Sichere elektronische Verträge und Transaktionen

Sicherheit kommt nie aus der Mode. Ganz im Gegenteil: Durch die Digitalisierung fast sämtlicher Bereiche der Gesellschaft sind sichere Systeme und sichere Kommunikation elementare Grundbausteine der IT und der IT-gestützten Prozesse und somit auch im Besonderen für elektronische Verträge essenziell. Moderne technische Alternativen für Verträge bedienen sich unter anderem der Blockchain-Technologie.

Von Burkhard Stiller und Thomas Bocek

Mit der Zunahme der elektronischen Kommunikation steigt auch der Bedarf, sämtliche Arten von digitalen Daten abgesichert und zuverlässig zu transportieren. Sowohl beim elektronischen Geschäftsverkehr mit den Kunden, bei der Kommunikation mit Behörden als auch bei geschäftsinternen Abläufen ist der Schutz sensibler Daten und Dokumente zu gewährleisten. Dieses umfasst damit die Sicherstellung, dass der Absender der Daten authentisch ist und dass die verschickten Daten auf dem Weg durch das Kommunikationsnetz nicht verändert wurden und damit unverfälscht bleiben. Damit kann sowohl die Authentizität als auch die Integrität der Daten als die Grundlage aller Transaktionen und elektronischer Verträge angesehen werden, die selber möglicherweise noch zu verschlüsselnde Vertragsinhalte – also von Dritten nicht erfolgreich semantisch interpretierbar – umfassen. Obwohl die Verwendung moderner Datenkommunikationseinrichtungen hilft, geografisch verteilte und damit möglicherweise technisch unterschiedliche Randbedingungen der Kommunikationsteilnehmer zu überbrücken, sind die rechtlichen Rahmenbedingungen noch nicht auf allen Ebenen entsprechend vereinheitlicht.

Zertifikate, ein zentraler Bestandteil

Auch wenn die Entwicklung von Sicherheitstechnologien nicht mit Zertifikaten begonnen hat, so sind Zertifikate zum Nachweis von Identitäten natürlicher Personen in der IT-gestützten Kommunikation als Schnittstelle zwischen Menschen und Maschinen jedoch als zentral anzusehen. Heutzutage basiert jedes asymmetrische Verschlüsselungsverfahren auf einem geheimen Schlüssel und einem korrespondierenden öffentlichen Schlüssel. Ein Zertifikat eines registrierten Zertifizierungsdiensteanbieters kann damit belegen, dass

- der öffentliche Schlüssel und damit auch der korrespondierende geheime oder private Schlüssel genau einer natürlichen Person zugeordnet werden kann
- die Identität derjenigen Person bestätigt ist, welche dieses Schlüsselpaar vorweisen und damit auch zur Absicherung von Daten verwendet kann.

Nun ist durch den Einsatz dieses zertifizierten Schlüsselpaares nicht nur eine Verschlüsselung möglich, sondern auch das Signieren einer Nachricht oder eines Dokumentes. Damit kann durch geeignete Verfahren beim Empfänger auch die Überprüfung der Integrität der Daten sichergestellt werden.

Die elektronische Signatur entsteht, indem für das zu unterzeichnende Dokument ein Hash-Wert (Prüfsumme) erstellt, dieser mit dem geheimen Schlüssel verschlüsselt und an das zu übermittelnde Dokument oder die Nachricht angehängt wird. Bei einer elektronischen Signatur benötigt somit der Empfänger auch das Zertifikat des öffentlichen Schlüssels, mit dem der verschlüsselte Hash-Wert entschlüsselt werden kann, um als Empfänger sicherzugehen, von wem dieses Dokument übermittelt wurde. Für die Überprüfung der Signatur wird nun der entschlüsselte Hash-Wert des empfangenen Dokumentes mit dem beim Sender unabhängig berechneten Hash-Wert des an ihn übermittelten Dokumentes verglichen. Wenn dieser Vergleich erfolgreich ist – die beiden Hash-Werte sind damit identisch –, konnte die Authentizität des elektronischen Dokumentes positiv bestätigt werden.

