

RADIUS and Securid

Michael Helm

13 May 2004

RADIUS & SecurID

- Support OTP initiatives
 - Security incidents spotlight password issues
 - Authentication Fabric testbed
 - Feasibility study: RADIUS, SecureID
- What role would ESnet play?
 - Why are we interested? Our GRID commitment
 - Isn't this a site problem?
- Project outline
- What do we need? We need your help...
 - SecureID advice
 - Project advice
 - Review

One Time Password Support

- Grid response to One Time Password Initiative
Several DOE sites and facilities are in danger of being overwhelmed by security issues and compromises traced back to re-usable passwords (among other things).
Grids, despite use of PKI, have some specific vulnerabilities.
Grid middleware developers are developing a response to this problem.
- Sites are looking to One Time Password-like techniques to meet security needs

Support OTP Initiatives

- Requirements Doc in progress
 - (*NERSC, Steve Chan & al*)
 - Consortium of DOE labs
 - Open invitation
- Project being developed
 - 2 foci: RADIUS
 - Motivated by GRID middleware
 - Refactoring Grid services
 - Only mention in passing today
 - Variety of OTP and tokens explored
 - At this moment, we propose a feasibility study to determine whether the approach will work, what issues might exist, determine scaling laws, &c

ESnet Role

- ESnet supports Office of Science programs –
 - ‘Candidate’ projects: cost effective centralizing/distribution/hierarchic management
 - ESnet provides internationally trusted PKI
 - the DOEGrids CA
 - Supports DOE Grid efforts
 - ESnet root CA
 - Other subordinate CA’s
 - ESnet proposes an Authentication Fabric*
 - An interoperable authentication fabric, through RADIUS, to support Grids and meet DOE and site security requirements
 - Voluntary
 - **Eli Dart, NERSC*

ESnet Role (2)

Isn't OTP/Authentication a site problem?

Most of the real work with OTP remains a “site by site” problem. But the driver for our proposal is Grid work

- Grids need a level of site interoperation
- N x M interop agreements are expensive
 - What kind of authentication federation do Grids really need?
- “Virtual Organizations” have tended to drive Grid work, more than sites, but ...
- This is an opportunity to leverage site infrastructure & reduce expenses
- We propose an interoperability framework & infrastructure

Résumé slides

The next set of slides describes the DOEGrids Certificate Authority / ESnet Public Key Infrastructure project and facilities. They demonstrate the work done to provide the DOEGrids services.

In addition we are supported by ESnet engineering and technical services.

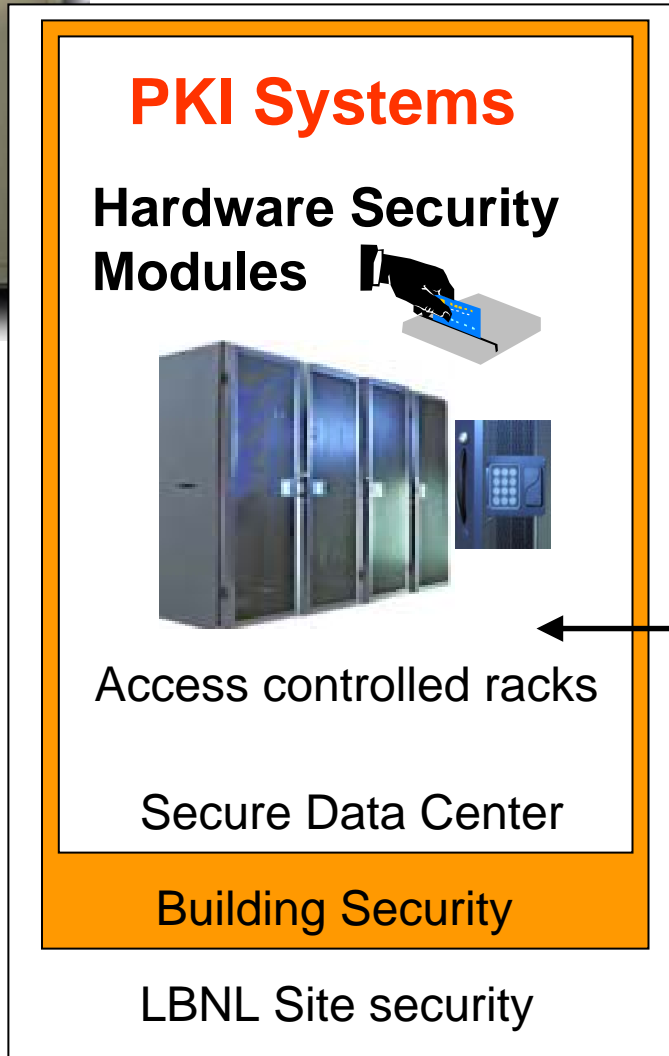
We can do the job.

