Erweiterte digitale Signatur

Beschreibung des Verfahrens

Der Informationsaustausch über digitale Netze (Intranet, Internet) ist grundsätzlich unsicher (Integritätsproblem, Authentizitätsproblem). Eine Lösung bietet hier die elektronische Signatur. Entsprechend der datentechnischen Gestaltung werden unterschieden:

1) einfache elektrische Signatur,
2) fortgeschrittene elektronische Signatur und
3) qualifizierte elektronische Signatur.

Einfache und fortgeschrittene elektronische Signaturen sind rechtlich **nicht geregelt**. Für qualifizierte elektronische Signaturen schreibt das Signaturgesetz vom 16.05.2001 [SigG, BGBl.I S.876] feste Verfahrensschritte und Schlüsseltechniken vor. Die Funktionsweise ist recht kompliziert, aber im Hinblick auf die rechtliche Wirkung als **eigenhändige Unterschrift** mit Sicherheit gleichwohl erforderlich. In rechtlich weniger bedeutsamen Fällen - aber dennoch mit **vertretbarer Sicherheit** - bietet sich folgendes Verfahren als digitale Signatur an:

CypherMatrix® als erweiterte digitale Signatur

Nach bisheriger Meinung "*könne die einfache elektronische Signatur nicht zweifelsfrei einer Person zugeordnet werden. Sie erfülle auch keine besonderen Sicherheitsanforderungen und habe daher wenig Beweiswert*". Diese Einschränkungen sind allerdings in dem hier vorgestellten Verfahren **nicht** gegeben. Generierung und Verifizierung der Signatur erfolgen auf Basis des **CypherMatrix** Verfahrens mit dem Hashwert des Dokuments (Nachricht, Datei) und dem Hashwert der persönlichen Daten des Signierenden, seinem digitalen Passbild und seiner digitalisierten Unterschrift.

Das Verfahren teilt digitale Zeichenfolgen (Dateien, digitale Nachrichten, Programme, "e-mail"-Kommunikation, Domain-Content, Identifikationsdaten sowie private und öffentliche Schlüssel) in **Blöcke** fester Länge (z.B: 42, **64**, 72, 128 Bytes). Jeder Block wird als Eingangs-Sequenz einer **kollisionsfreien** Einweg-HashFunktion unterworfen. Eine ausführliche Beschreibung finden Sie im Internet unter:

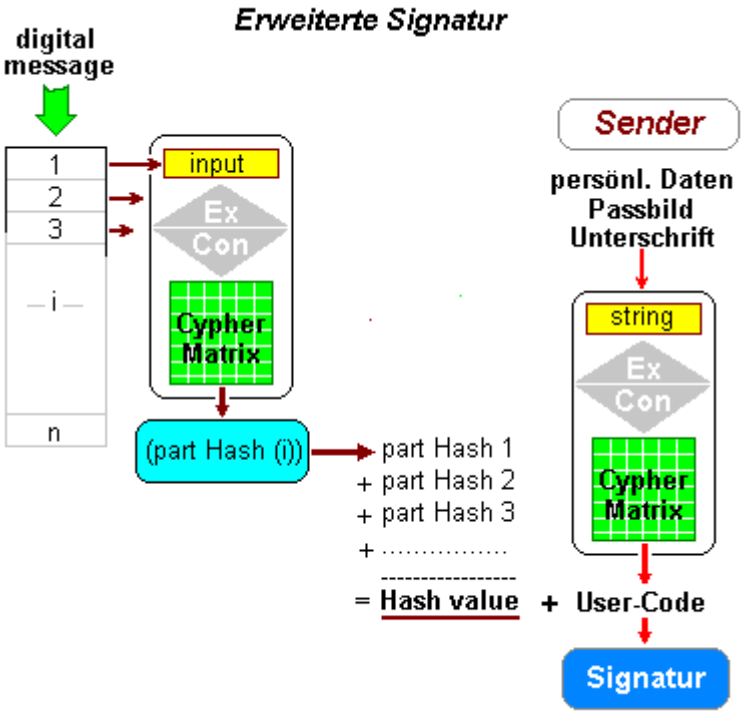
CypherMatrix Hashverfahren
Basisfunktion

Der **Hashwert** stellt eine eindeutige Abbildung der Eingangs-Sequenz in Form einer Zahl dar. Mit den Hashwerten kann gerechnet werden (addieren, subtrahieren, multiplizieren, dividieren und MODULO rechnen). Die Hash-Werte der einzelnen Blöcke addieren sich zu einem **finalen Hashwert** für die gesamte digitale Zeichenfolge (Datei).

