Firma digitale

Sigillo digitale che produce un legame univoco e non manipolabile tra una persona fisica e un documento elettronico (p. es. un'e-mail). Sulla base del documento da firmare viene calcolata una checksum (o somma di controllo, codice hash) secondo un determinato algoritmo. La checksum viene crittografata con la chiave di firma segreta del mittente e inviata al destinatario insieme al documento originale. Utilizzando lo stesso algoritmo questo produce un nuovo codice hash basato sul documento. Inoltre utilizzando la chiave pubblica del mittente decifra il codice hash che ha ricevuto e che è stato creato inizialmente dal mittente. Se i due codici hash corrispondono, può essere sicuro che il documento gli è giunto senza essere stato contraffatto e che il mittente è effettivamente la persona che dice di essere.