

Summary

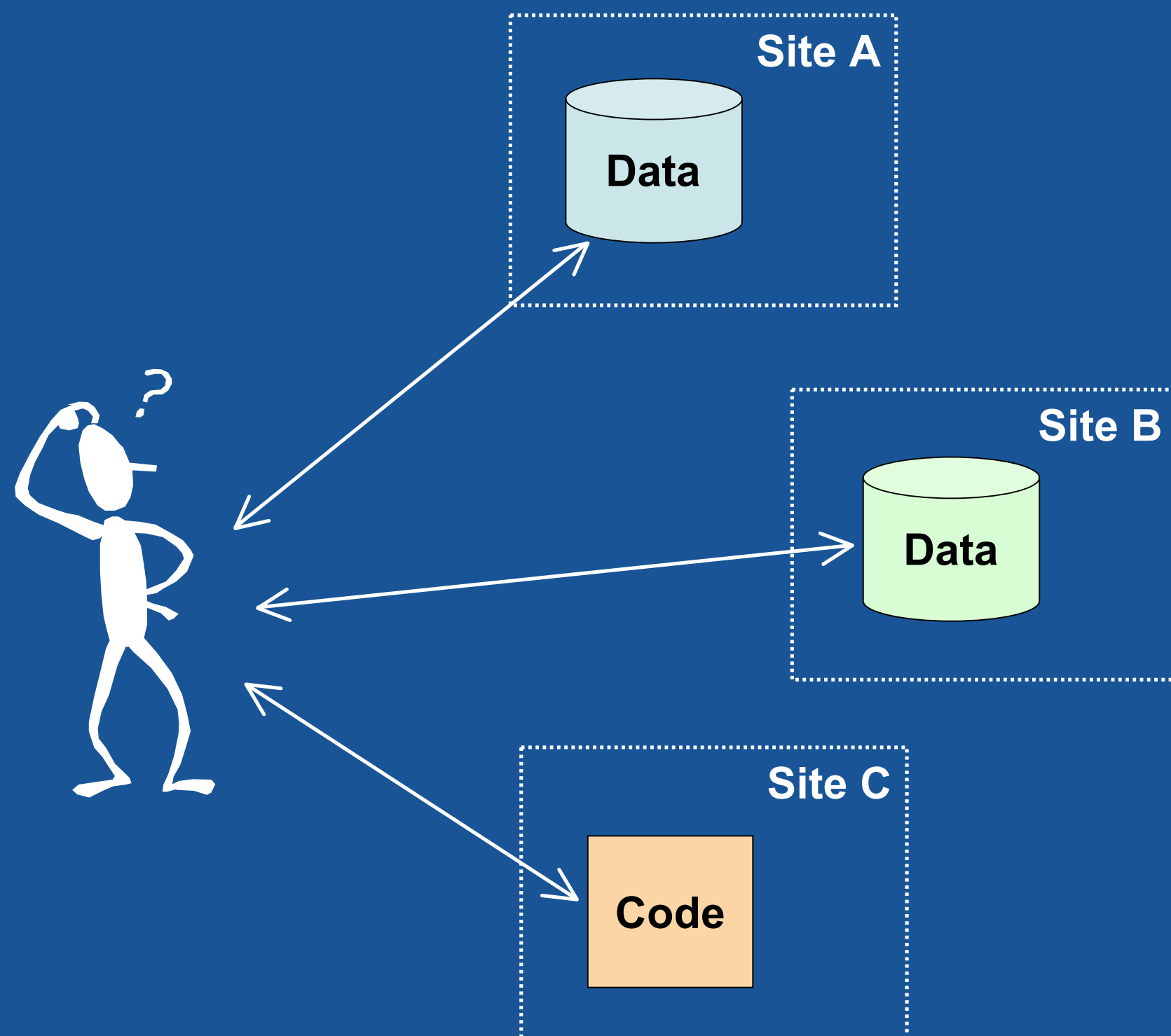
- Security in a geographically distributed and administratively divided computing environment such as the U. S. Fusion Grid (FusionGrid) is inherently difficult
 - Authentication across user namespaces
 - Authorization across administrative domains
 - Secure data storage and transfer

- FusionGrid developers solved these problems using
 - X.509 credentials & a credential management system
 - a new authorization manager
 - a new secure version of MDSplus

