

# Intergramm

Genial einfaches Verfahren zum Signieren und Verschlüsseln von  
Internet-Nachrichten

## Beschreibung des Verfahrens

### Zusammenfassung

Die **dreiteilige digitale Signatur** ist ein vollkommener Ersatz der eigenhändigen Unterschrift bei Dokumenten, die im Internet oder per Fax versendet werden. Solche als **Intergramme** bezeichneten elektronischen Mitteilungen können äußerst einfach mit einem Mausklick unterschrieben, verschlüsselt, gesendet, empfangen, entschlüsselt und geprüft werden, lassen sich auf Papier ausdrucken und wie normale Schriftsachen handhaben. Die dreiteilige digitale Signatur besteht aus drei Zahlen, zum Beispiel:

**72085 33172**

**04381 80478**

**42866 39105**

Die dreiteilige digitale Signatur weist die Echtheit eines Intergramms nach, das heißt, die Unversehrtheit des Textes und die Identität desjenigen, der unterschrieben hat. Sie entspricht einer fortgeschrittenen bzw. qualifizierten elektronischen Signatur nach der EU-Richtlinie 199/93/EG vom 13. Dezember 1999 bzw. dem deutschen Signaturgesetz vom 22. Mai 2001.

Intergramme ermöglichen vielerlei Anwendungen, beispielsweise rechtlich verbindliche einseitige Willenserklärungen oder Abschluss von Verträgen über das Internet, Internetwahlen vom heimischen PC aus.

### Einleitung

Unter den Schlagworten „virtuelles Rathaus“ und „globaler Marktplatz“ brechen Staat und Wirtschaft eine Lanze für die Verwendung der digitalen Signatur als nächsten Schritt auf dem Weg zu einer bürgerfreundlichen Verwaltung und zu erhöhter Wettbewerbsfähigkeit der Unternehmen. Die Begeisterung der angesprochenen Kundschaft für diese neue Technik hält sich bis jetzt aber noch in Grenzen. Solange der normale Bürger, Verbraucher oder ein KMU nicht wirklich davon überzeugt ist, dass die digitale Signatur ihm selbst Vorteile bringt, wird sie trotz aller Ermunterungen nicht akzeptiert werden. Was bei der herkömmlichen digitalen Signatur bisher fehlt, sind preiswerte, komfortable und vor allem transparente Lösungen.

Die neue **dreiteilige digitale Signatur** ändert diese Lage. Die neue Signatur kann bei den verschiedensten elektronischen Bürgerdiensten und geschäftlichen Transaktionen, bei denen es auf eine anwenderfreundliche

verschlüsselte Übermittlung authentischer Nachrichten (von **Intergrammen**) ankommt, genutzt werden.

### **Die herkömmliche digitale Signatur**

Als Ersatz für die eigenhändige Unterschrift eines Textes verwendet man bei Internet-Mitteilungen die digitale Signatur. Diese ist seit etwa 35 Jahren bekannt und beruht auf dem sogenannten asymmetrischen kryptographischen Verfahren mit privatem und öffentlichem Schlüssel. Der private Schlüssel muss geheim gehalten werden und ist deshalb nur mit einem Code des Eigentümers nutzbar. Er wird in verschlüsselter Form auf einer Chipkarte bereitgestellt. Deren Verwendung setzt voraus, dass der Computer des Nutzers mit einem Kartenleser ausgestattet ist. Der öffentliche Schlüssel kann als Datei der elektronischen Mitteilung beigefügt oder aus einer allgemein zugänglichen Schlüsselsammlung abgerufen werden.

Um eine herkömmliche digitale Signatur zu erzeugen, wird der Text zunächst mit einer Einwegfunktion zu einem Hashwert komprimiert. Dieser wird mit dem privaten Schlüssel und einem asymmetrischen Algorithmus zur digitalen Signatur verschlüsselt, die dem Text beigegeben wird. Zum Verifizieren der Unversehrtheit des Textes und der Echtheit seiner Unterschrift wird der Hashwert zweimal erneut berechnet: erstens aus dem Text mit der Einwegfunktion, zweitens durch Entschlüsseln der digitalen Signatur mit dem zum privaten Schlüssel gehörenden öffentlichen Schlüssel und dem asymmetrischen Algorithmus. Nur wenn beide Hashwerte übereinstimmen, ist der Text unversehrt und die Signatur echt.

