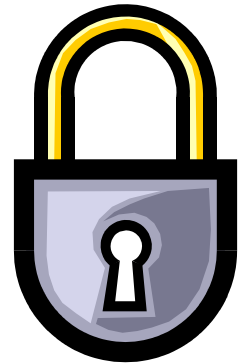


PKI and CKM[®] Scaling Study



NCASSR Kick-off Meeting
June 11-12, 2003

Jim Basney

jbasney@ncsa.uiuc.edu

<http://www.ncsa.uiuc.edu/~jbasney/>

Project Summary

- Collaboration with InfoAssure, Inc. to assess scalability of PKI and CKM[®]
- InfoAssure will provide DoD and Intelligence community requirements
- NCSA will perform an analytical and performance modeling study
 - Evaluate PKI and CKM[®] management overhead
 - Credential generation, distribution, revocation
 - Trust management and risk mitigation
 - Evaluate system performance
 - Using NCSA supercomputers to generate loads

Research Relevance

- High costs of deploying and managing PKIs discourages adoption
- Poor usability results in high support costs and decreased productivity
 - Difficulty obtaining and renewing credentials
 - Lost or compromised credentials
 - Forgotten passphrases
 - Confusing authentication errors
- Scalable PKI requires scalable processes and procedures
 - Automate processes whenever possible
 - Eliminate common usability issues with better system design

Research Relevance

- Establishing inter-organizational trust is hard
 - Conflicting requirements and trust models
 - Identity verification
 - Key management
 - Authentication methods
 - Technology conflicts
 - Incompatible certificates, protocols, algorithms
- Traditional solutions
 - Audits
 - Insurance
 - Contracts with penalties
- Support for alternative trust models can help

PKI Trust Models

- CA based
 - Hierarchical (shared root CA)
 - Cross-certification (may be asymmetric)
- Relying party based
 - Local list of trusted CAs
 - Web browser model
- Fully distributed (PGP “web of trust”)
 - Individuals sign keys rather than CAs
 - Good fit for ad-hoc communities
- Federated trust
 - User establishes binding between credentials
- Third-party authorization services
 - X.509 Attribute Authorities
 - SAML/XACML/XrML Authorities
- Credential wallets
 - Universal acceptance of a single credential is unlikely
 - Issue different credentials for different purposes, stored in user’s “wallet”
 - Negotiation protocols choose credential

Project Milestones

- 1st Quarter
 - Complete initial CKM[®] training
 - Establish PKI and CKM[®] evaluation infrastructure
- 2nd Quarter
 - Review requirements provided by InfoAssure
 - Begin PKI modeling and evaluation
- 3rd Quarter
 - Complete PKI modeling and evaluation
 - Begin CKM[®] modeling and evaluation
- 4th Quarter
 - Complete CKM[®] modeling and evaluation
 - Deliver final report

Project Team

- NCSA Grid and Security Technologies staff
 - Jim Basney, Project Lead
 - Senior Security Engineer (to be hired)
 - Rafael Bonilla, Security Engineer
 - Adam Slagell, Security Engineer
- Related Activities
 - MyProxy Online Credential Repository project
 - Global Grid Forum working groups
 - Authorization Frameworks and Mechanisms
 - CA Operations
 - OGSA Security
 - NCSA Grid PKI Activities (TeraGrid)
 - Other NCASSR projects