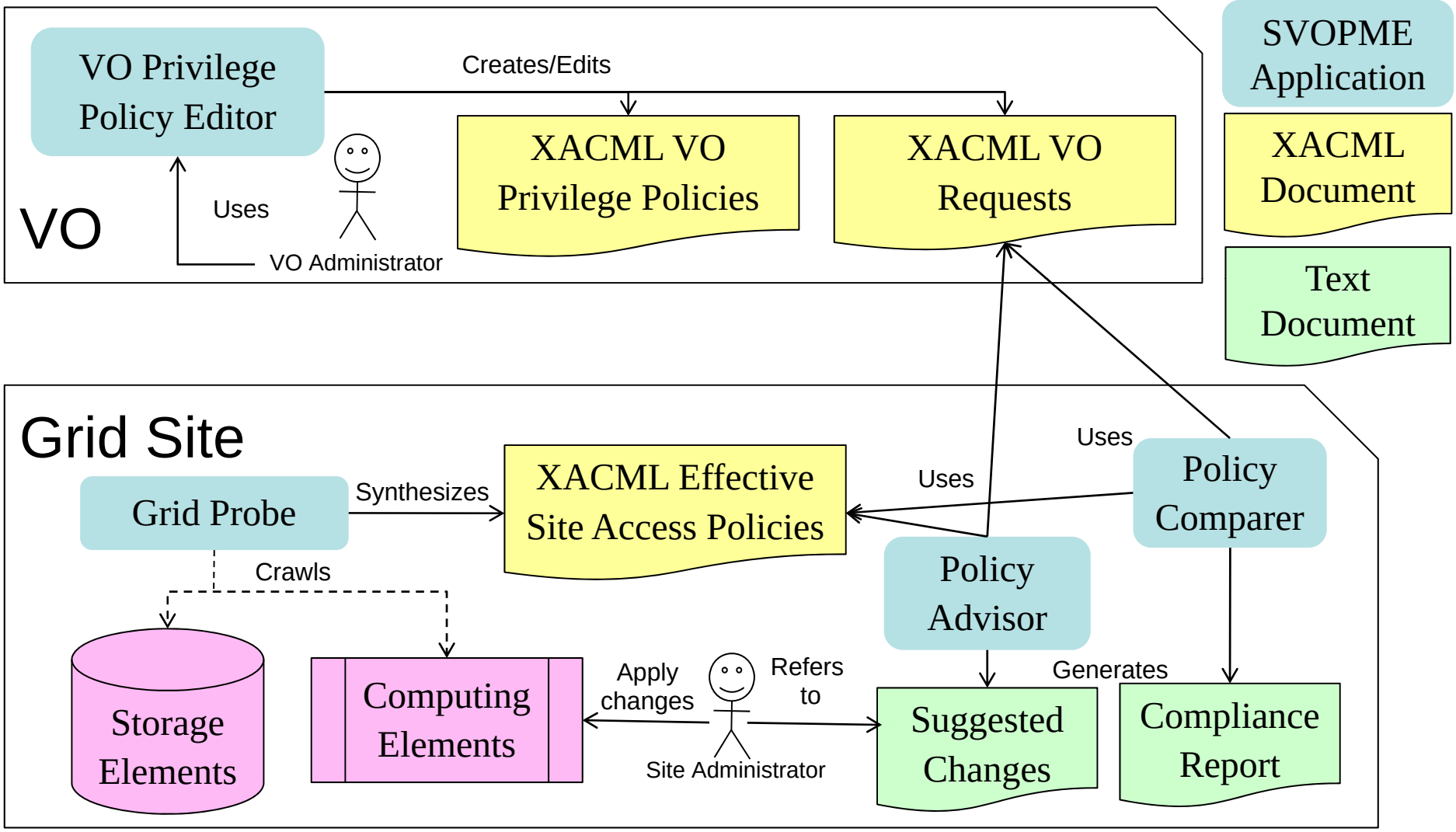
- No need to understand what ad-hoc jobs VOs use to test privileges
- Sites that want to support a VO have a semi-automated mechanism to enforce the VO policies
- Privilege enforcement remains responsibility of the sites, informed by formal VO policy assertions
- Sites can advertise and prove that a VO is supported
- Automation helps minimize work and errors
- Sties retains full control of their configurations without revealing actual configurations

