



Alliance Public Key Infrastructure: History and Future

**Randy Butler, NCSA Associate Director
Von Welch, NCSA Senior Systems Developer**

February 2000

PROJECT MOTIVATION	3
CURRENT ALLIANCE STRATEGIES	3
Kerberos.....	3
SSH.....	3
WHAT IS PKI?	4
PKI Support	4
ACCOMPLISHMENTS	5
Certificate Policy Written	5
Certificate Authority Established.....	5
Grid Security Infrastructure Demonstrated at SC99	5
Application Interface Chosen	6
Packaging and Deployment	6
Documentation and Support	6
Collaborations.....	6
YEAR ONE SUMMARY	6
PAPERS	7

Project Motivation

Authentication to resources is a critical early service when considering the foundation services that will support the Grid. Authentication is identified in Foster's "[Building the Grid: An Integrated Services and Toolkit Architecture for Next Generation Networked Applications](#)" as residing in both the Grid Services (middleware) and Grid Fabric. Strong authentication of users and resources allows sites to secure resources while allowing users maximum flexibility in a distributed environment. A unified Alliance authentication scheme together with a unified Alliance account management scheme makes it possible to think about our two goals, **strong authentication and single sign-on to Alliance resources**. In order to provide focus to this project we have limited our target solution to the six Advanced Computational Resources Sites (ACRS), while considering expansion beyond the Alliance.

Alliance solutions must consider scalability because there are thousands of Alliance users and potentially tens of resources sites. Any solution we adopt will likely be around for the lifetime of the Alliance or another 10 years. In that time we see the prospect for our solutions, if successful, to be expanded well beyond the walls of the Alliance Virtual Machine Room (VMR).

The VMR is in reality a handful of separate computational policy domains, each with their own set of policies and local implementation issues. We are unwilling to dictate dramatic system administration changes at these sites because that approach does not lend itself well to expanding our solution outside of the immediate Alliance community. Our approach, therefore, is to create layers on top of local policy and technical implementations. Further we will use standards-based interfaces between these layers to accommodate the highest level of local flexibility.

Current Alliance Strategies

Early in this project we identified the need to document authentication strategies at each of the Alliance ACRS sites. Three of the sites support clear-text Unix style authentication, two sites support Kerberos Version 5 (V5), and all sites support SSH Version 1 (V1). We define strong authentication as one that securely identifies an entity in a way that assures confidentiality of the entity's secret (password) and that provides the resource owner confidence in the entity's stated identity. Clear-text authentication does not meet our definition of strong authentication. In fact clear-text authentication is sorely lacking and is the cause of great concern in the Internet community today. This method was discounted early in the project.

Kerberos

Kerberos V5 has gained momentum in the last year with a number of sites embracing it to solve their local campus and department authentication needs. Two of the ACRS made major commitments to Kerberos V5 in the last year and both are satisfied with the results. Kerberos does meet our definition of strong authentication, basic services like ftp, telnet, and the r-commands are well supported and support in third-party applications is growing. Kerberos utilizes tickets that provide a solid base upon which to build single sign-on capabilities including something called *cross-realm authentication* that allows consenting sites to accept tickets from each other.

Kerberos however does require a substantial investment in systems administration and systems programming support to integrate it into local computational domains. NCSA's effort took approximately 3 to 4 FTE years to bring into production and we are currently expending 1+ FTE time to support it in the form of continuing site development needs, administrative support, and user consulting. Kerberos is one of those technologies that technical people have strong opinions about — either they like it or they hate it. While it does solve many of our cited needs it does so, unfortunately, at a heavy price. In the final analysis we did not see it as a good long- or even short-term solution for the Alliance.

SSH

In place and supported by all six ACRS sites, SSH is a popular choice by system administrators because it uses a simple link encryption scheme to protect the confidentiality of a user's password. Further the

integration of SSH into an environment is trivial. Users have widely accepted SSH because the tools are simple and do what is needed from a user's perspective, and because the user has the ability to manage the environment.

Drawbacks to SSH are few but significant. SSH's RSA-style (Rivest-Shamir-Adleman Internet encryption) authentication utilizes public and private key pairs. SSH's implementation of RSA depends on the users for key management and for the establishment of cross authentication between resources. This is a feature many sites are against because they lose central authorization control of the users, making it difficult to shutoff a particular user without being invasive of user privacy. Because every user is required to establish cross authentication between utilized resources, authentication is tedious and wasteful. SSH does allow for Kerberos style authentication. However this implies that the site has Kerberos support, which, as noted, is not a simple undertaking.