Die Authentizität von Text und Signatur setzt weiter voraus, dass das verwendete asymmetrische Schlüsselpaar tatsächlich dem in der elektronischen Mitteilung benannten Inhaber gehört, und nicht etwa einem Betrüger, der den signierten Text und den öffentlichen Schlüssel unter dem Namen eines anderen in den Verkehr gebracht hat. Auch muss kontrolliert werden, ob das Schlüsselpaar noch gültig ist. Beide Forderungen werden im allgemeinen mit Hilfe eines Trustcenters erfüllt, welches die Zuordnung eines bestimmten öffentlichen Schlüssels zu einem Eigentümer und die Gültigkeit des Schlüsselpaares durch Auskünfte, Zertifikate oder Übermittlung des öffentlichen Schlüssels garantiert.

Nach dem am 22. Mai 2001 in Kraft getretenen deutschen Signaturgesetz und der zu diesem Gesetz gehörende Signaturverordnung [⊗](#) vom 16. November 2001 können digitale Signaturen eigenhändige Unterschriften rechtsgültig ersetzen. Bei etwa 3 800 Gesetzesstellen war zuvor die gesetzliche Schriftform vorgeschrieben und deshalb keine digitale Signatur möglich.

Interesse an dieser rechtlichen Anerkennung der digitalen Signatur haben vor allem Firmen, die ihre Dienste im Internet anbieten, weil sich die Beweislast zum Kunden hin verlagert. Die Akzeptanz der Verbraucher hält sich allerdings noch in Grenzen, vor allem wohl wegen der Kompliziertheit der neuen Technik:

- Bevor der Nutzer digital signierte Mitteilungen verschicken kann, muss er sich seinen öffentlichen Schlüssel von einer amtlich genehmigten Zertifizierungsstelle beglaubigen lassen, das heißt in erster Linie, ein mit der digitalen Signatur dieser Stelle versehenes Signaturschlüssel-Zertifikat

besorgen, das die Zuordnung dieses Schlüssels zu seiner Person bescheinigt.

- Beim ersten Kontakt mit einem Korrespondenzpartner muss der Nutzer diesem außer seinem mit digitaler Signatur unterschriebenen Text seinen öffentlichen Schlüssel, sein Signaturschlüssel-Zertifikat und den öffentlichen Schlüssel der Zertifizierungsstelle übermitteln, oder er muss dem Empfänger der Mitteilung angeben, wo letzterer den öffentlichen Schlüssel sicher erhält.
- Strenggenommen muss der Empfänger einer Erstmitteilung, um sicher zu sein, dass der öffentliche Schlüssel der Zertifizierungsstelle nicht gefälscht ist, bei der Regulierungsbehörde als Wurzelinstanz ein Zertifikat für den ihm angegebenen öffentlichen Schlüssel der Zertifizierungsstelle einholen.
- Wenn sein privater Schlüssel unbrauchbar wird, z.B. durch Ablauf der Gültigkeitsdauer, Verlust oder Beschädigung der Trägerchipkarte, sowie missbräuchliche Verwendung durch Dritte, muss der Nutzer im Geflecht der Sicherheitsinfrastruktur (PKI) umfangreiche Stornierungs- und Re-Initialisierungsmaßnahmen treffen.
- Insgesamt ist das Regelwerk zur Nutzung der herkömmlichen digitalen Signatur, insbesondere in der qualifizierten Form nach Signaturgesetz, derart kompliziert, dass selbst Fachleute viele Stunden brauchen, um sich mit ihm vertraut zu machen.
- Die herkömmliche digitale Signatur kann niemand in sich aufnehmen. Deshalb wird sie auch meistens nicht auf dem Bildschirm gezeigt oder mit dem Text zusammen ausgedruckt.

Kosten und komplizierte Technik sind nicht die einzigen Akzeptanzhürden: Hinzu kommt die Vielfalt von Kreditkarten und anderen Karten, die von den Kartenherausgebern häufig als Trägermedium für den privaten Schlüssel empfohlen werden, sowie deren Bestreben, immer mehr Funktionen auf derselben Karte unterzubringen, was die Anwendung nicht erleichtert.

### Die dreiteilige digitale Signatur

Über eine Alternative zur herkömmlichen digitalen Signatur wurde erstmals in der Zeitschrift COMPUTER UND RECHT, Ausgabe 6/2000, S. 411/412 berichtet. Diese Signatur besteht aus drei einfachen Zahlen, beispielsweise:

72085 33172  
04381 80478  
42866 39105


Die **dreiteilige Signatur** ist leicht wahrnehmbar, so dass es sich lohnt, sie mit dem Text auf Papier auszudrucken und hat auch andere Vorzüge. Die Bedeutung ihrer drei Teile ist leicht zu verstehen:

- **erste Zahl (Unterzeichnerkennung K): wer hat den Text erzeugt?** Kennzeichnet die Identität des Unterzeichners und ist für verschiedene Personen immer unterschiedlich. Berechnet sich aus den persönlichen Daten des Unterzeichners wie Name, Geburtstag, Geburtsort, oder wird als Zufallszahl erzeugt.