ESnet PKI team

- DOEGrids CA
 - Built
 - Deployed
 - Operate
- 3 FTE + support
- PKI for Office of Science projects
 - Primarily Grid ID's
 - Other uses
- Federation – community

DOEGrids Security

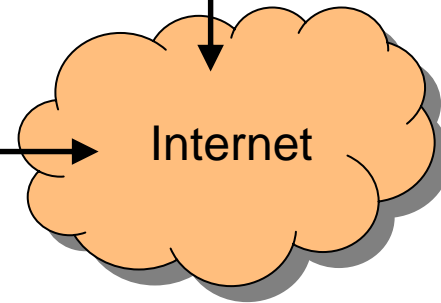
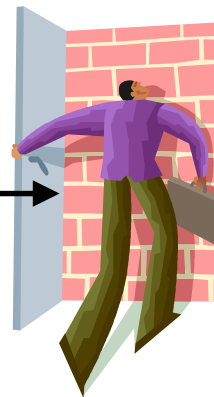
Offline Vaulted Root CA



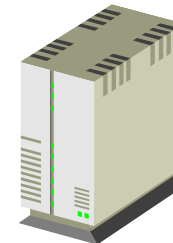
Grid User



Fire Wall



Internet



Intrusion Detection

Features In Depth

- LDAP
 - Directory of accounts (certificates)
- Hardware Security Module
 - Move private key to “hardware” domain
 - Unique expertise
- Support Multiple CA Profiles
 - DOEGrids: conventional PKI
 - NERSC: Long Term Credential Store CA
 - ESnet SSL: Classic SSL server certificates
- Statistics
 - <http://www.doe grids.org/pages/DOEGridsCAStats.html>

Federation and Community Leadership

- Manage & host DOEGrids Policy Management Authority
 - Sets policies for certification in DOEGrids
 - Manages membership and domain of services
 - Office of Science participating programs have “stake” in CA!
- International Grid Federation (see supporting slides)
 - Work to establish Asian Pacific Policy Management Authority
 - Member of European Data Grid and joined new EGEE Federation
 - Joined TERENA Top level CA registry
- Experimental OCSP service
 - Demonstrate improved certificate validation techniques
 - Demonstrate improved delivery of certificate services
- Provide NERSC PKI with a secure CA (see supporting slides)
- Global Grid Forum – Grid Standards organization

NERSC PKI (2)

