Woo and Lam Pi 1

Author(s): Woo, Lam 1994
Last modified October 27, 2001

Summary: One way authentification protocol with public keys and trusted server, simplification of Woo and Lam Pi f.

Protocol specification (in common syntax)

```
A, B, S :   principal
Nb :        nonce
Kas, Kbs :  skey

1..   A  ->  B  :   A
2..   B  ->  A  :   Nb
3..   A  ->  B  :   {A,B,Nb}Kas
4..   B  ->  S  :   {A, B, {A, B, Nb}Kas}Kbs
5..   S  ->  B  :   {A, B, Nb}Kbs
```

Requirements

see Woo and Lam Pi f.

References

[WL94], [CJ97].

See also

Woo and Lam Pi f, Woo and Lam Pi 2, Woo and Lam Pi 3, Woo and Lam Pi.

Citations

[CJ97] John Clark and Jeremy Jacob. A survey of authentication protocol literature : Version 1.0., November 1997.

[WL94] T. Y. C. Woo and S. S. Lam. A lesson on authentication protocol design. *Operating Systems Review*, 1994.