- **zweite Zahl (Textsiegel S): um welchen Text handelt es sich?** Kennzeichnet die Identität eines Textes und ist für verschiedene Texte immer unterschiedlich. Berechnet sich mit einem öffentlichen Einwegalgorithmus als Hashwert aus allen Schriftzeichen des Textes und ihrer Anordnung.
- **letzte Zahl (Unterschriftsbeweis U): wurde der Text wirklich vom Unterzeichner genehmigt?** Kennzeichnet die Tatsache, dass der Unterzeichner den Text aktiv gebilligt hat und ist für verschiedene Texte und für verschiedene Unterzeichner auch bei gleichem Text immer unterschiedlich. Berechnet sich als Hashwert aus dem Textsiegel S mit einem geheimen (privaten) Einwegalgorithmus, der vorzugsweise durch eine **Geheimzahl G** definiert ist, unter alleiniger Kontrolle des Unterzeichners.

Die Software zum Betrieb des Verfahrens mit der dreiteiligen digitalen Signatur besteht aus drei komplementären Teilen: einem Teil für die PCs der Nutzer (**Client**), einem zweiten Teil für den PC einer vertrauenswürdigen Instanz (**Instance**) (eines Zertifizierungsdiensteanbieters nach Artikel 2, Ziffer 11 der EU-Richtlinie 1999/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen), einem dritten Teil für ein autonomes Modul in Form eines gegen äußere Einflüsse und Wahrnehmungen abgeschirmten Internetservers (**Server**). Dies Modul entspricht funktionell einer sicheren Signaturprüfeinheit nach Artikel 2, Ziffer 8 der EU-Richtlinie. Es enthält eine geheime Datenbank zur verschlüsselten Speicherung der Wertepaare K-G aller Nutzer.

Bei der Initialisierung prüft die vertrauenswürdige Instanz zunächst die Identität eines neuen Nutzers. Dann werden vom System unter der Aufsicht der Instanz und bei Einhaltung der nötigen Sicherheitsvorkehrungen für den neuen Nutzer K- und G-Werte erzeugt, ohne dass die Instanz diese Werte erfährt. Hierbei wird das Wertepaar K-G in die Datenbank aufgenommen. Im gleichen Zug wird für den Nutzer ein zunächst noch nicht initialisiertes **Signierwerkzeug (USB-Stick, 3,5“-Diskette, oder Chipkarte)** hergestellt, das den G-Wert in verschlüsselter Form enthält, so dass der Nutzer ihn nicht erfährt. Der K-Wert wird unverschlüsselt gespeichert. Der neue Nutzer erhält zusätzlich einen Code, mit dem er daheim auf seinem PC nach Installation der Nutzersoftware sein Signier-Werkzeugs initialisieren kann.

Um die dreiteilige digitale Signatur zu erzeugen, schreibt der Nutzer zunächst seinen Text, legt sein Signier-Werkzeug ein (USB-Anschluss, Diskettenlaufwerk oder Chipkartenleser), und authentisiert sich durch Zusammenfügen einiger persönlicher Assoziationen (entsprechend dem patentrechtlich geschützten Authentisierverfahren **bio-ident** )<sup>⊗</sup>), wodurch seine Geheimzahl G verfügbar wird. Durch einen Mausklick wird der Text mit einer in der Client-Software enthaltenen Einwegfunktion zum Textsiegel S komprimiert. Dieses wird mit dem durch die Geheimzahl G definierten Einwegalgorithmus zum Unterschriftsbeweis U umgeformt. Die somit erzeugte dreiteilige digitale Signatur [K S U] wird dem Text beigegeben.

Jeder, der einen mit dieser Signatur unterschriebenen Text (ein Intergramm) zu Gesicht bekommt, sei es auf dem Bildschirm, oder auch als Papierdokument,

