

Eine digitale Signatur ist ein kryptografisches Verfahren, mit dem die Echtheit und Unverändertheit elektronischer Daten überprüft werden kann. Sie wird beispielsweise verwendet, um Dokumente, E-Mails oder Software digital zu unterzeichnen und sicherzustellen, dass diese nach der Signierung nicht unbemerkt verändert wurden.

Digitale Signaturen basieren auf der asymmetrischen Kryptografie. Dabei werden zwei mathematisch miteinander verbundene Schlüssel verwendet: ein privater und ein öffentlicher Schlüssel. Der private Schlüssel dient zur Erstellung der Signatur und muss geheim gehalten werden. Mit dem zugehörigen öffentlichen Schlüssel kann die Signatur anschließend überprüft werden.

Bei der Signierung wird zunächst ein sogenannter Hashwert aus den zu unterzeichnenden Daten berechnet. Dieser stellt eine Art digitalen Fingerabdruck des Dokuments dar. Aus dem Hashwert wird mithilfe des privaten Schlüssels eine digitale Signatur erzeugt. Wird das Dokument nachträglich verändert, schlägt die Überprüfung der Signatur normalerweise fehl.

Digitale Signaturen kommen unter anderem bei PDF-Dokumenten, elektronischen Verträgen, signierten E-Mails und Software-Updates zum Einsatz. Digitale Zertifikate können dabei helfen, den verwendeten öffentlichen Schlüssel einer bestimmten Person oder Organisation zuzuordnen. Die Vertrauenswürdigkeit hängt unter anderem davon ab, ob das Zertifikat gültig ist und die Identität des Schlüsselinhabers zuverlässig geprüft wurde.

Eine digitale Signatur ist nicht mit einer eingescannten handschriftlichen Unterschrift oder einem eingefügten Unterschriftsbild gleichzusetzen. Während solche Bilder lediglich eine Unterschrift darstellen, ermöglicht eine digitale Signatur eine technische Prüfung der Integrität und der Zuordnung zum verwendeten Signaturschlüssel.

In der Europäischen Union unterscheidet die eIDAS-Verordnung zwischen einfachen, fortgeschrittenen und qualifizierten elektronischen Signaturen. Die qualifizierte elektronische Signatur erfüllt besondere gesetzliche Anforderungen und hat grundsätzlich die gleiche Rechtswirkung wie eine handschriftliche Unterschrift.

Digitale Signaturen sind ein wichtiger Bestandteil der modernen IT-Sicherheit. Sie ermöglichen die zuverlässige Überprüfung elektronischer Daten und schaffen eine technische Grundlage für vertrauenswürdige digitale Geschäftsprozesse.

Weiterführende Informationen

Elektronische Signatur, Digitale Zertifikate, Asymmetrische Verschlüsselung, Hashwert, PDF, eIDAS