Merkmale einer elektronischen Signatur

Eine elektronische Signatur, welche die gemäss Bundesgesetz über die elektronische Signatur (abgekürzt ZertES, 943.03) folgend definierten vier Merkmale aufweist, wird als fortgeschrittene elektronische Signatur bezeichnet. Es sind dies:

- die ausschliessliche Zuordnung zur Inhaberin oder zum Inhaber
- die Identifizierung der Inhaberin oder des Inhabers
- die Erzeugung einer Signatur mit Mitteln, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann
- die Ermöglichung der Erkennung von nachträglichen Veränderungen der Daten, auf die sie sich bezieht

Wird zusätzlich eine sichere Signaturerstellungseinheit verwendet, die vor Fälschungen von Schlüsselpaaren schützt, und werden weitere zehn vorgegebene Merkmale berücksichtigt (u.a. Seriennummer, Signaturprüfschlüssel und Namen, Niederlassungsstaat, qualifizierte

elektronische Signatur der Anbieterin von Zertifizierungsdiensten), dann ist eine qualifizierte elektronische Signatur erreicht.

Bei der Verwendung einer qualifizierten elektronischen Signatur in der Kommunikation oder dem Aufsetzen eines Vertrages sind alle Beteiligten typischerweise an einem gewünschten, gemeinsamen Zustand interessiert, der unter dem Begriff «rechtssicher» subsumiert wird, also als eine durch eine rechtlich anerkannte und massgebliche sowie als eine beweis- und revisionssichere Form definierte Handhabe. Zum Beispiel wird eine rechtssichere, elektronische Aktenführung einerseits durch das Anwenden von «Mindestanforderungen an die Aktenführung» ermöglicht, welche z.B. im Kanton St. Gallen durch den Art. 4 des Gesetzes über die Aktenführung und Archivierung vom 19. April 2011 (sGS 147.1; abgekürzt GAA) geregelt ist. Allerdings ist es zurzeit kantonal unterschiedlich, ob eine qualifizierte elektronische Unterschrift grundsätzlich als «rechtssicher» eingestuft wird oder nicht. Da der Bundesrat die Anwendung der elektronischen Signatur für juristische Personen und Behörden vereinfachen möchte, um den elektronischen Geschäftsverkehr weiter zu fördern, sind hier entsprechende gesetzliche Anpassungen und vor allen Dingen Vereinheitlichungen notwendig und vordringlich anstehend.

Da es eine Vielzahl von Zertifizierungsinstanzen im nationalen und internationalen Raum gibt, muss eine digitale Signatur von einer vertrauenswürdigen dritten Instanz (z.B. also einer Behörde) ausgestellt sein, um die Integrität, Echtheit und Authentizität des Zertifikats nachzuweisen. Damit ergibt sich zwangsläufig die Notwendigkeit einer obersten Zertifizierungsinstanz. In der Schweiz können Verwaltungseinheiten von Bund, Kantonen und Gemeinden als Anbieterinnen von Zertifizierungsdiensten anerkannt werden, ohne im Handelsregister eingetragen zu sein (ZertES). Es können aber auch natürliche oder juristische Personen sein, die eine Reihe von im ZertES definierten Bedingungen erfüllen müssen (z.B. SuisseID). In Deutschland ist nach dem deutschen Signaturgesetz (SigG) die Bundesnetzagentur die zuständige Behörde und damit mit dem Aufbau und der Überwachung einer sicheren und zuverlässigen Infrastruktur für qualifizierte elektronische Signaturen betraut. Das österreichische Signaturgesetz (SigG) sieht eine Überwachung von Zertifizierungsdiensteanbietern vor, welche sich vor der Ausübung ihrer Tätigkeit bei der für die Überwachung zuständigen Aufsicht, der Rundfunk und Telekom Regulierungs-GmbH, anmelden müssen.