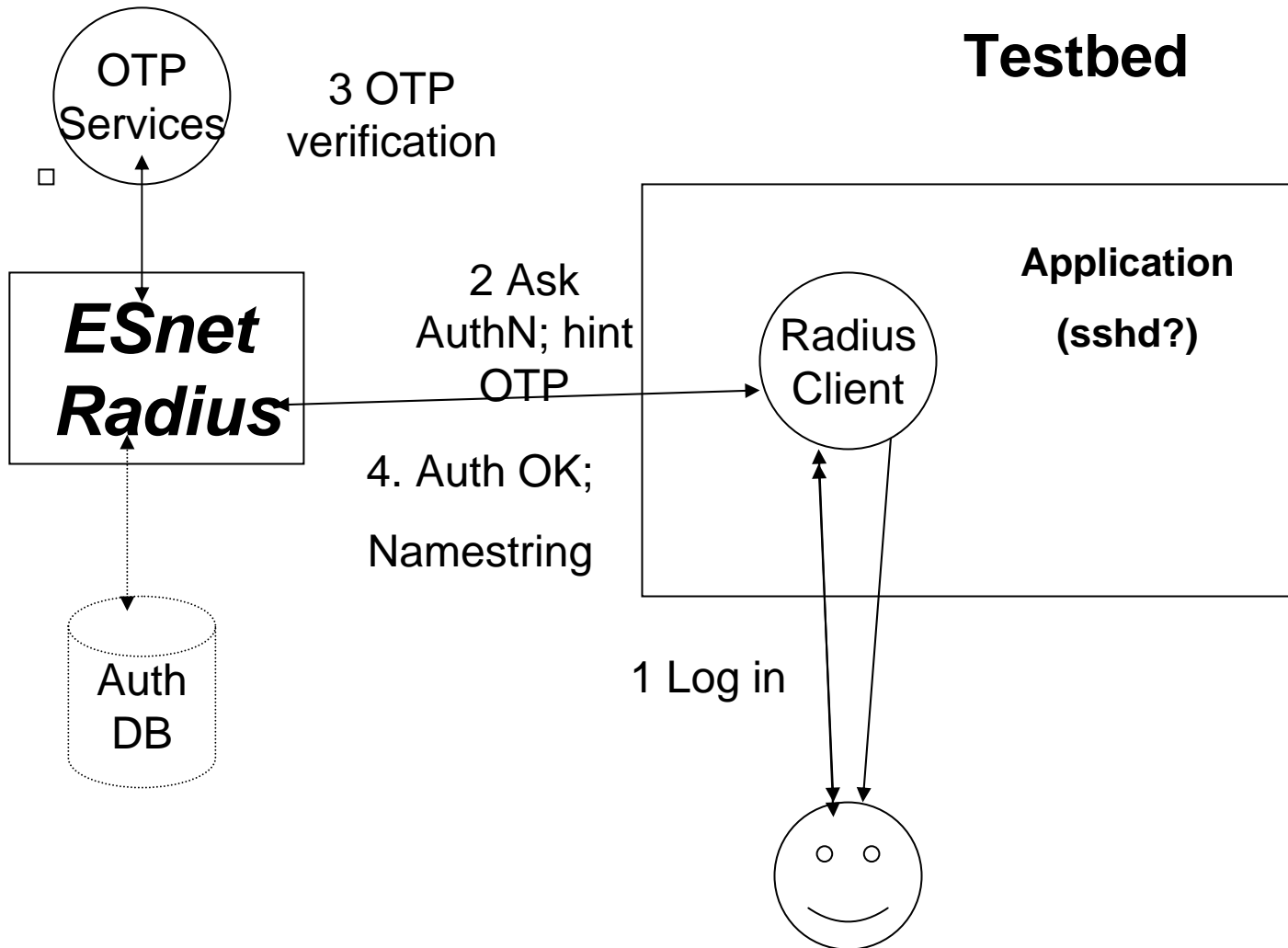
- **To get NERSC PKI accepted Internationally, ESnet established a new process for evaluating CAs**
 - Draft GGF document on CA profiles
 - First submission scheduled for next Global Grid Forum
 - Identifies 3 known CA profiles
 - Classic PKI (i.e. DOEGrids)
 - Large site integrated proxy services (SIPS)
 - Credential stores (i.e. NERSC)
 - EU Grid Policy Management Authority will contribute to Document.
- Service Level Agreement
 - Establishes clear operational requirements
- Certificate Policy/Certification Practices Statement
 - Helping NERSC to produce an internationally approved set of policies and procedures for their CA
- Peer with international community
 - Establishing NERSC as a full member of the International trust community.

