CCITT X.509 (1)

Author(s): CCITT 1987
Last modified November 22, 2002

Summary: One message protocol from the recommendations of the CCITT for the CCITT.X.509 standard.

Remark

This protocol presented here is actually a simplified version from [BAN89] and [AN96].

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)
```

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

Description of the protocol rules

The timestamp `Ta` and nonce `Na` are not used here.

`Xa` and `Ya` are the data transmitted, the privacy of `Ya` is ensured by its encryption with the public key of `B` and the authenticity of `Xa` and `Ya` is ensured by the encryption with the private key of `A`.

Remark

As explained in [BAN89], in the original protocol specification [CCI87], only a hash of the data is signed, for efficiency reasons. This means that the message should be specified by:

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

where `h` is a one-way function.

Requirements

The protocol must ensure the confidentiality of `Ya`: if `A` and `B` follow the protocol, then an attacker should not be able to obtain `Ya`.

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

References

[CCI87], [BAN89].

Claimed attacks

[AN96]. Failure of the authenticity of `Xa` and `Ya`.

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

See also

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

Comment sent by Michael Roe (*20/11/2002*)

The requirements section should include a confidentiality property: if `A` and `B` follow the protocol, then an attacker should not be able to obtain `Ya`.

Note of the moderator: this property has been added above, following the comment.

Comment sent by Michael Roe (*20/11/2002*)

In this protocol, private keys are used for different two operations: digital signature and message decryption. The processing done with the key is not the same in the two cases, and the difference can matter in protocol verification. The notation ought to distinguish the two operations

Citations

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

[BAN89] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. Technical Report 39, Digital Systems Research Center, february 1989.

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