SVOPME Currently Support These Types of Policies

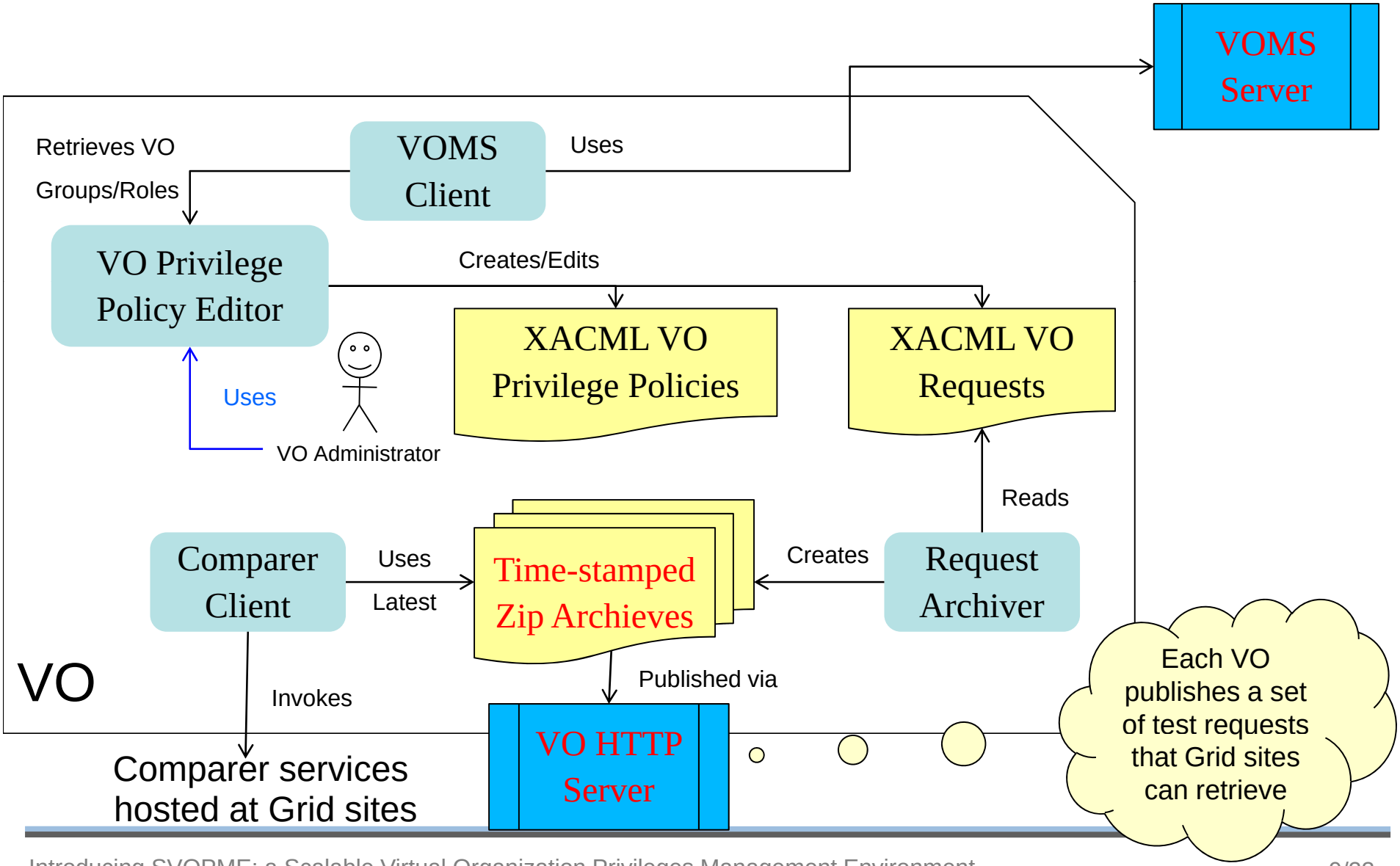


- **Account Type Policy:** Run job from Group(G) and Role(R) using Pool (unique)/ Group (shared) accounts.
- **Account Mapping Policy:** Must have accounts for all users in Group (G) and Role(R) (may be pool accounts or Group accounts).
- **Relative Priority Policy:** Jobs from Group (G1) and Role (R1) should have higher priority than those from user of Group (G2) and Role (R2).
- **Preemption Policy (Batch system):** Jobs from Group (G) and Role (R) should be allowed to execute for n consecutive hours without preemption.
- **Package Installation Policy (Storage):** Allow Group (G) and Role (R) to install software in $OSG_APP (assuming there is NO space reserved for any VO)
- **Unix Group Sharing Policy (Batch system):** Accounts belonging to /Group/Role=A and /Group/Role=B must share the same unix Group ID
- **File Privacy Policy (Storage):** Files Privacy Policy: Users belonging to /Group/Role=A expect privacy for their files