- Future computing infrastructures such as ITER will need to deal with these same problems
 - ITER in particular will require collaboration across administrative domains and even international boundaries
- These solutions may be applied to future computing environments such as ITER

Authentication

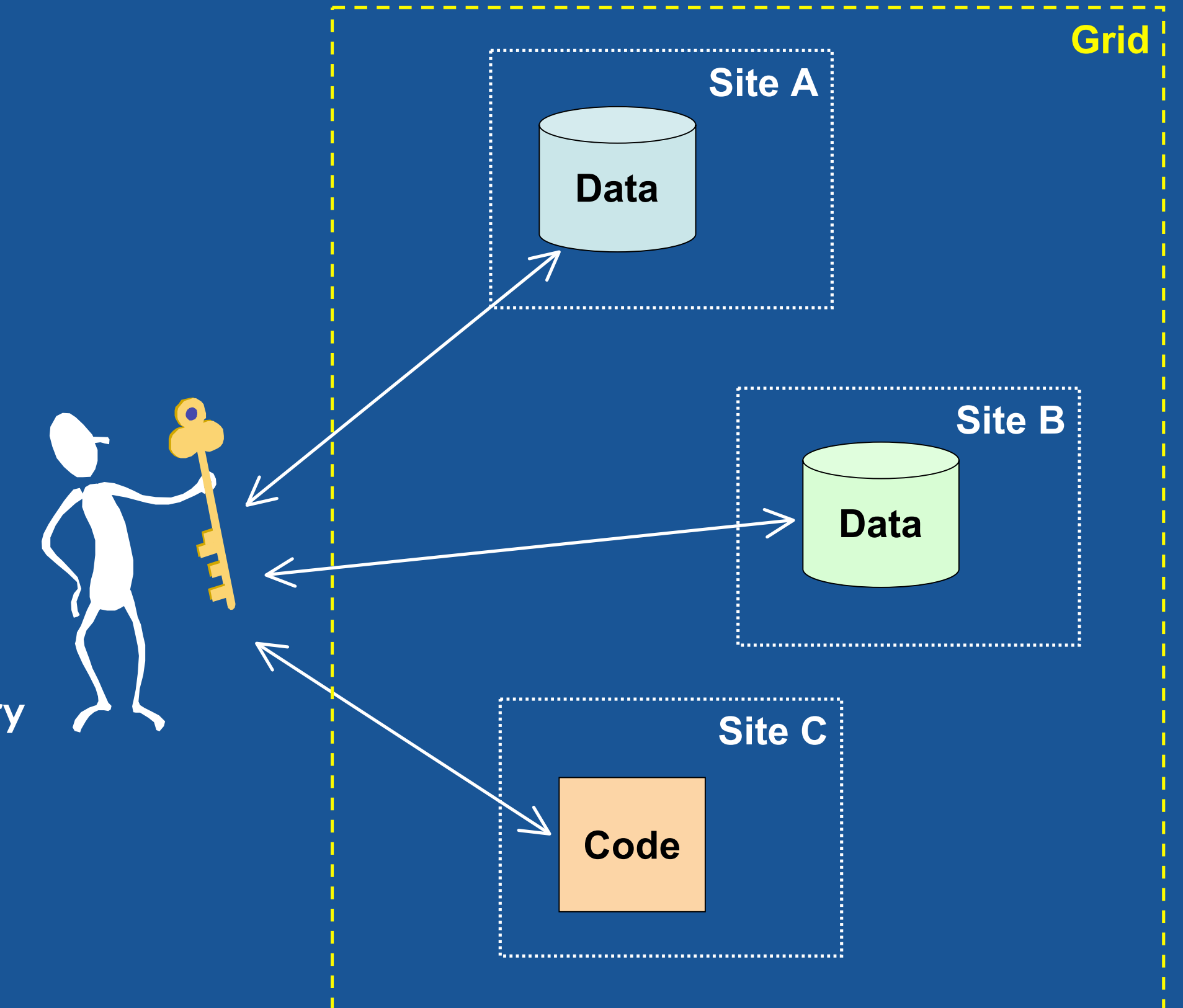
How does a scientist authenticate with resources in different administrative domains?