Um einen relativ kurzen Wert zu erhalten, wird die Summe der dezimalen Hash-Werte im Zahlensystem zur Basis 62 ausgewiesen. Die Werte können auch jederzeit in äquivalente Zahlen anderer Zahlensysteme (z.B. Basis 59, 65, 77) umgeformt werden.

Generierung der "Signatur"

Die folgende Skizze zeigt die Zusammenhänge:



Zur persönlichen Zuordnung einer digitalen Information (Nachricht, Datei, e-mail) werden der Hashwert der **persönlichen Daten** des Senders (Signatar) und der Hashwert der zu **signierenden Information** addiert und zu einem gemeinsamen digitalen Wert zusammengefasst.

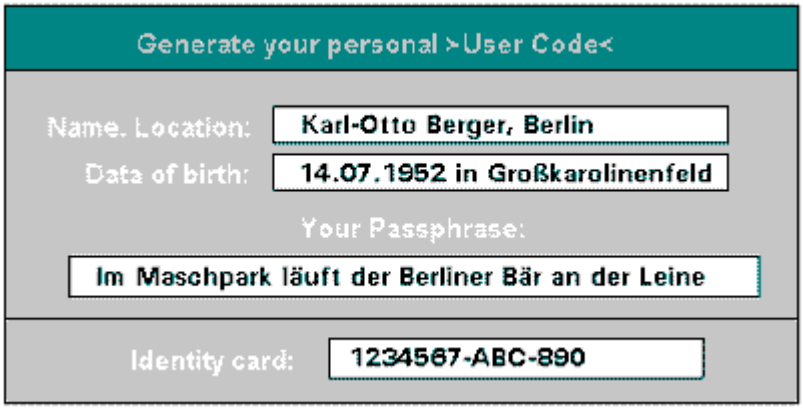
Identifikations-Daten als Hashwert

Die persönlichen Daten (**Identifikationsdaten: ID**) des Senders werden bereits bei der Installation des Programms erfasst und mit der Hashfunktion des Programms sein **User-Code** errechnet, der dann die Basis für künftige Verfahrensschritte liefert. Zum Beispiel:

1. Persönliche Angaben

Als persönliche Daten sind der Name des Anwenders, sein Wohnort sowie die Daten seiner Geburt (Datum und Geburtsort), eine persönliche **Passphrase** mit bis zu 48 Zeichen und die Daten seines Personalausweises oder Reisepasses einzugeben. Aus diesen Daten generiert das Verfahren den **User-Code** des Senders. Dazu folgendes Beispiel:

(alle Namen und Daten sind frei erfunden)



	Basis 62	hexadezimal	dezimal
Hashwert **Identifikationsdaten:**	lkg0kXRaC	250AB965D49588	1 042 635 531 952 520

Als **Passphrase** dienen am Besten unsinnige, zusammenhanglose, widersprüchliche und von anderen Personen möglichst nicht nachvollziehbare Textpassagen (von mindesten 36 und höchstens 48 Byte Länge) , wie zum Beispiel:

Heidschnucken suchen jeden Tag Weinbergschnecken
Der Kater „Rosso“ schläft immer in der Vogelkoje
Hucleberry Finn in concert on blue Spice Islands

Die **Passphrase** können Sie nach der Eingabe sofort wieder vergessen. Sie wird nur als Schlüssel zur sicheren Referenzverbindung zwischen Anwender und Portalbetreiber benötigt und später nie wieder verwendet. Bildlich gesprochen wird der Sicherungskasten „Referenzverbindung“ mit der Passphrase abgeschlossen und der Schlüssel anschließend in die Spree geworfen. Niemand soll ihn dann weder suchen noch finden.