Probleme elektronisch geschlossener Verträge

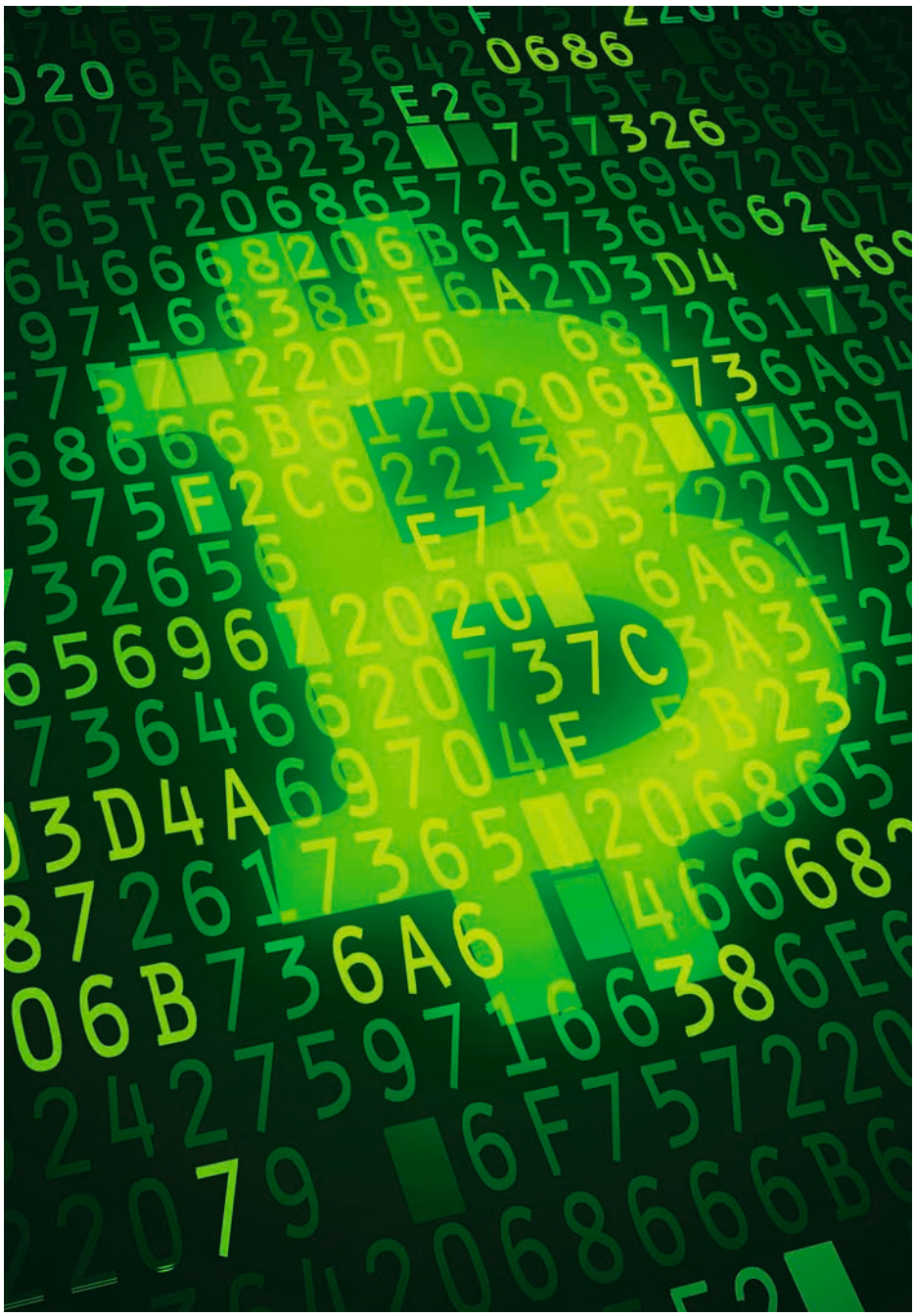
Die Verwendung von elektronischen Kommunikationsmöglichkeiten und der damit als elektronischer Schriftverkehr definierte Datenaustausch kann allerdings auch problematisch werden, wenn zum Beispiel über den Inhalt als auch den Zeitpunkt eines Vertrags bzw. des Vertragsabschlusses Unstimmigkeiten auftreten oder sich gar eine der beiden Parteien auf formelle Fehler beruft. Damit sind beim Einsatz von beispielsweise

E-Mails zum Austausch, Verhandeln und Abschliessen von Verträgen rechtssichere Dokumentationen entscheidend, um sehr viele Einzelverträge, welche in gewissen Geschäftsbereichen in kürzester Zeit abgeschlossen werden müssen, abschliessen zu können. Diese müssen u.a. den Verlauf der Verhandlungen in Form von Änderungsschritten nachträglich erkennbar und belegbar machen. Generell gilt heutzutage immer noch, dass einem elektronischen Dokument mit eingescannter Unterschrift im juristischen Ergebnis kein höherer Beweiswert zukommt als einer gewöhnlichen E-Mail.

