- Korjattu X.509 (ITU 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.	$A \longrightarrow B:$	$N_B, B\ S_A(N_B, B)$

- Huom: Avaimen voi yhä kopioida istunnosta toiseen.

  Mahdollinen korjaus: lasketaan varsinaiset istuntoavaimet yksisuuntaisella funktiolla avainmateriaaleista K_{AB} ja K_{BA} sekä osapuolten nimistä.

$$K'_{AB} = HASH(A, B, K_A^+, K_B^+, K_{AB}).$$

Avaimen kontrollivektori CV

(*Key Control Vector*)

- Avaimen käyttötarkoitus:
  - kenen avain
  - kelpoisuusaika
  - salaus/avaus/allekirjoitus
  - pääavain/istuntoavain.
- Käyttötarkoitus ym. kontrollitiedot pitää liittää kiinteästi avaimeen.
  1. Luodaan avaimelle K määrämuotoinen CV ja säilytetään se aina avaimen yhteydessä.
  2. Lasketaan sormenjälki $H = h(CV, K)$.
  3. Käytetään avainta H.