In the end, SSH was deemed to be a valid short-term solution but not so for the long term. Without the central control and a real key management strategy we did not see it fitting into the needs of the Alliance. Further our sense from talking with other sites and projects is that they also feel it is at best a short-term solution given today's implementation.

Something more is required because we did not feel that any of the current solutions offered us what we needed. It does not take long however to recognize the effort governments, major projects, and corporations are pouring into an authentication technology called PKI.

What is PKI?

Public Key Infrastructure (PKI) is based on third-party trust. This third-party vouches for the identity of an individual or other entity. The physical "proof" is held within a digital certificate that has been digitally signed by this third party. In this way two parties that otherwise do not have any relationship can trust the identity of the each other. A typical use of this certificate is to authenticate to a compute resource. So instead of presenting a password you (or your program) present this digital certificate as "proof" of identity.

In order to establish trust each party must have faith in the third party that certifies identities. In PKI parlance, this third party is a Certificate Authority (CA). Trust of the CA is established through a Certificate Policy (CP) that is generally written by the relying parties who are the ones taking the risks. The CP states all policies related to how the CA establishes identity and how it manages keys and certificates.

The Policy Management Authority (PMA) is an empowered team from the relying parties. The PMA manages the CA through the policy. They are responsible for the upkeep of the CP and for keeping track of how well the CA conforms to the CP. The CP includes references to how tight security controls are for the CA's servers and critical information and states the frequency and form of CA audits. Local Registration Authorities are responsible for identity confirmations. The CA generates certificates, publishes them, and publishes the revocation lists that are utilized as a means to reject compromised keys.

Current PKI implementations utilize certificates that are based on the X509 V3 standard (an international standard for authentication) with the goal of interoperability between implementations. This meets one of our stated goals to allow for the expansion of our solution beyond the Alliance, addressing scalability nicely by establishing the third-party trust model. A site or entity does not need to store users' public keys; rather the site first authenticates the CA's signature by decrypting it with the CA's well-known public key. Next the public key bound by the CA's signature in the user's certificate is used to present a challenge to the user. Only the holder of the matching private key can successfully respond to the challenge. So this clearly meets our definition of strong authentication.

PKI Support

PKI deployment is growing rapidly for support of general authentication needs. While not a simple solution it offers scalability, interoperability, strong authentication, and implementation flexibility. PKI enjoys wide-spread use today on the web and is supported by the major web browsers. It appears to be a very good long-term authentication strategy for the Alliance. This was verified by holding an open meeting on authentication at Argonne National Laboratory (ANL) in December 1998. In that meeting we presented our case for building an Alliance PKI and also offered an implementation strategy. ACRS technical and policy

reps attended this meeting as well as staff from NASA, NPACI, and DOE. This meeting was followed up by an NPACI-sponsored meeting on roughly the same subject and overall our strategy was strongly supported. NASA already has a PKI testbed in place between the IPG labs and has detailed plans on a NASA-wide rollout. Government agencies and industry are also actively deploying PKI.

In our December 1998 meeting we agreed not only to build an Alliance PKI but to utilize the Grid Security Infrastructure (GSI) developed under the Globus project to take advantage of [X509 V3 digital certificates](#). We agreed to target July 1, 1999, as the production date of the Alliance PKI although this date was not met. We anticipate that the early adopters of this service will be a handful of Alliance projects that require distributed computing capabilities and those involved in systems administration of Alliance resources. Current authentication strategies supported at the sites such as Kerberos or SSH will still be available and will likely continue to handle the bulk of authentication in the first year.

Accomplishments

We have already made great progress on the Alliance PKI. To date we have received broad acceptance from both the technical and policy types within the Alliance. Overall sites see this as a powerful new tool that has positive impact that reaches beyond the Alliance. Coordination with related efforts is key to building an effective PKI solution. Towards this cause we have made presentations at multiple workshops and meetings and have coordinated our efforts closely with both NPACI and NASA IPG.

Certificate Policy Written

The heart of PKI is the Certificate Policy (CP) that defines what things are important and sets direction that is used to guide how the CA is implemented. This is a crucial internal document for Alliance staff but it is also documentation that is used by others in deciding whether to trust our certificates. The Alliance stated policy and rules in the CP can be compared directly to NASA's CP, for example.