Dem Absender einer Nachricht steht es selbstverständlich frei, vor dem Anwenden einer elektronischen Signatur den Inhalt der Nachricht, also die E-Mail oder mögliche Anhänge, hier beispielsweise des Vertragstextes im PDF-Format, noch mit einer Verschlüsselung vor dem Mitlesen Dritter zu schützen. Diese Verschlüsselung selber kann ebenso mittels eines öffentlich-privaten Schlüsselpaars geschehen oder aber durch symmetrische Methoden nach dem vorherigen Austausch eines Sitzungsschlüssels erfolgen. Die formell elektronische Signatur kann damit auf die Daten im Klartext (inhaltlich Dritten gegenüber erkennbar) wie auch auf die verschlüsselten Daten (Dritten gegenüber verborgen) gleichermassen angewendet werden.

Moderne elektronische Verträge

Nun haben sich in jüngerer Zeit technologische Alternativen herauskristallisiert, die elektronische Transaktionen für speziell definierte Abläufe sicher, rechtssicher als auch technisch effizient und gar verteilt, teilweise ohne jedwede zentrale Kontrolle, ermöglichen. Dieser Art von elektronischen Verträgen liegen sogenannte Blockchains (Blockketten) zugrunde. Diese Ketten bestehen aus einer Reihe von formatierten (Daten-)Blöcken, in denen jeweils ein Transaktionsdatum oder mehrere Transaktionsdaten zusammengefasst sind. Neue Einträge in diese Kette, das sind somit neue Blöcke, können nur in einem rechenintensiven Prozess erstellt werden, im Englischen als «Mining» bezeichnet. Diese neuen Blöcke werden anschliessend über ein Netzwerk an alle Teilnehmer verteilt, die in den gegebenen Vorgang oder die Applikation involviert sind, aber sie stehen auch allen anderen Interessierten offen.



© depositphotos

Das am weitesten verbreitete Beispiel einer öffentlichen Blockchain ist das Bitcoin-System.

Es kann grundsätzlich zwischen privaten und öffentlichen Blockchains unterschieden werden. Die privaten Blockchains sind nicht öffentlich zugänglich und müssen deshalb nicht allen Sicherheitsvorkehrungen genügen, wie dieses für öffentliche Blockchains gilt, wo jedermann Zugriff hat. Das derzeit am weitesten verbreitete Beispiel einer öffentlichen Blockchain ist das Bitcoin-System, welches eine elektronisch-kryptographische Cyber-Währung eingeführt hat, welches ferner ein Double-Spending der Bitcoins verhindert und vollständig dezentral betrieben wird. Der Vertrag in diesem Zusammenhang stellt die «implizite» Numerierung aller Transaktionen (also aller Bezahlvorgänge und damit der Austausch der Bitcoins zwischen Transaktionspartnern) in der Blockchain dar. Diese steht allen Interessenten zum Nachvollziehen von Transaktionen zur Verfügung (Beweisbarkeit), lässt allerdings keine Rückschlüsse auf die die Transaktion ausführenden Personen zu (Pseudonymität).

Technisch gesehen werden die Transaktionen innerhalb eines Blocks durch einen sogenannten Merkle-Baum paarweise miteinander «gehasht». Der letzte Hash-Wert, auch als Root-Hash bezeichnet, wird als Prüfsumme in den Header des Blocks eingetragen. Der Root-Hash

erlaubt dann im Anschluss das Verketten der Blöcke, da jeder nachfolgende Block in seinem Header den Hash-Wert des gesamten vorherigen Block-Headers enthält. Damit ist ebenfalls die Reihenfolge der Blöcke eindeutig definiert. Dieser Ansatz schliesst praktisch aus, dass nachträgliche Modifikationen vorangegangener Blöcke bzw. der in ihnen gespeicherten Transaktionen möglich sind, da die Hashes aller nachfolgenden Blöcke in typischerweise kurzer Zeit auch neu berechnet und in die Blockkette eingepasst werden müssten. Durch das sehr rechenintensive Ermitteln der Prüfsummen der Blöcke ist dieses mit realistischerweise vorhandener Hardware und Rechenleistung nicht machbar.