2. Passphoto des Anwenders (jpg, gif):

Eine visuelle Zuordnung zum Sender erreicht das Verfahren durch eine Digitalisierung des Passphotos (jpg, gif) des Anwenders und Einbindung in den User-Code:

	Basis 62	hexadezimal	dezimal
Hashwert **Passphoto:**	tKf9oZAGz	2AEC09CF764F6D	12 081 475 901 345 645

3. Eingescannte Unterschrift des Anwenders (jpg, gif):

Eine Verifizierung des Anwenders fast wie auf herkömmlichen Unterlagen (Quittung, Vertrag) wird erreicht durch eine Digitalisierung seiner persönlichen Unterschrift – möglichst vor einem Notar. Die digitale Unterschrift wird in den User-Code einbezogen:

	Basis 62	hexadezimal	dezimal
Hashwert **Unterschrift:**	okBUT9kMJ	275CE291B38EA7	11 079 652 268 543 655

Die Hashwerte der Identifikationsdaten, Passphoto und Unterschrift werden zum **User-Code** addiert, der sowohl beim Anwender als auch in der Internet-Datenbank gespeichert wird.

	Basis 62	hexadezimal	dezimal
Identifikationsdaten:	lkg0kXRaC	250AB965D49588	10 426 365 531 952 520
Passphoto:	tKf9oZAGz	2AEC09CF764F6D	12 081 475 901 345 645
Unterschrift:	okBUT9kMJ	275CE291B38EA7	11 079 652 268 543 655
User-Code:	2TpWf2GMDU	7753A5C6FE739C	33 587 493 701 841 820

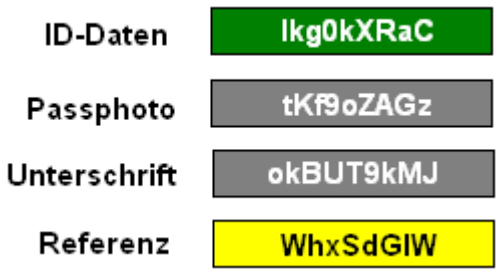
Um das Verfahren sicher und vertrauenswürdig zu gestalten, können Passphoto und persönliche Unterschrift des Anwenders vor einem Notar vollzogen und dem Betreiber des Portals vorgelegt werden, bevor die digitale Verbindung freigeschaltet wird.

Um für den Datentransfer zwischen Anwender und der Internet-Datenbank eine sichere Basis zu schaffen, wird der User-Code in eine User-Referenz umgewandelt. Dieser Vorgang stellt eine Einweg-Hashfunktion dar, die von Dritten nicht nachvollzogen werden kann.

	Basis 62	hexadezimal	dezimal
User-Code	2TpWf2GMDU	7753A5C6FE739C	33 587 493 701 841 820
User-Referenz (8 Bytes)	**WhxSdGIW**	68C36CC069A4	115 188 552 460 708
User-Referenz (16 Bytes)	WhxSdGIWckWqWMvq	. . . .	2.51502807064424531E+28

Die **User-Referenz** bildet die Brücke für den Datenaustausch zwischen Anwender und der Internet-Datenbank Sie kann in der Länge alternativ zwischen 8 und 16 Bytes festgelegt werden.

Zur Registrierung seiner Teilnahme am digitalen Signatur-Verfahren sendet der Anwender die folgenden Daten – und soweit erstellt, auch die Bestätigung des Notars – an den Betreiber der Internet-Datenbank.



Das Verfahren verschlüsselt alle Daten und speichert sie online in der Internet-Datenbank: **Signatur-Portal**. Dort stehen sie dem Empfänger einer signierten Nachricht zur Prüfung und Datenabgleich zur Verfügung.

Ein praktisches Beispiel

Als zu signierende Nachricht wird die Datei „KOBerger.txt“ (13.993 Bytes) gewählt.

Karl-Otto Berger
Berlin

Firma
Sonnenkollektoren **POLYSOL**
33609 Bielefeld

27.10.200

Ihr Angebot vom 17.10.2009 wie beschrieben und signiert: (teleCode: **wUOXuPPRJ**)

1 Voltaik Komplettsystem „**POLYSOL**“
(Schutzklasse II) zur Montage auf Schrägdach
\+ 1 Zentralsteuerungseinheit
\+ 24 Sonnenkollektoren (Größe 2x2 m)
\+ 8 Umwandler (Gleich-/ Wechselstrom)
\+ Kabel und Befestigungsmaterial
einschl. Transport und Montage vor Ort
zum Gesamtpreis von **€ 125.375,00**

nehme ich an.

