Digitale Signatur

Ist ein digitales Siegel, das einen eindeutigen und nicht manipulierbaren Zusammenhang zwischen einer natürlichen Person und einem elektronischen Dokument (z.B. E-Mail) herstellt. Aus dem zu signierenden Dokument wird nach einer bestimmten Rechenvorschrift eine Checksumme (Hashwert) berechnet. Die Checksumme wird mit dem geheimen Signaturschlüssel des Senders verschlüsselt und mit dem Originaldokument an den Empfänger gesandt. Dieser erzeugt unter Verwendung der gleichen Rechenvorschrift erneut einen Hashwert aus dem Dokument. Ausserdem entschlüsselt er mit dem öffentlichen Schlüssel des Senders den ihm zugesandten Hashwert, den der Sender zu Beginn erzeugt hat. Sind beide Hashwerte gleich, so kann er davon ausgehen, dass das Dokument unverändert bei ihm angekommen ist und der Sender tatsächlich derjenige ist, den er vorgibt zu sein.