- **Job Suspension Policy (Batch system):** Do not suspend / resume jobs submitted from /Group/Role=A
- **Disk Quota Policy (Storage):** Assign disk quota of X GB and Y MB to accounts mapped to /Group/Role=A

SVOPME Architecture Overview



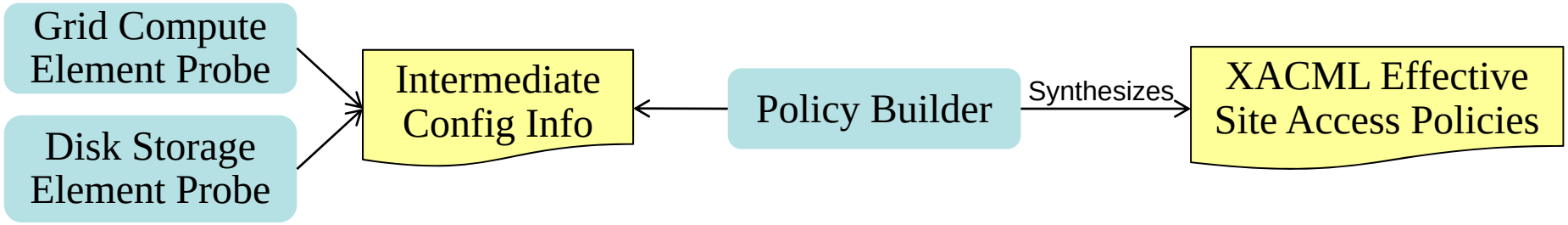
SVOPME VO Tools Make VO Privilege Policies available to Sites



SVOPME Grid-Site Release

- **Grid-site and VO packages are downloaded and installed separately**
- **Grid-site release can be obtained from: https://ice.txcorp.com/trac/svopme/attachment/wiki/Download/svopme_grid.tar.gz**
- **We are ready to help in any areas**
  - Installation
  - Configuration
  - Defining privileges
- **Installation is relatively straightforward:**
  - One environment variable
  - A list of URLs where VOs publish their policies
  - Set up cron jobs to invoke tools periodically
  - Set up Policy Comparer web service
- **Detailed Instructions for Grid Sites: https://ice.txcorp.com/trac/svopme/wiki/SiteInsts**
- **Currently, SVOPME is available on FermiGrid's Integrated Testbed (ITB), we wish to make it available at more sites**