hat die Möglichkeit, sich von dessen Unversehrtheit und der Authentizität des Unterzeichners zu überzeugen, und zwar folgendermaßen: Wenn das Intergramm auf Papier geschrieben ist, wird der Text zunächst mit einem Scanner in den PC eingelesen und mit einem OCR-Programm in eine Textdatei umgewandelt. Die Verifizierung läuft wie folgt ab: Zunächst wird das Textsiegel S mit der Nutzersoftware aus dem Text neu berechnet und mit dem Pendant in der dreiteiligen digitalen Signatur [K S U] verglichen. Danach wird die Signatur über das Internet oder auch in anderer Weise zum Modul (Server) gesendet. Innerhalb des Moduls gibt die Server-Software automatisch und von außen her unausspähbar die Kennung K in die Datenbank ein, stellt die Geheimzahl G bereit errechnet mit ihr den Unterschriftsbeweis U aus dem Textsiegel S neu und vergleicht diesen U-Wert mit demjenigen in der Signatur [K S U]. Nur das Ergebnis dieser Überprüfung: „Signatur gültig“ oder „Signatur ungültig“ gelangt nach draußen. Sicherheitshalber können, falls einmal ein Modul ausfallen sollte, separat erreichbare Modul-Duplikate zur Verfügung stehen.

In der Abbildung 1 ist das Verfahren zur Erzeugung und Überprüfung von Intergrammen mit der dreiteiligen digitalen Signatur schematisch dargestellt.

Die dreiteilige Signatur kann bei Dokumenten angewendet werden, die konventionell, per Fax oder elektronisch übermittelt oder einfach nur dauerhaft aufbewahrt werden sollen. Mit dieser Signatur versehene papiergebundene Dokumente können wie die bisher eigenhändig unterzeichneten Schriftstücke gehandhabt und abgelegt werden, erfordern also keine zweigleisige Aktenverwaltung, nämlich eine elektronische und eine konventionelle. Texte, die verschlüsselt, also als Intergramm, zu übermitteln oder einfach nur aufzubewahren sind, werden mit der Geheimzahl G unter Verwendung eines dem Verfahren eigenen symmetrischen Kryptoalgorithmus ver- und entschlüsselt. Intergramme durchlaufen das Modul und werden dort von der Modulsoftware in der Weise umgeschlüsselt, dass nur die Client-Software des Empfängers sie entschlüsseln kann.

Das 'Intergramm'-Verfahren läuft seit Jahren problemlos im Internet. Interessenten können sich nach ihrer Anmeldung beim Intergramm-Administrator sehr einfach ein Signier-Werkzeug herstellen lassen. Wer will, kann seine Intergramme statt über das Internet natürlich auch als normales e-Mail, als Fax oder als Papierdokument verschicken, allerdings nur unverschlüsselt.

Intergramme bieten sich wegen ihrer Einfachheit und Kostenvorteile für die verschiedensten elektronischen Transaktionen und Bürgerdienste an. Im virtuellen Rathaus, also im Verkehr zwischen einem zentralen Online-Dienstleister und dessen Kunden, lassen sich Intergramme beispielsweise nach folgendem Schema nutzen: Der Online-Dienst als vertrauenswürdige Instanz prüft zunächst die Personalien des Kunden und stellt dann für ihn mit der Instanzsoftware ein Signier-Werkzeug her. Die Nutzersoftware überspielt sich der Kunde beim Online-Dienst auf einen Datenträger oder er lädt sie sich daheim aus dem Internet auf seinen PC herunter. Mit dem Signier-Werkzeug unterschreibt der Kunde nach seiner Authentisierung am heimischen PC mit einem Mausklick seine Intergramme und sendet sie mit einem weiteren Mausklick - automatisch verschlüsselt - über das Internet an den zuständigen Sachbearbeiter des Online-Dienstes. Der Sachbearbeiter besitzt ebenfalls ein

personalisiertes Signier-Werkzeug und auf seinem PC die Nutzersoftware. Nach seiner Authentisierung entschlüsselt er mit einem Mausklick die eingehenden Intergramme und überprüft mit einem zweiten Mausklick deren Signatur. Die Kommunikation in entgegengesetzter Richtung, also vom Online-Dienst zum Kunden, erfolgt in analoger Weise.

### **Vorteile von Intergrammen**

Das Intergramm-Verfahren mit der dreiteiligen digitalen Signatur hat folgende Vorzüge:

- Die Signatur ist nach Umfang und Funktion ein vollkommenes Äquivalent der eigenhändigen Unterschrift auf einem Papierdokument.
- Sie ist - im Gegensatz zur herkömmlichen digitalen Signatur - leicht zu lesen und ohne weiteres mit dem Text ausdrückbar.
- Das für die Verwendung herkömmlicher digitaler Signaturen erforderliche komplizierte Schlüssel- und Zertifikatsmanagement entfällt.
- Der Nutzer braucht sich keine teuren Chipkartenleser anzuschaffen, ein preiswerter USB-Stick oder ein Diskettenlaufwerk reicht zum Authentisieren aus.
- Das Signier-Werkzeug erfordert keine schwer zu behaltenden PINs oder Passwörter.

