- **Kolmisuuntainen X.509-autentikointi**

  CCITT/ITU-standardi (1988-1993)

1. $A \longrightarrow B:$	$T_A, N_A, B, E_B(K_{AB})$
	$S_A(T_A, N_A, B, E_B(K_{AB}))$
2. $B \longrightarrow A:$	$T_B, N_B, A, N_A, E_A(K_{BA})$
	$S_B(T_B, N_B, A, N_A, E_A(K_{BA}))$
3. $A \longrightarrow B:$	$N_B,\ S_A(N_B)$

  - A on saanut avaimen K_{BA}.
  - Aikaleimat ja globaali kello tarpeettomia. Aikaleimat voivat saada arvon $T_A = T_B = 0$, eikä niitä tarvitse tarkistaa.
  - Sanoman 3 pitäisi osoittaa B:lle sanoman 1 tuoreus. Sanoma 2 sitoo nonssit R_A ja R_B yhteen.

Tuomas Aura TKK / Digitaalitekniikka

- **Heikkous 2**:

  Vanhan istuntoavaimen haltuunsa saanut hyökkääjä voi siirtää X.509-autentikoinnin eteenpäin (BAN89). (Aikaleimoja ei käytetä.)

$$
\begin{array}{lll}
A \longrightarrow B: & 0, N_A, B, E_B(K_{AB}), & \\
 & S_A(0, N_A, B, E_B(K_{AB})) & \\
\ldots & & \\
A \longrightarrow M: & 0, N'_A, M, E_M(K_{AM}), & (1') \\
 & S_A(0, N'_A, M, E_M(K_{AM})) & \\
M(A) \longrightarrow B: & 0, N_A, B, E_B(K_{AB}), & (1) \\
 & S_A(0, N_A, B, E_B(K_{AB})) & \\
B \longrightarrow M(A): & 0, N_B, A, N_A, E_A(K_{AB}), & (2) \\
 & S_B(0, N_B, A, N_A, E_A(K_{AB})) & \\
M \longrightarrow A: & 0, N_B, A, N'_A, E_A(K_{MA}), & (2') \\
 & S_M(0, N_B, A, N'_A, E_A(K_{MA})) & \\
A \longrightarrow M: & N_B,\ S_A(N_B) & (3') \\
M(A) \longrightarrow B: & N_B,\ S_A(N_B) & (3)
\end{array}
$$