CCITT X.509 (1c)

Author(s): M. Abadi and R Needham 1996
Last modified November 11, 2002

Summary: Correction of the CCITT X.509 (1) one message protocol.

Protocol specification (in common syntax)

```
A, B :     principal
Na, Nb :   nonce
Ta, Tb :   timestamp
Ya, Yb :   userdata
Xa, Xb :   userdata
PK, SK :   principal -> key (keypair)
h :        userdata -> userdata (one-way)

1.   A  ->  B  :   A, {Ta, Na, B, Xa, {Ya, {h(Ya)}SK(A)}PK(B)}SK(A)
```

Description of the protocol rules

See CCITT X.509 (1). The solution proposed in [AN96] to correct the authentication flaw in the CCITT X.509 (1) one message protocol is to sign the secret data `Ya` before it is encrypted.

Requirements

The protocol must ensure the recipient `B` of the message that the data `Xa` and `Ya` originate from `A`.

References

[AN96], [CCI87].

See also

CCITT X.509 (1), CCITT X.509 (3).

Citations

[AN96] Martín Abadi and Roger Needham. Prudent engineering practice for cryptographic protocols. *IEEE Transactions on Software Engineering*, 22(1):6–15, January 1996.

[CCI87] CCITT. The directory authentification framework. Draft Recommendation X.509, 1987. Version 7.