Mit freundlichen Grüßen

Karl-Otto Berger
Berlin

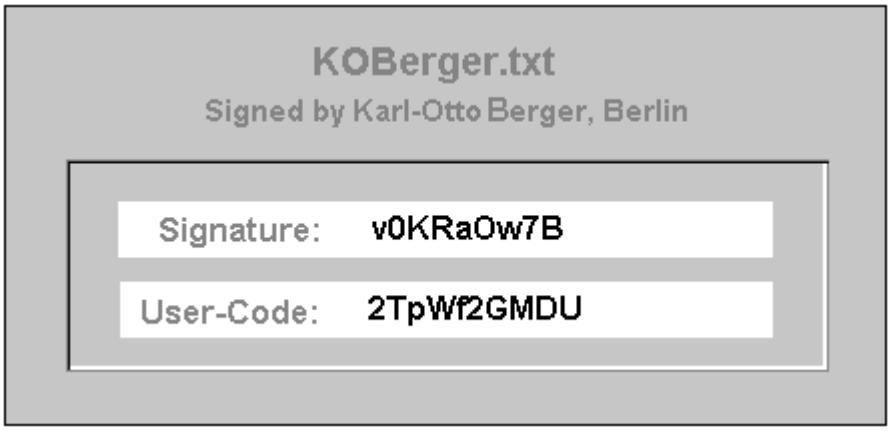
Hinweis: **Erklärung signiert**

Das Verfahren errechnet den Hashwert der Datei: „**KOBerger,txt**“ mit:

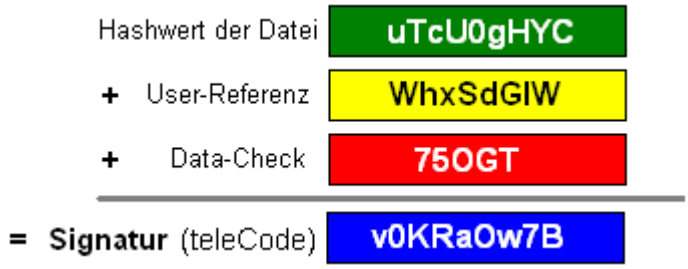
	Basis 62	hexadezimal	dezimal
Hashwert „**KOBerger.txt**“	uTcU0gHYC	2BCF4E2B4BDB7C	12 331 358 639 348 604

Aus der Zusammenfassung der Hashwerte ergibt sich die **Signatur** (teleCode) für die Datei wie folgt:

Hashwert der Datei	uTcU0gHYC	2BCF4E2B4BDB7C	12 331 358 639 348 604
Referenz-Code	WhxSdGIW	68C36CC069A4	115 188 552 460 708
Data-Check	75OGT	63DE3A5	104 719 269
Signatur (teleCode)	v0KRaOw7B	2C38119E4A28C5	12 446 547 296 528 581



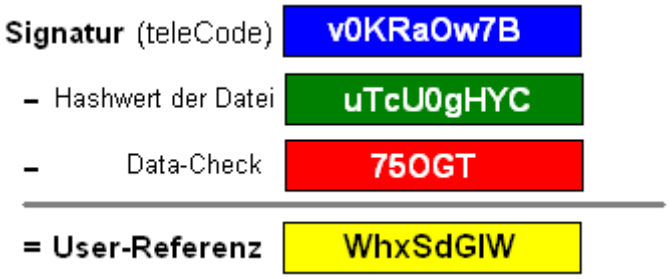
Zum Signieren der digitalen Nachricht werden der **Hashwert** der Information und die **User-Referenz** des Senders addiert und zusammen mit der Datei **„KOBerger.txt“** als Signatur (teleCode) an den Empfänger geschickt. Aus Sicherheitsgründen wird in die Addition ein **Data-Check** einbezogen. Sein Wert ergibt sich aus den digitalen Daten der Nachricht, kann aber von den Beteiligten nicht errechnet oder anderweitig herausgefunden werden.



