Example of Principle 5

Consider the (slightly simplified) one-message version of the CCITT X.509 protocol:

Msg 1. $a \rightarrow b : a, \{t, b, x, \{y\}_{PK(b)}\}_{SK(a)}$.

The protocol is intended to ensure the integrity of x and y, and to guarantee the secrecy of y. However, b receives no guarantee that a actually knew y:

Msg 1. $A \rightarrow I_B : A, \{T, B, X, \{Y\}_{PK(B)}\}_{SK(A)}$
Msg 1′. $I \rightarrow B : I, \{T', B, X', \{Y\}_{PK(B)}\}_{SK(I)}$.

The dual of Principle 5

When a principal signs material that is subsequently encrypted, it should not be inferred that the principal intended the signed material for the principal whose key is used for the encryption.

Example of the dual of Principle 5

Consider the following protocol, which aims to authenticate a to b, and to guarantee the integrity and secrecy of the value y:

Msg 1. $a \rightarrow b : a, b, \{b, \{t, y\}_{SK(a)}\}_{PK(b)}$.

The protocol has the following attack:

Msg 1. $A \rightarrow I : A, I, \{I, \{T, Y\}_{SK(A)}\}_{PK(I)}$
Msg 1′. $I_A \rightarrow B : A, B, \{B, \{T, Y\}_{SK(A)}\}_{PK(B)}$.

Principle 6

Be clear about what properties you are assuming about nonces. What may do for ensuring temporal succession may not do for ensuring association—and perhaps association is best established by other means.