Notes on 2nd PKI Workshop

Bob Cowles
bob.cowles@stanford.edu

CA Managers Meeting, CERN
12 June 2003

Work supported by U. S. Department of Energy contract DE-AC03-76SF00515

References

- Main page
  http://middleware.internet2.edu/pki03
- Proceedings at
  http://middleware.internet2.edu/pki03/PKI03-proceedings.html
- Published Papers
  http://middleware.internet2.edu/pki03/presentations/pki03pp.pdf

Some Random Info

- 121 participants -- 27 years of research into PKI issues
- All problems have been solved
- Program Committee:

Peter Alterman	NIH
Matt Blaze	AT&T Labs Research
Bill Burr	NIST
Yassir Elley	Sun Microsystems
Carl Ellison(chair)	Intel
Stephen Farrell	Baltimore Technologies
Richard Guida	Johnson & Johnson
Peter Honeyman	University of Michigan
Ken Klingenstein	University of Colorado
Neal McBurnett	Internet2
Clifford Neuman	USC
Eric Norman	University of Wisconsin
Tim Polk	NIST
Ravi Sandhu	George Mason University
Krishna Sankar	Cisco Systems
Frank Siebenlist	Argonne National Laboratory

Consumer PKI

- Alma Whitten (Why Johnny Can’t Encrypt)
- Security is weird – Not like normal s/w
  - Explore safely, undo errors, define goals (tell when done), recognize success
- Need for research in interface for security
- Important to include security tasks well in advance so time is budgeted properly

Canadian PKI

- Credential repository
- Similar to VSC
- Passes back long term credential
- Just a little scary

Random Comments

- IE
  - 34 ways to go wrong when a user gets a cert
  - Very easy to end up with passphrase-less private keys
  - Enrollments failed in > 60% of the cases
- Challenge for PGP email is: can’t change server, client or user
- After 27 years, still haven’t solved the problem of how to deal with revoked and expired keys with respect to long term documents
- Lots of interest in online repositories of various flavors
- Discussion of proof of possession of private key