Abgleichen der Daten mit dem Signatur-Portal

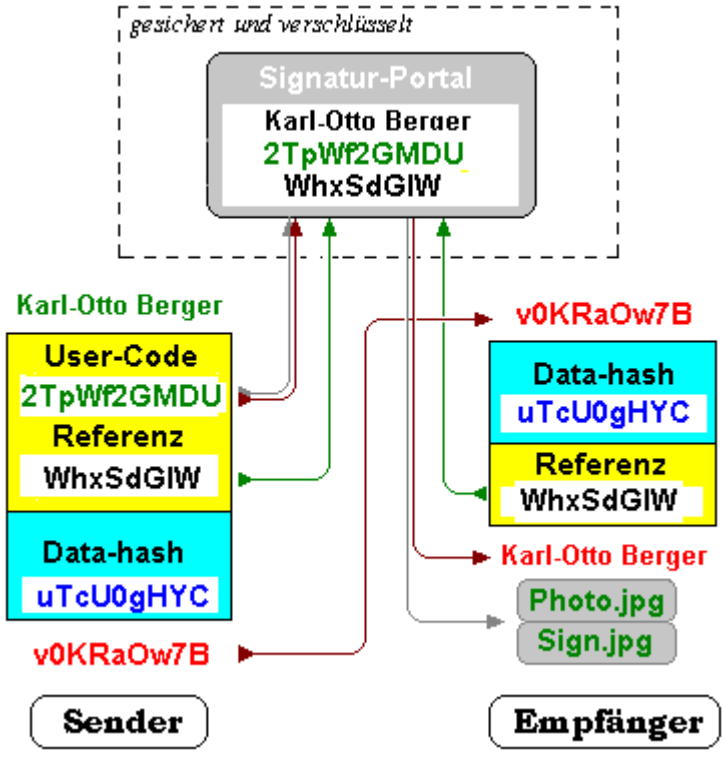
Der Empfänger einer signierten Nachricht kann mit der Hashfunktion des Verfahrens zuerst den **Hashwert** der Datei (plus **Data-Check**) ermitteln und dann aus der Differenz zur erhaltenen **Signatur** die **User-Referenz** des Senders erhalten. Das **Signatur-Portal** übernimmt die Funktion des **vertrauenswürdigen Dritten** und ersetzt insoweit die Zertifizierungsstelle der qualifizierten

elektronischen Signatur. Der Empfänger errechnet die **User-Referenz** des Senders wie folgt:



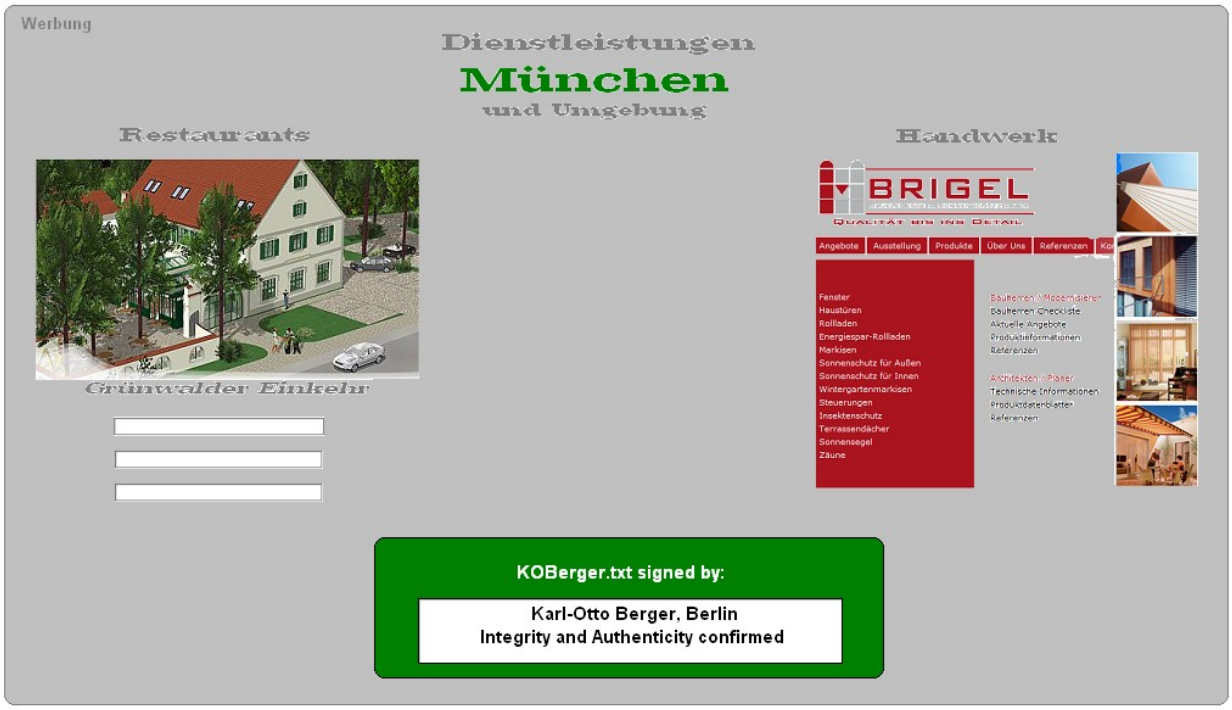
Durch eine Abgleichung der **User-Referenz** mit den in der Internet-Datenbank gespeicherten Daten lassen sich sowohl die **Integrität** der Nachricht als auch die **Identität** des Absenders feststellen. Im Falle der Übereinstimmung wird die Unversehrtheit der Nachricht (**Integrität**) bestätigt und der Name des Absenders (**Authentizität**) mitgeteilt. Zusätzlich kann auch noch das **Passphoto** und die **Unterschrift** des Senders abgerufen werden. Damit kommt die Identifizierung des Senders fast einer persönlichen Gegenüberstellung gleich.