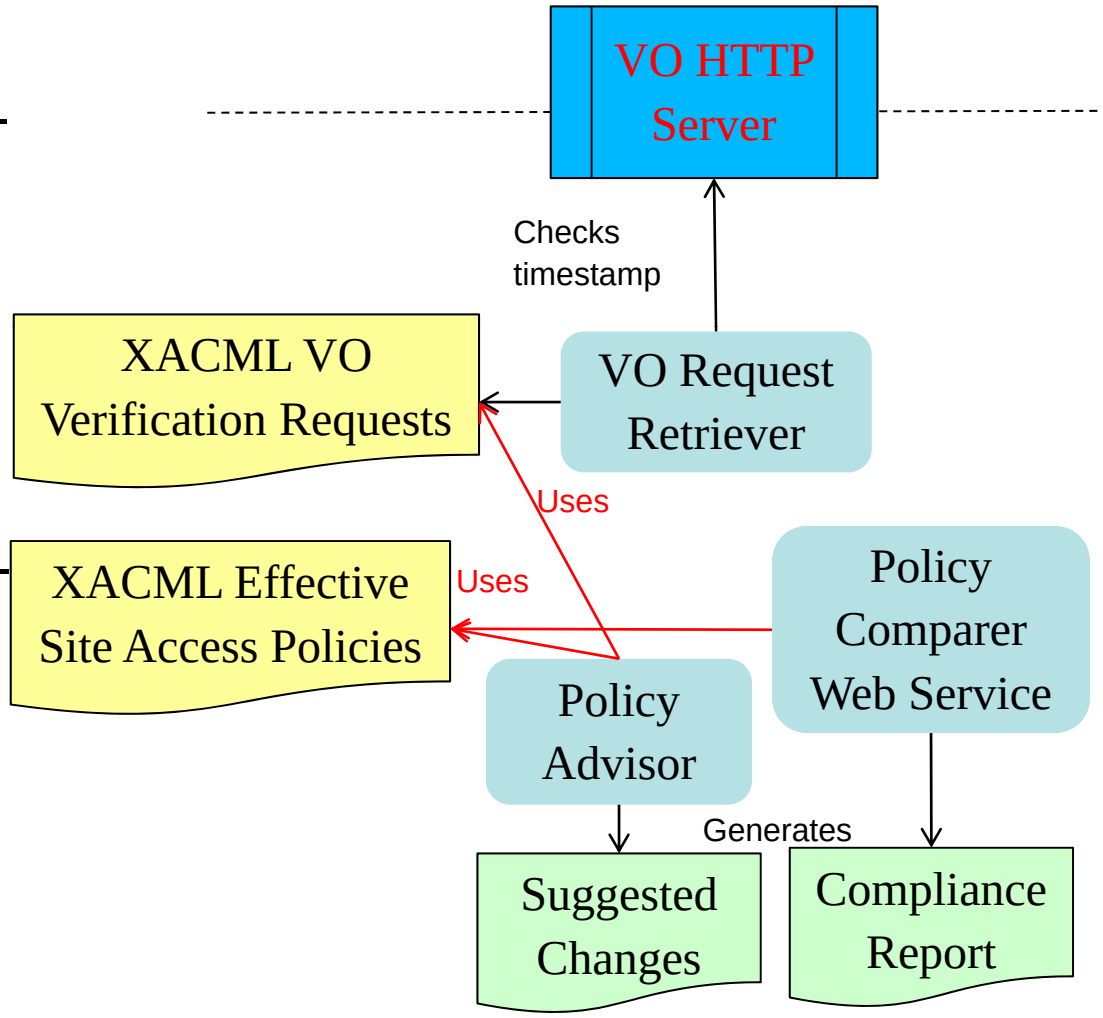
Mechanism for Synthesizing Grid Site Privilege Policies



- **"Grid Probe" in a nutshell**
  - Policy building and configuration crawling functions are separated
  - Depending on the target resources, different info is necessary: there are multiple crawling executables
  - Invoked by different cron tasks with different privileges (some do require root privilege, one at this moment)
  - Dump the info as simple text files at a specific directory
  - Allow site-specific probes (customization)
- **Configuration checked**
  - Condor/GUMS config
  - Disk quota/directory permissions
- **Policy Builder**
  - Parses the intermediate configuration info
  - Synthesizes the effective privilege policies of a site into XACML policies
- **Different site configurations/policies may require new probes/builders**
  - We can help add support for new resources and policies

Analyzing Site Configurations

- **VO Request Retriever**
  - Checks if the local VO verification requests is up-to-date
  - Cache the new verification requests if needed
- **Policy Comparer and Advisor**
  - Test compliance by testing the verification requests one-by-one
  - Since all requests and policies are based on our XACML profiles, reports and advises can be derived



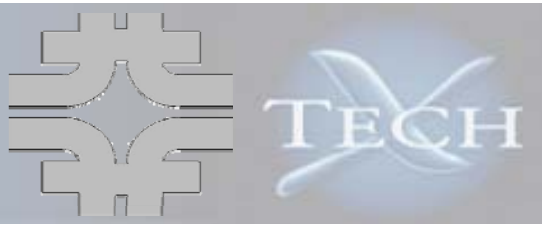
VO/Grid Policies Comparer

- Example output:

```
    [java] VO/Grid Grid Accounts Policy Comparison
    [java] ---------------------------------------
    [java] /TECHX/Role=User is mapped to 1 account(s) on the
Grid site. Passed!
    [java] No Account Mapping Policies for /TECHX/VISITORS
were found on the Grid site.
```