Project Outline

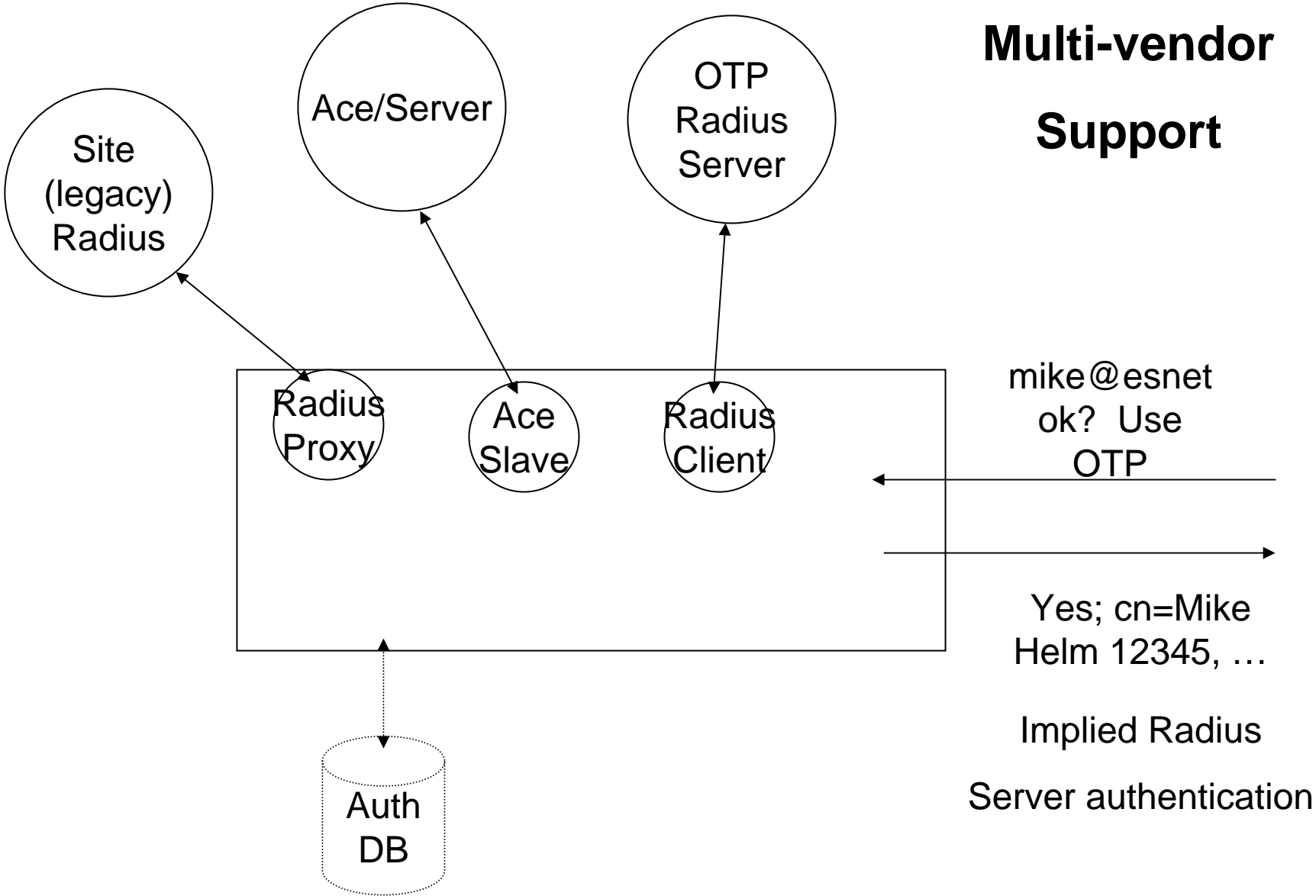
- Feasibility study
 - Simple:
 - One OTP product
 - RADIUS service
 - One simple Application: login, sshd, ?
 - Complex:
 - Multiple OTP products -or-
 - Multiple servers of one OTP product
 - HA configurations
 - Geographical dispersion
- ESnet proposal – pilot project

Feasibility study

Testbed



ESnet Radius Multi-vendor Support



ESnet Radius (2)

- Appliance
- Dedicated Hardware
- Minimal ports open
- High Availability
- Geographical dispersion



ESnet Radius (3)

Data Model

- Sites manage data
 - RADIUS as Federation point
- ESnet manages infrastructure & “transport”
- Partition RADIUS server
 - Sites manage/federate populating user db
 - Only Grid data (name) provided to grid app
 - For now?

ESnet Radius (5)

What does login look like to customers?

