with PA-ENC-TIMESTAMP pre-authentication method

Protocol Purpose

Mutual authentication

Definition Reference

-

Problems considered: 7

Attacks Found

None

Further Notes

The AS, TGS and S cache the timestamps they have received in order to prevent replays as specified in RFC 1510.

HLPSL Specification

```
role authenticationServer(
              A,C,G    : agent,
              Kca,Kag   : symmetric_key,
              SND, RCV : channel(dy),
              L        : text8((k514(|)-1(|7-2058y2251,)514(sy54(sy5y:)-514A(ic)1(_ke)1
```

```
/\ not(in(T1',L))
```