- Policy Comparer Grid Service
  - Allow VO users to check privilege policy compliance at a site
  - Instead of cached verification requests, users supply a list of verification requests related to policies of interests
  - SVOPME provides a policy comparer client as part of the VO tools
  - Currently only provide text reports – should provide a mechanism for further automate the information gathering

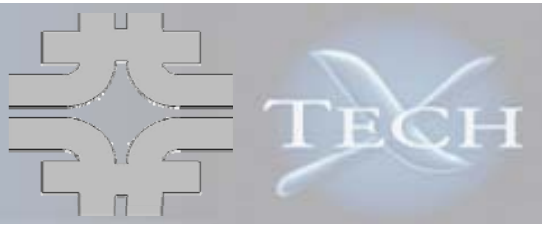
Grid Policies Advisor



- Provide advices for the **Grid site administrator** on what amendments need to be done on the site; such that the Grid site complies with the VO policies
- Can be invoked to check against policies of one VO
- Example output:
  - VO requested 3 accounts for VISITORS role via VO policies
  - Site-policies derived from GUMS do not match

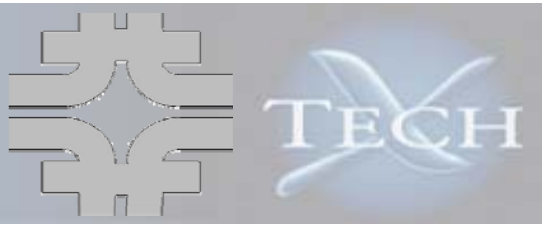
```
    [java] VO/Grid Grid Accounts Policy Advices
    [java] ------------------------------------
    [java] No matching Grid Accounts Policy was found for
/TECHX/VISITORS on the Grid site. Create a mapping in GUMS config
such that /TECHX/VISITORS be mapped to at least 3 account(s)
    [java] TECHX/Role=VO-Admin mapped to 1 account(s)
(techxVOadmin) on the Grid site, is not suffient enough. Needs to
be mapped to atleast 3 accounts.
```

Experiments on FermiGrid's Integrated TestBed



- **Using "Dzero" and "Engage" VO's privileges as a real-world examples**
- **Validation requests are copied over to the site (FGITB) using the "Retriever" tool**
- **Two different probes run with different privileges**
- **"Engage" VO will continue to expand and incorporate other smaller sub-VO's**
- **Was able to detect several anomalies**
  - Enhanced disk quota probes – multiple filesystems
  - Re-wrote quota/filesystem probe to use python – easier for admins to examine
  - Detected one missing account mapping
  - Legacy pool account configurations
- **Separating probes allows easy adaption to site with unconventional confiurations**

Possible Concerns on Site Resources



- **Resource Loads**
  - ITB installation did not cause any concerns
  - Grid probes
    - Run as cron jobs, should consume nearly no cycles
    - No need to run too often
  - Policy builder
    - Run only when necessary, (i.e., configuration changes)
    - Mostly text manipulations
  - VO request retriever
    - Runs as a crob job
    - Uses network/storage
  - Policy Comparer
    - Runs on-demand
    - Can be a potential DNS point (if anyone can query)
    - Alternatively, run as crob jobs and publish results
  - Policy Advisor
    - Runs as a cron job, or when necessary
    - Load depends on the XACML engine/# of policies
- **Security**
  - Site configurations are not exposed
  - VOs can not modify configurations directly
  - Comparer web service is the only exposure

SVOPME VO Release

- **VO package can be obtained from:** https://ice.txcorp.com/trac/svopme/attachment/wiki/Download/svopme_vo.tar.gz
- **Detailed Instructions for VO:** https://ice.txcorp.com/trac/svopme/wiki/VoInsts

Conclusions

- SVOPME ensure uniform access to resources by providing an infrastructure to propagate, verify, and enforce VO policies at Grid sites
- We are soliciting interested VO's and sites to deploy SVOPME in a production environment
- We love to hear your comments and suggestions
  `https://ice.txcorp.com/support/wiki/MidSys/SVOPME`