Because we are forwarding (proxying for) multiple authentication domains, login users will need to specify their realms, eg
mike@es.net

Login may look much like Windows domain login

Local name + realm (domain) == unique account name

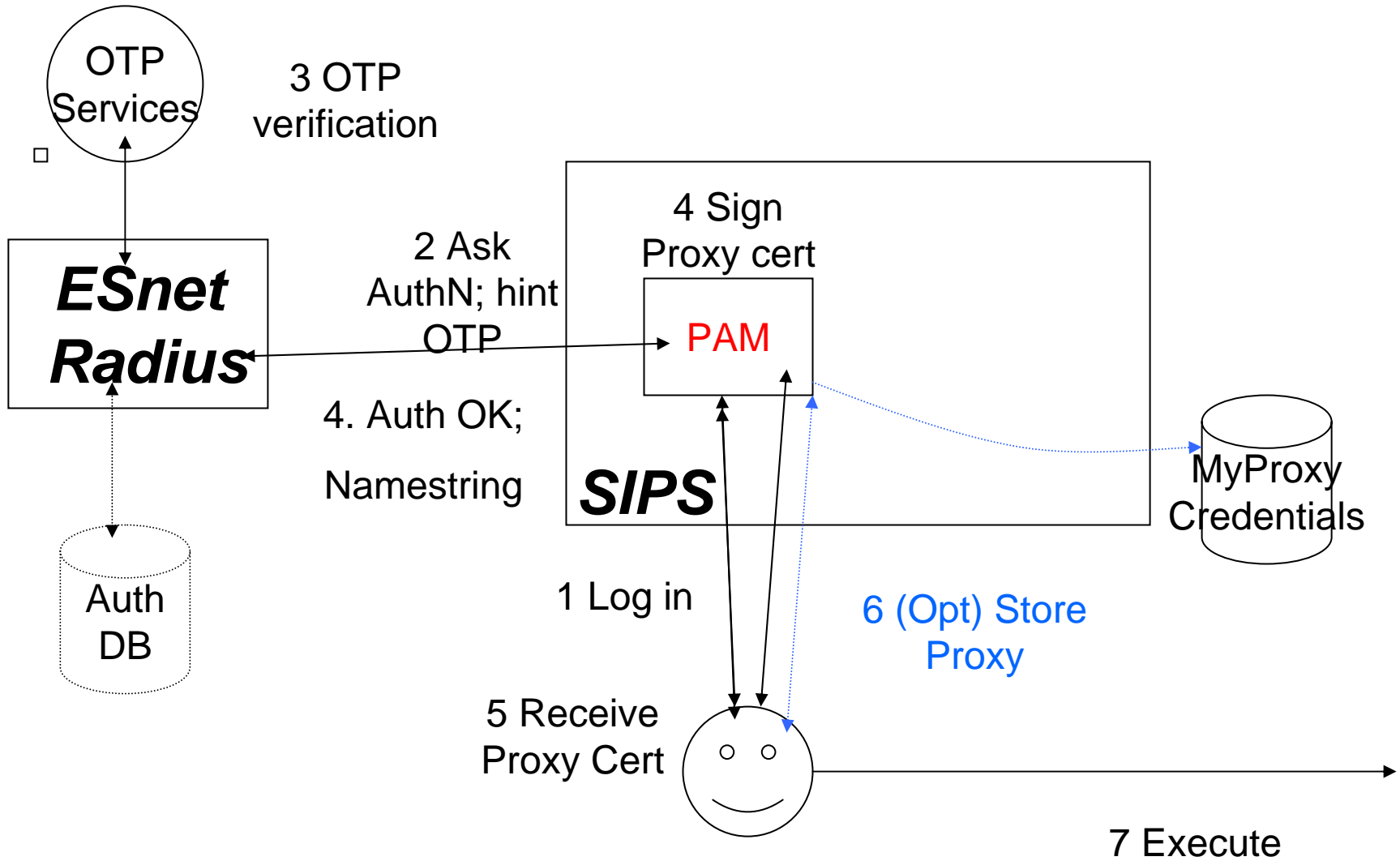
ESnet RADIUS Authentication Fabric (Summary)

- ESnet RADIUS – Authentication Router
- Deploy as many units as needed
 - One or more per site
- ESnet provides a “transport layer” but sites manage most of the data content directly
- Routers should present identical data everywhere (federation), but could proxy for other RADIUS servers, proxy between
- RADIUS servers could be used to support other site infrastructure