Weitere Vorzüge von Intergrammen:

- Sie kommen praktisch in Echtzeit beim Empfänger an, weil sie nicht wie Emails über die Server verschiedener Provider laufen.
- Sie gestatten einen vom Email-System vollkommen unabhängigen Nachrichtenaustausch.
- Unverschlüsselt können sie auch als normales Email, als Fax oder als Papierdokument verschickt werden.
- Sie können ausgedruckt wie eigenhändig unterzeichneten Schriftstücke gehandhabt, registriert und archiviert werden, erfordern also keinen zweigleisigen Verwaltungsablauf.

Für Online-Dienstleister hat die Verwendung von Intergrammen zusätzliche Vorteile:

- Weil der Online-Dienst selbst die Identität des Nutzers prüft, selbst dessen individuelles Signier-Werkzeug herstellen kann, um sie ihm persönlich auszuhändigen, ist er von keinem externen Trustcenter abhängig und behält die volle Zugangskontrolle.
- Bei eventuellem Missbrauch des Online-Dienstes oder Zweifel an der Authentizität eines Nutzers kann die Zugangsberechtigung sofort und ohne umständliche Prozeduren gesperrt werden.

## Anwendungen von Intergrammen

**Virtuell abgeschlossener notarieller Kaufvertrag** (Abbildung 2): Nach Einverständnis unter den Parteien wird der endgültige Vertragstext beim Notar geschrieben. Dieser authentisiert sich mit seinem Signier-Werkzeug, unterschreibt das Dokument mit Mausklick und schickt es mit einem weiteren Mausklick verschlüsselt über das Internet an den Verkäufer (Kennung 93689 68378). Der Verkäufer authentisiert sich an seinem PC mit seinem Signier-Werkzeug, lädt sich das vom Notar unterschriebene Dokument auf seinen Bildschirm, fügt einen Genehmigungsvermerk bei, unterschreibt das Ganze mit einem Mausklick und schickt das Dokument in dieser Form mit einem weiteren Mausklick verschlüsselt über das Internet weiter an den Käufer (Kennung 97116 96336). Der Käufer authentisiert sich an seinem PC mit seinem Signier-Werkzeug, lädt sich das vom Verkäufer erhaltene zweifach unterschriebene Dokument auf seinen Bildschirm, fügt einen Genehmigungsvermerk bei, unterschreibt das Ganze mit einem Mausklick und schickt das Dokument in dieser Form mit einem weiteren Mausklick verschlüsselt über das Internet weiter an den Notar (Kennung 80679 96609). Der Notar authentisiert sich an seinem PC mit seinem Signier-Werkzeug, lädt sich das vom Käufer erhaltene dreifach unterschriebene Dokument auf seinen Bildschirm, druckt den hiermit rechtskräftig zustande gekommenen Kaufvertrag auf Papier aus und legt das fertige Dokument in sein Archiv. Des weiteren übermittelt er dem Verkäufer und dem Käufer elektronische Kopien, die von diesen auf Papier ausgedruckt werden können.


**Online-Einzugsermächtigung** (Abbildung 3): Der Kunde authentisiert sich mit seinem Signier-Werkzeug und gibt an seinem PC die Daten in das Formular ein. Mit einem Mausklick errechnet sich die digitale Signatur aus dem eingegebenen Text und wird in den letzten drei Zeilen vermerkt. Durch Anklicken eines Menuefelds „Absenden“ wird das Formular verschlüsselt und per Internet an den zuständigen Sachbearbeiter des Unternehmens übermittelt. Dieser öffnet das Formular auf seinem PC, nachdem er sich mit seinem personalisierten Signier-Werkzeug authentisiert hat und überprüft mit einem Mausklick die Authentizität der Ermächtigung. Bei positivem Ergebnis bearbeitet der Sachbearbeiter den Vorgang und legt das ausgedruckte Formular wie eine eigenhändig unterschriebene Einzugsermächtigung ab.

**Überweisung von Geldbeträgen** (Abbildung 4): Das in das System einbezogene Kreditinstitut eröffnet für jeden Kunden unter dessen Kennung K ein Konto. Eine Überweisung verläuft folgendermaßen: Der Auftraggeber authentisiert sich mit seinem Signier-Werkzeug, füllt am PC die Zeilen 01 bis 05 des Formulars aus und klickt auf seine Maustaste. Die digitale Signatur wird aus dem eingegebenen Text errechnet und in den Zeilen 06 bis 08 vermerkt (Signatur 1). Das dermaßen vervollständigte Formular wird per Mausklick verschlüsselt über das Internet an das Kreditinstitut gesandt, nachdem dessen Bezeichnung und Kennung 7302561807 in die Zeilen 9 und 10 eingetragen wurde.