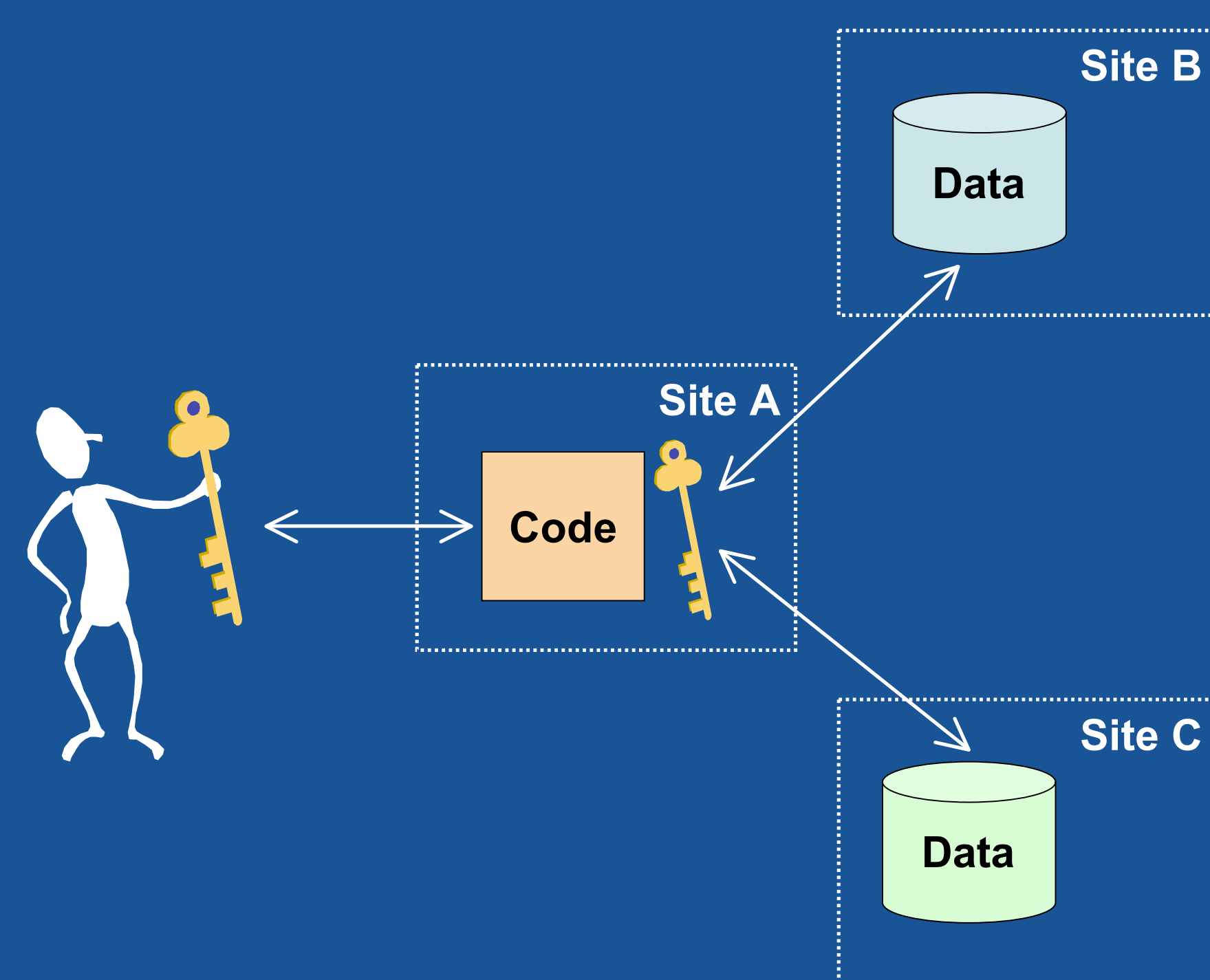
- Scientists that would authenticate with multiple resources must use multiple authentication methods
- Many usernames & passwords
- Administrators have no way to uniquely identify a single scientist across multiple resources
- A single sign-on is needed

FusionGrid users are identified with X.509 credentials to provide a single sign-on capability

- FusionGrid uses X.509 credentials to identify users
 - Certificate + Private Key
- One user, one credential
- Use the same credential for all resources
- One username & password
- Unified authentication is one necessary piece of building a grid