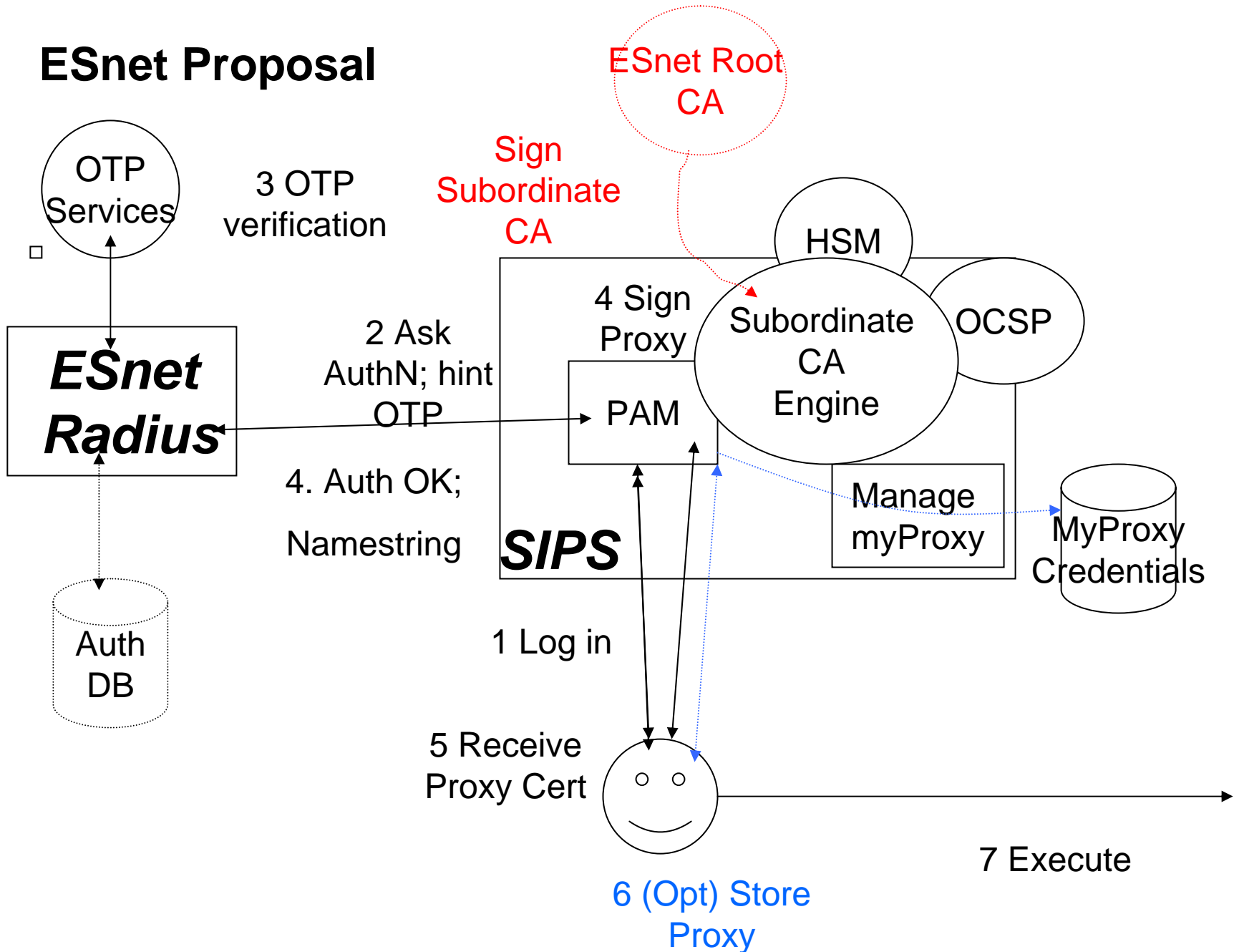
Where are we going with this?

- Support Grids
- Grid Middleware Response
 - Gridlogon
 - Evolution of MyProxy to long term credential store
 - Site Integrated Proxy Services (SIPS)
 - Generate Grid proxy certs directly
 - (Originally) Integration into local Authentication infrastructure
 - ESnet variant: Focus on RADIUS (RAPS?)