Wenn das Konto des Kunden gedeckt ist und die Signatur 1 vom Kreditinstitut durch Kontakt mit dem Modul verifiziert wurde, wird der im Formular angegebene Betrag auf das Konto 7305251704 des Empfängers gebucht und ein Bestätigungsvermerk des Kreditinstituts in die Zeile 11 des Formulars

eingetragen. Nachdem sich der Sachbearbeiter mit seinem Signier-Werkzeug authentisiert hat, wird dessen digitale Signatur mit einem Mausklick aus dem gesamten eingegebenen Text errechnet und in den Zeilen 12 bis 14 vermerkt (Signatur 2). Das dermaßen vervollständigte Formular wird per Mausklick verschlüsselt über das Internet dem Empfänger übermittelt, der sofort über die Gutschrift verfügen kann.

Hat der Empfänger noch kein Konto unter einer Kennung beim systemtragenden Kreditinstitut eingerichtet, so bietet letzteres ihm eine Neueröffnung an und schreibt ihm danach den angewiesenen Betrag gut. Verzichtet der Empfänger hierauf, so überweist ihm das Kreditinstitut sein Guthaben auf konventionellem Weg auf ein von ihm zu benennendes Konto.

**Internetwahlen** (Abbildung 5): Abweichend von den anderen Intergramm-Anwendungen, bei denen es darauf ankommt, die **Identität** des Nutzers durch die dreiteilige elektronische Signatur nachzuweisen, behält beim **i-voting**  der Eigentümer des Signier-Werkzeuges, also der Wähler, seine Unterzeichnerkennung K für sich, damit die Stimmabgabe **anonym** bleibt.

Die elektronische Stimmabgabe verläuft folgendermaßen: Der Wähler holt sich vor der Wahl sein Signier-Werkzeug bei der Wahlbehörde ab, nachdem er sich dort ausgewiesen hat und festgestellt wurde, dass er im Wählerverzeichnis aufgeführt ist. Bei dieser Gelegenheit kann er sich auch die Nutzersoftware und den Stimmzettel als elektronische Datei auf einen Datenträger überspielen, wenn er nicht bevorzugt, sich Software und Stimmzettel aus dem Internet herunterzuladen.

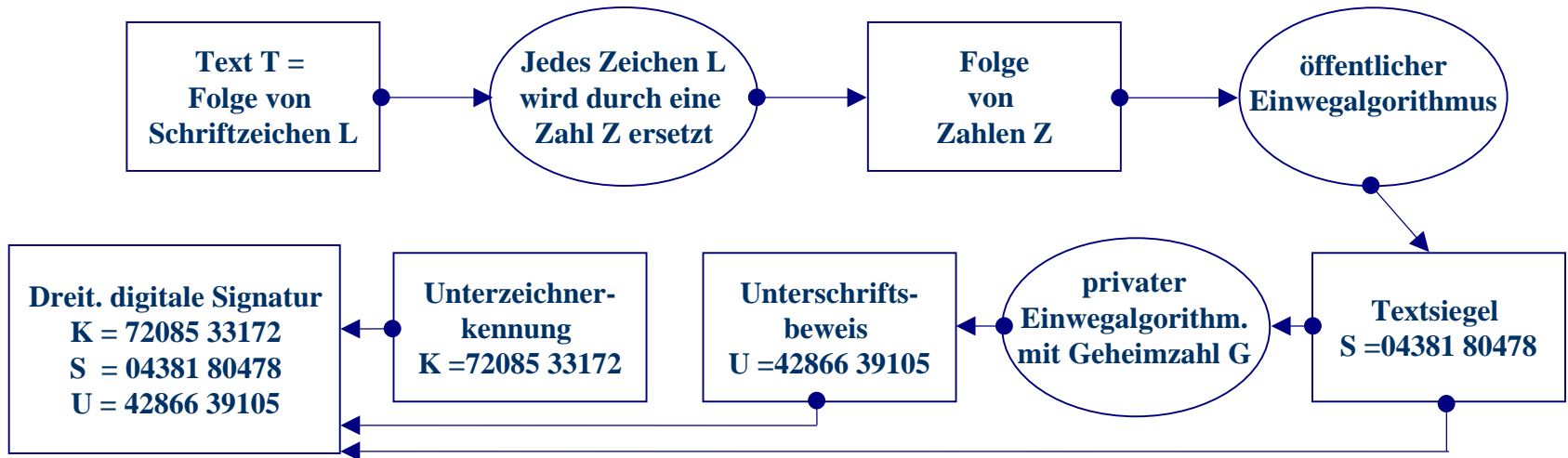
Am Wahltag kreuzt der Wähler am PC-Bildschirm seinen Kandidaten an, nachdem er sein Signier-Werkzeug in den PC eingelegt hat, unterzeichnet durch Mausklick den ausgefüllten Stimmzettel und sendet diesen durch einen weiteren Mausklick verschlüsselt per Internet an die elektronische Stimmzettelbox des Wahlamts. Nach Wahlende führt der Wahlleiter sein personalisiertes Signier-Werkzeug in den PC des Wahlamts ein, authentisiert sich, wodurch die verschlüsselten elektronischen Stimmzettel aus der Stimmzettelbox auf den PC des Wahlamts heruntergeladen und entschlüsselt werden. Durch Mausklick wird die Signatur jedes Stimmzettels verifiziert.