The Alliance CP is complete. It was given to NPACI and they in turn used it as the basis for their own CP. We have also exchanged CPs with NASA IPG so that we can assure interoperability among certificates.

NPACI and the Alliance have agreed to accept each other's certificates. This means that researchers will need a certificate from any PACI-funded site. They will eventually be able to use this single certificate to authenticate across PACI sites.

Certificate Authority Established

Funding from NSF has allowed us to subcontract the CTD Division of ANL to run the Alliance Certificate Authority, which is undergoing final reviews. The CA is scheduled for early production in January 2000. An Alliance Policy Management Authority (PMA) has been assigned to oversee the operation of the CA. This committee met for the first time in August 1999.

One of our hopes was to leverage this work and specifically the CA to benefit related projects. There is an obvious close relationship between the Alliance and the Globus Project, and as a result we agreed to utilize this CA to produce certificates for the general Globus "Grid" community. Further we extended an offer to NPACI to utilize this CA as a PACI-wide solution; however they decided to deploy their own CA. We continue to discuss relationships with NASA IPG and the Committee on Institutional Cooperation (CIC) possibly leveraging this CA for their needs.

Grid Security Infrastructure Demonstrated at SC99

Grid Security Infrastructure (GSI) was initially developed under the Globus project and was recently supplemented by an NSF NGI grant and the Alliance to solve the very problems outlined in this paper. GSI is based on GSS-API (see below), uses the SSLeay protocol, which is the de facto industry standard, and handles standard X509 V3 certificates. It has broad support for proxy certificate generation and use, which allows us the flexibility to run batch style jobs with minimal exposure of a user's private key. The current clients supported by GSI are SSH and FTP.

GSI was deployed to the six ACRS sites prior to SC99 and single sign-on was demonstrated. We are now working out a deployment and support strategy for GSI clients.

Application Interface Chosen

We have determined that we will utilize the Generic Security Services Application Programming Interface (GSS-API) whenever possible as the interface between our Alliance PKI authentication software and applications such as the SSH client and FTP. Further we have already extended SSH and FTP to accept the GSS-API so that they can be used as part of the GSI. The modified SSH Windows clients have been picked up by the commercial company Van Dyke, which today sells a popular SSH Windows client, SecureCRT.

Packaging and Deployment

Through our efforts we hardened the GSI software. We generated documentation and adopted a strategy to deploy in the fall of 1999 at the [six Alliance ACRS](#) sites. Early adopters will begin using our PKI implementation soon and are hoping for a group of 200 participants by the end of 2000.

Documentation and Support

We have edition 1 of the GSI User Guide available. It walks the user through the steps to get the software installed, request a certificate, load their certificate and private key, and the use of the various tools. NCSA Consulting staff are reviewing the documentation and will make any edits based on end-user needs. Support for end-users is expected to come from NCSA Consulting Services.

Collaborations

The NSF NGI (Next Generation Internet) grant funded a number of collaborative PKI activities:

- hosted a strategy meeting in December 1998
- attended an NPACI hosted coordination meeting in February of 1999
- presented at an I2 event late spring 1999
- presented numerous times at Alliance events
- presented at the EDUCAUSE SAC conference
- participated in the EDUCAUSE sponsored workshop on PKI

We continue to openly share our experiences through the recently organized Grid Forum, and more specifically in the Grid Security Working Group co-chaired by Randy Butler and Andrew Grimshaw.

Year One Summary

We have a policy defined, have organized the PMA, and understand how the CA will function and what services it provides. The CA was operational on target of January 2000. GSI is the solution to user-to-Grid authentication interface. We have slipped our target date of July 1, 1999 by a little but are confident in the amount of progress we continue to make.

We envision gaining needed experience running the Alliance PKI over the next year. With what we learn, we anticipate that the implementation will be modified while still maintaining a production service. At this point we do not see any technical roadblocks but we do envision some policy changes as we gain experience. Policy modifications such as the strength of the identity verification, which is responsible for the verification, how is it done, and lifetimes for the certificates all elements that our implementation of PKI should be able to accommodate. We recognize the need to continue to monitor and adjust our approach and thus we will continue to devote technical and policy FTE time towards this effort. We are working openly and have participated in numerous workshops and conferences sharing our approach.

Papers

[Design and Deployment of a National-Scale Authentication Infrastructure](#). R. Butler, D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, V. Welch. Describes our experience designing, developing, and deploying the Grid Security Infrastructure.