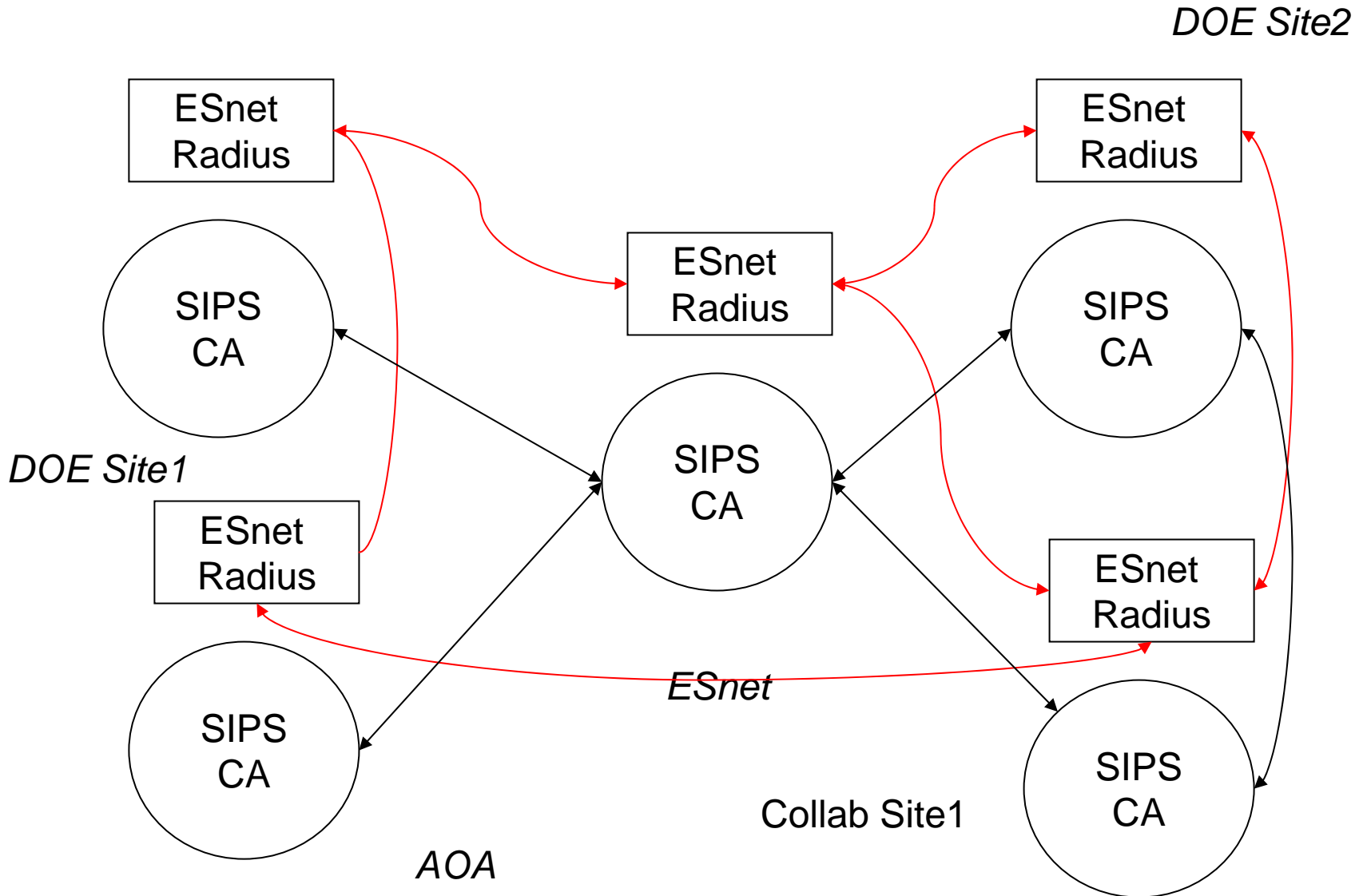
ESnet Proposal



ESnet Proposal



Put It Altogether!



Put It Altogether

- The ESnet RADIUS servers replicate their data amongst each other
 - Master-slave configuration developed from pilot
- SIPS or GRIDLOGON
 - Instances of a single, distributed CA?
 - Locally managed CA infrastructure?
 - *(This is another part of the project!)*

What do we need?

- SecureID advice
 - We have focused on RADIUS
 - RADIUS & SecureID *appear* to play together
 - Vendor relations
 - Configuration, servers, demo app
- Project advice
 - Is this feasible? What might we be missing?
- Review
 - What would need to make it useful for you?
 - Alternatives: the GA & PPPL interop

Discussion

- ... and thanks!