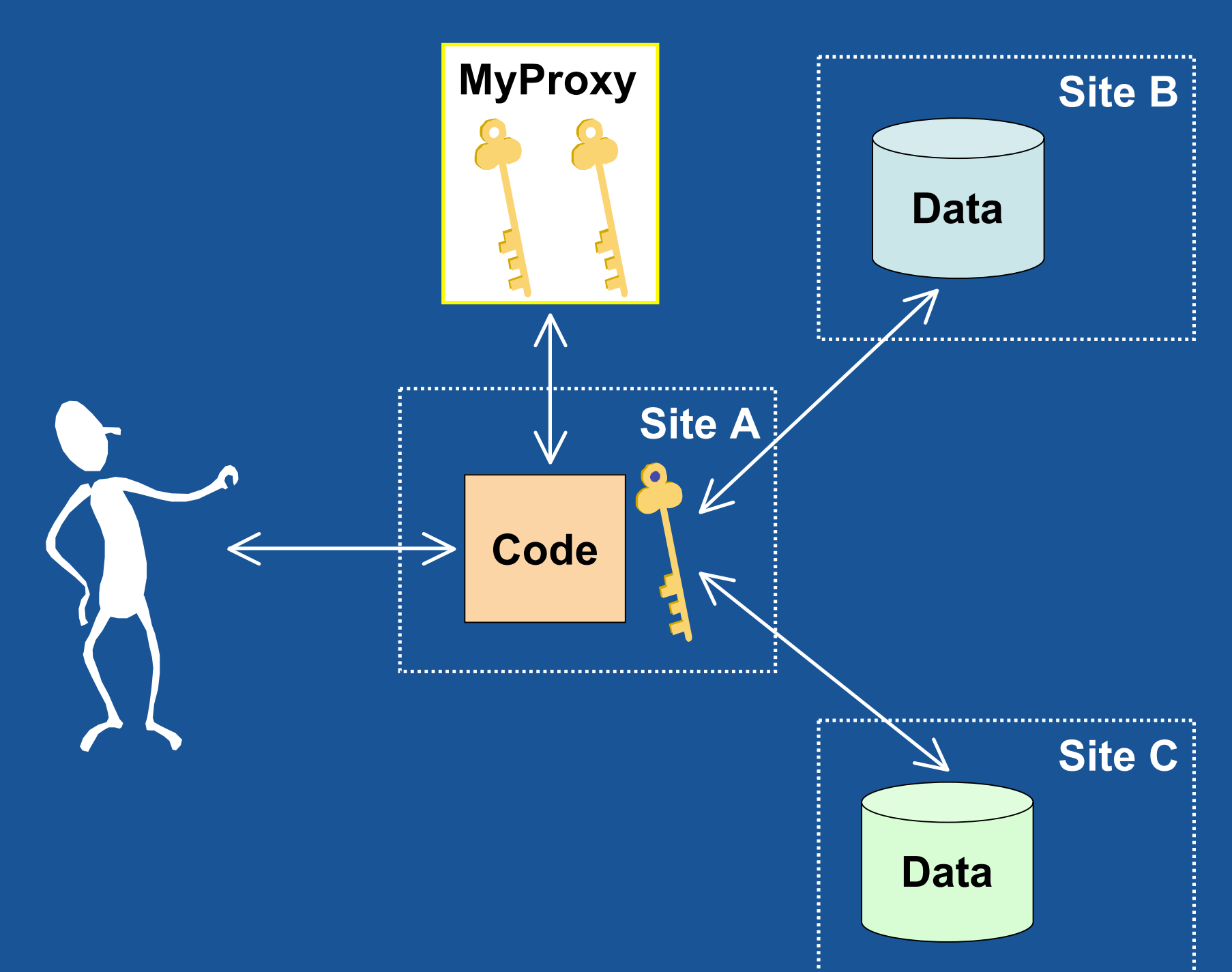
Delegation allows codes to act on behalf of users



- Use of Globus Security Infrastructure (GSI) allows for delegation of credentials
- Example: you launch a code, which uses a delegated proxy to do work on your behalf
- The code itself authenticates with databases to read/write data, for example