## Abbildungen 1 bis 5

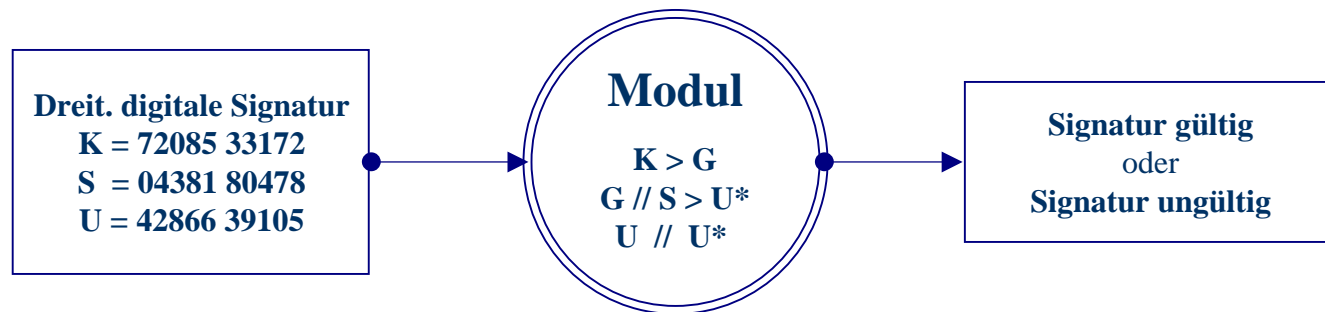


# Abbildung 1: Dreiteilige digitale Signatur

## Erzeugung



## Überprüfung



## **Abbildung 2**

**{{ Mail von: Notar, Datum: 15.08.2011 15:29, Mailname: Urkunde }}**

**{{ Mail von: Moritz Krause, Datum: 15.08.2011 15:33, Mailname: Urkunde }}**

**{{ Mail von: Max Müller, Datum: 15.08.2011 15:41, Mailname: Urkunde }}**

**URKUNDE  
DES NOTARS  
SIEGFRIED NEUBURGER  
BAD AIBLING  
Urkundenrolle Nr. A 1756  
Jahrgang 2011**

**Vertrag über GmbH-Verkauf**

**Heute, den fünfzehnten August zweitausendundelf (15. August 2011) erscheinen**

**virtuell vor mir, Siegfried Neuburger Notar in Bad Aibling, mit den  
Amträumen in Bad Aibling, Frühlingstrasse 111:**

**erstens: Herr Moritz Krause, geboren am 11. November 1966, 87654  
Waldkirchen, Lindenstraße 1, nach Angabe in gesetzlichem Güterstand lebend,  
im folgenden Verkäufer genannt;**

**zweitens: Herr Max Müller, geboren am 12. April 1975, 76543 Feldkirchen,  
Erlenstraße 44, ledig, im folgenden Käufer genannt.**

**Über die Personenechtheit verschaffte ich mir Gewissheit durch elektronische  
Einsichtnahme in das Register der Bundesnotarkammer.**

**Auf Ansuchen der Erschienenen beurkunde ich:**

**Der Verkäufer überträgt mit Wirkung zum 1. September 2011 an den Käufer  
seine gesamten Anteile in Höhe von 20 % an der ABC-GmbH in 83055  
Rosenheim, Bahnhofsstraße 6, eingetragen beim Amtsgericht Traunstein, Rolle  
B 4456.**

**Der Käufer zahlt spätestens am 31. August 2011 an den Verkäufer den Betrag  
von € 500.000,00 (fünfhunderttausend Euro).**