Speziell mit der Bitcoin-Blockchain lassen sich mit Hilfe dieser Transaktionen Bitcoins zwischen Transaktionspartnern «überweisen». Um auf diese Bitcoins zugreifen zu können, wird eine sogenannte Skriptsprache verwendet. Mit deren Funktionen kann sichergestellt werden, dass nur der Besitzer auf seine Bitcoins zugreifen kann, was heisst, dass die Befehle der Skriptsprache u.a. kryptographische Funktionen beinhalten. Auch lassen sich andere Konstrukte, wie beispielsweise P2SH (Pay-to-Script-Hash), realisieren. Allerdings sind keine generellen elektronischen Verträge aufsetzbar. Speziell in der Bitcoin-Blockchain werden die Bitcoins in Form von «Adressen» abgelegt. Da nur genau durch das vollständige Wissen dieser Adresse und der exakten Kenntnis der korrespondierenden privaten Schlüssel diese Bitcoins ausgegeben werden können, besteht ein relativ grosser Anreiz, elektronische Geldbörsen mit Bitcoin-Inhalten anzugreifen. Um diesem Trend praktikabel entgegenzuwirken, wurden Mechanismen entworfen, die das Erstellen und Speichern von Schlüsseln vollständig ohne Netzanbindung, also off-line, in einer sogenannten «cold wallet» erlauben. Aber auch P2SH-Verfahren, welche mehrere, voneinander unabhängige, private Schlüssel benötigen, um eine Transaktion auszulösen, können zur zusätzlichen Sicherheit eingesetzt werden. Diese Verfahren werden als Multi-Signatur-Verfahren (multisig) klassifiziert.

Für allgemeine elektronische Verträge, die mehr als nur eine elektronische Münze als Bestandteil einer Transaktion benötigten, wurde u.a. Ethereum entwickelt, welches eine Bitcoin-ähnliche, aber viel mächtigere Skriptsprache kennt. Diese ist Turing-vollständig und erlaubt es u.a., Nachrichten an Skripte in anderen Transaktionen zu schicken. Auch können beliebige Daten in der betreffenden Blockchain gespeichert werden.

Zukünftige Anwendungsgebiete elektronischer Verträge

Die Anwendungsgebiete für zukünftige, verteilte, elektronische Verträge sind über die Bitcoin-Blockchain und Ethereum herausgehend vielfältig. So ist es zum Beispiel möglich, eine autonome Organisation mit verteilen, elektronischen Verträgen zu erstellen, welche die notwendigen Geschäftsregeln definiert, die fortlaufend – also bei jeder Transaktion – auf ihre Einhaltung überprüft werden, beispielsweise in einem Grundbuchamt für Handänderungen. Ferner kann aber auch eine Kühlkette überwacht werden, welche die Produkttemperaturen regelmässig in einer Blockchain speichert. Damit kann der Zugriff auf diese Blockchain jedem, der Produkte dieser Kühlkette einsehen möchte – also auch einem Endkunden, zur Überprüfung der eingetragenen Transaktionen erlaubt werden. Die Herausforderung an die Blockketten – nicht nur in diesen speziell genannten Anwendungen, sondern allgemeiner formuliert – liegen u.a. noch in nicht vollständig erforschten Lösungen, welche im besonderen eine gleichzeitig effiziente, sichere und verteilt-elektronische Vertragserstellung erlauben und welche ebenso mit der in der realen Welt bestehenden Infrastruktur aus digitalen Zertifikaten und Signaturen interagieren können. ■

PROF. DR.
BURKHARD STILLER
ist Professor für Kommunikationssysteme am Institut für Informatik der Universität Zürich.

DR. THOMAS BOCEK
arbeitet in dieser Gruppe für Kommunikationssysteme als Oberassistent und Leiter des Bereichs Overlay-Netze.