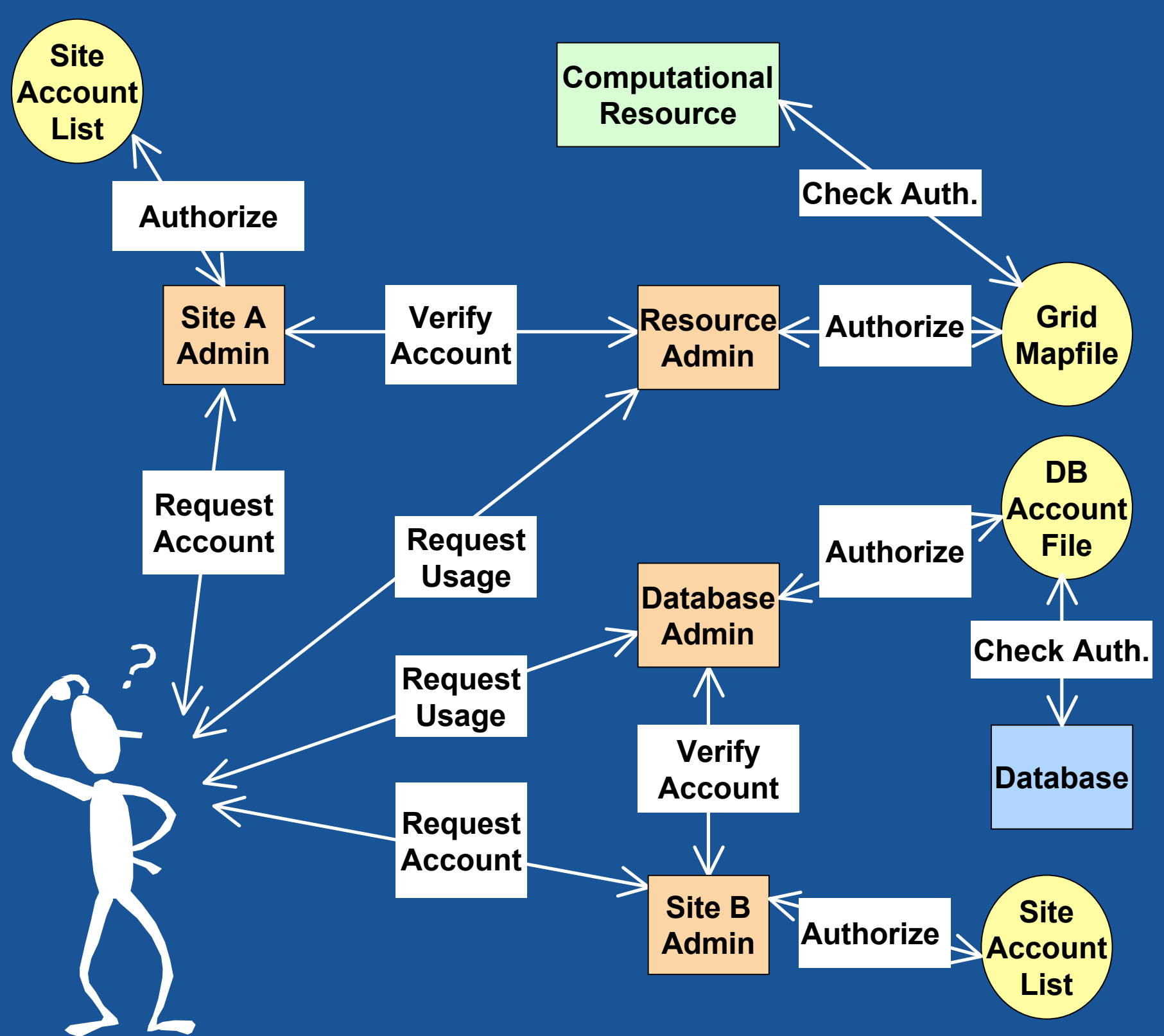
A MyProxy server is used to store credentials

- Self-management of credentials proved to be troublesome
- FusionGrid now uses a MyProxy credential storage server
- Users get a delegated proxy from MyProxy by entering username & password
- Example: enter password to sign on, then code uses delegated proxy to authenticate