**Die Kosten dieses Vertrages tragen die beiden Erschienenen zu gleichen Teilen.**

**Der Notar hat die Erschienenen per Intergramm über die Tragweite dieses  
Vertrages belehrt.**

**Diese Urkunde wurde vom Notar am 15. August 2011 wie unten 1 elektronisch unterschrieben und an den Verkäufer elektronisch weitergeleitet:**

**Diese Urkunde nebst Unterschrift des Notars wurde vom Verkäufer am 15. August 2011 genehmigt, wie unten 2 unterschrieben und an den Käufer elektronisch weitergeleitet:**

**Diese Urkunde nebst Unterschrift des Notars sowie Genehmigungsvermerk und Unterschrift des Verkäufers wurde vom Käufer am 15. August 2011 genehmigt, wie unten 3 unterschrieben und an den Notar elektronisch zurückgeschickt:**

**IMPRESSUM[  
77272724  
4895330729  
6841380133}**

**IMPRESSUM[  
86800966  
2437937725  
3580986880}**

**IMPRESSUM{  
57640874  
0048157285  
5919868413}**

## Abbildung 3: Einzugsermächtigung

Hiermit ermächtigen Sie uns widerruflich, die zu zahlenden Beträge bei Fälligkeit zu Lasten Ihres Kontos durch Lastschrift einzuziehen													
Gültig ab	1	5	-	1	2	-	2	0	0	5			
Kundennummer	9	8	7	6	3	5	4	7					
Verbrauchsstelle	K	7	/	8	2	3							
Name	M	u	s	t	e	r	m	a	n	n			
Vorname	M	a	n	f	r	e	d						
Straße/Haus Nr.	L	i	n	d	e	n	s	t	r	.	6	7	
Postleitzahl	0	2	6	2	7								
Ort	J	a	u	e	r	n	i	c	k				
Telefon-Nr.	0	5	6	3	2	-	5	3	4	3	3	3	
Name der Bank	S	o	n	n	e	n	b	a	n	k			
Bankleitzahl	9	2	3	7	4	5	0	0					
Kontonummer	4	4	7	5	3	2	-	5	4				
Sonstige Mitteilungen	G	ü	l	t	i	g		b	i	s			
	3	1	-	1	2	-	2	0	0	7			
Digitale Signatur	5	5	2	5	9	0	1	4	8	8			
	8	3	4	3	7	0	6	3	2	5			
	4	2	6	0	2	6	3	7	3	4			

# Abbildung 4: Formular für elektronische Überweisung

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25		
	Empfänger																										
01	P	L	U	T	A	-	G	M	B	H																	01
	Kennung																										
02	7	3	0	5	2	5	1	7	0	4																	02
	Währung												Betrag														
03	E	U	R																								03
	Ausstellungsdatum												Uhrzeit														
04	1	4	-	0	9	-	2	0	0	5																	04
	Auftraggeber																										
05	H	.	H	a	n	n	e	m	a	n	n																05
	Signatur des Auftraggebers (Signatur 1)																										
06	K	=	3	7	5	3	1	0	8	4	0	1															06
07	S	=	8	3	0	2	7	1	1	8	4	9															07
08	U	=	1	6	0	4	7	3	2	6	9	9															08
	Kreditinstitut																										
09	F	i	n	a	n	z	b	a	n	k																	09
	Kennung																										
10	7	3	0	2	5	6	1	8	0	7																	10
	Bestätigungsdatum des Kreditinstituts												Uhrzeit														
11	1	4	-	0	9	-	2	0	0	5																	11
	Signatur des Kreditinstituts (Signatur 2)																										
12	K	=	7	3	0	2	5	6	1	8	0	7															12
13	S	=	0	3	8	5	8	2	9	4	2	7															13
14	U	=	5	8	2	0	0	2	8	4	8	3															14
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25		

**Abbildung 5**  
**Signierter Stimmzettel für Internetwahlen**  
**(i-voting)**

<b>ABRAHAM Max</b>	<input type="radio"/>
<b>BECKER Günter</b>	<input type="radio"/>
<b>CAESAR Heinz</b>	<input type="radio"/>
<b>DREIER Helmut</b>	<input type="radio"/>
<b>EBERHARD Oskar</b>	<input type="radio"/>
<b>FOCKER Adalbert</b>	<input type="radio"/>
<b>GREINER Bernhard</b>	<input type="radio"/>
<b>HOLZHAUER Daniel</b>	<input checked="" type="radio"/>
<b>ISENACKER Quirin</b>	<input type="radio"/>
<b>JELAFFKE Ulrich</b>	<input type="radio"/>
<b>KOLBENHAUER Kurt</b>	<input type="radio"/>
<b>LEIMENER Bartel</b>	<input type="radio"/>

72085 33172  
04381 80478  
42866 39105