Authorization

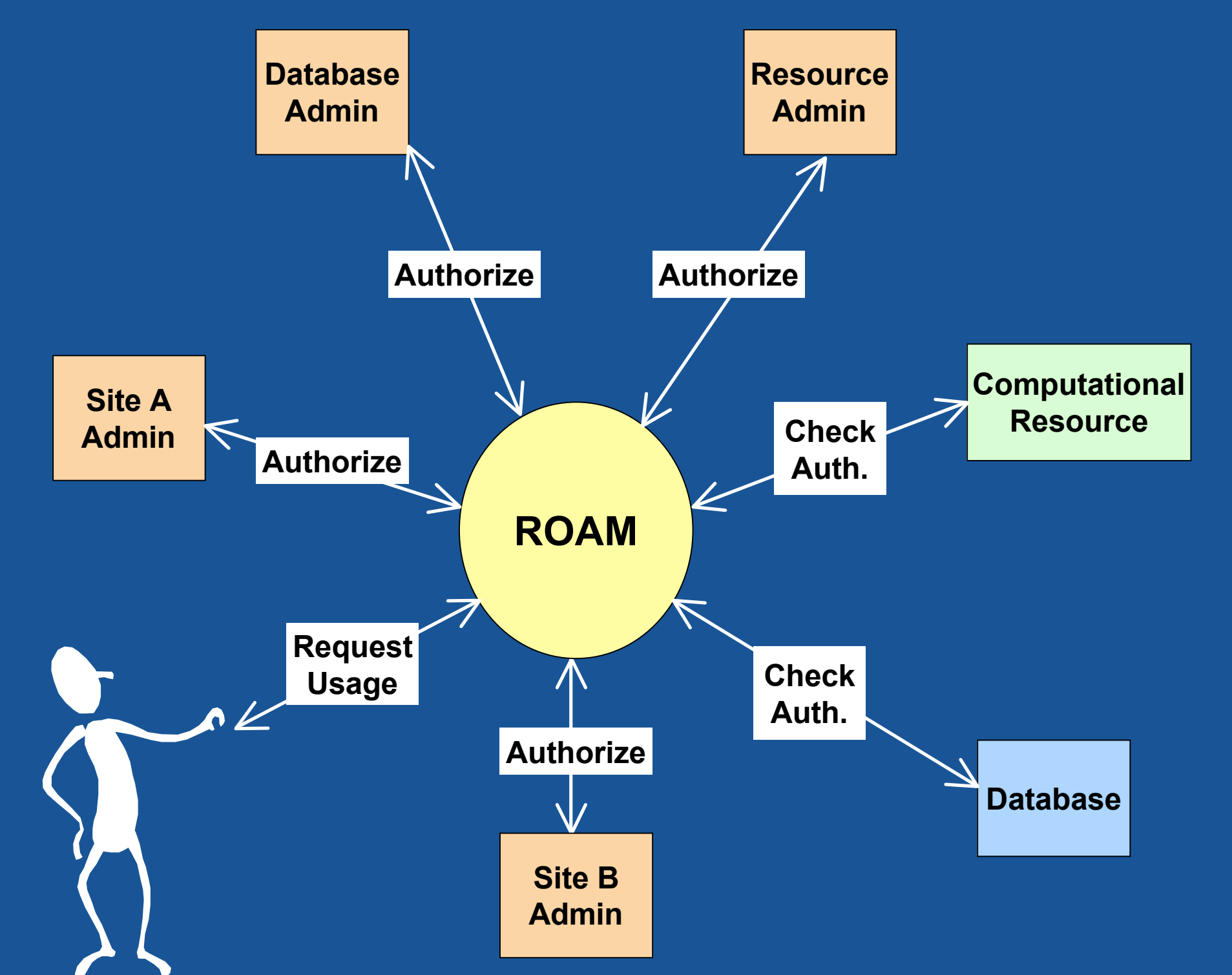
How do stakeholders control access to their resources?



- Scientists must get authorization to use the various resources of a grid
- This can be a confusing process
- No cohesive picture of authorization policy
- Each resource administrator has an independent access control mechanism
- No "one place" to go to do authorizations

The new ROAM authorization manager simplifies authorization

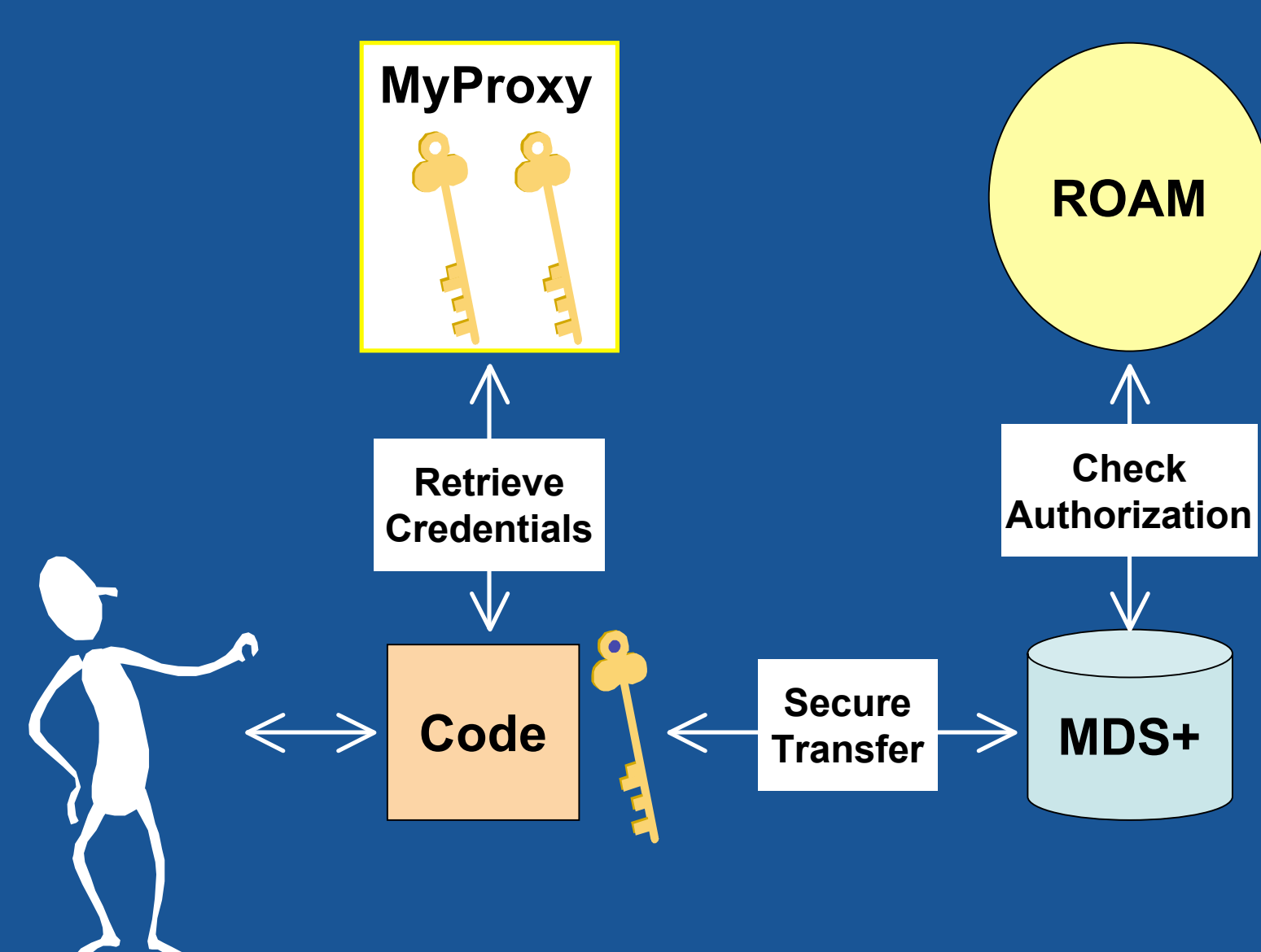
- FusionGrid developed the Resource Oriented Authorization Manager (ROAM) to make authorization easier
- Provides:
 - A coherent authorization model
 - Centralized information
 - Control remains distributed for maximum flexibility
- One place to go for authorization requests
- Used by administrators, codes, and users



Secure Data Storage and Transfer

MDSplus modified to work with delegated X.509 credentials (MyProxy) and ROAM

- MDSplus provides secure data storage and transfer for FusionGrid
- Updated to work with GSI
 - FusionGrid developers built a "lite" version that even works on Mac OS X
- Can handle proxy certificates or delegated proxy certificates
 - Works with MyProxy
- Can contact ROAM for authorization checks and account mapping
 - No /etc/mdsip.hosts or /etc/grid-mapfile needed!



Future Computing Environments

ITER and other future computing environments will need to address these same security issues

- Moving forward, one vision to increase computing power available for between-shot tokamak analysis is to move computing onto the WAN
- This introduces the same challenging security issues addressed by FusionGrid: Authentication, Authorization, and Secure data storage & transfer
- Site security requirements (Firewalls, One Time Passwords) must be reconciled with distributed computing requirements (Credentials)
 - Today, site security and grid computing conflict
 - They must interoperate
- ITER will require collaboration across administrative domains and international borders
- The solutions developed for FusionGrid and the lessons learned may be used to solve security issues for these future computing environments