Schematisch stellen sich die Zusammenhänge wie folgt dar:



Bei Übereinstimmung mit den Daten des Absenders werden die **Integrität** der Nachricht bestätigt und dem Empfänger der Name des Absenders (**Authentizität**) mitgeteilt.

Von der Datenbank kommt dann beispielsweise folgende Antwort zurück:



Die Werbeeinblendungen können der Region des anfragenden Empfängers zugeordnet werden.

Der Empfänger kann dann auch noch **Passbild** und **Unterschrift** des Senders anfordern und beispielsweise anhand der folgenden Information selbst visuell verifizieren:

Speicherbedarf in der Datenbank

Die Speicherung der Daten eines Anwenders in der **Internet-Datenbank** umfasst folgende

Bestandteile:

1. Persönliche Daten: Referenz, User-Code und Namen mit Wohnort:	80 Bytes
2. Passphoto-Datei:	12.768 Bytes
3. Unterschrift:	4.080 Bytes

	16.908 Bytes
	ca. 17.000 Bytes
	==========

Bei einem Speicherbedarf von ca. 17 KB pro Teilnehmer lassen sich bei einer Server-Kapazität von 1 TB insgesamt etwa 58 823 529 000 Anwender unterbringen. Das dürfte für Mitteleuropa ausreichen.

Datenschutzbestimmungen

Die Datenschutzgesetze der Länder (z.B: DSG NRW v. 29.4.2003) bestimmen die Regeln für die Verarbeitung personenbezogener Daten. Es fragt sich, ob und in welchem Umfang das hier vorgestellte Verfahren von den gesetzlichen Vorschriften berührt wird.
Nach der Definition des Gesetzes sind personenbezogene Daten:

> **Einzelangaben über persönliche oder sachliche Verhältnisse**
> **einer bestimmten oder bestimmbaren natürlichen Person.**

Das hier vorgestellte Verfahren arbeitet nicht direkt mit personenbezogenen Daten, allenfalls mit deren **Hashwerten**. Infolge der Einweg-Eigenschaft der Hash-Funktion können die Daten auch nicht direkt ausgelesen werden. (Ausnahme: verschlüsselte Speicherung des Namens des Anwenders). Es liegt offenbar ein **Anonymisieren** oder **Pseudonymisieren** i.S. Par.3 Abs.7 und 8 DSG NRW vor. Insoweit sind die Datenschutzbestimmungen zu beachten.

Anwendungen

1. CypherLine

Die einfachste Form des Verfahrens als **"CypherLine"** richtet eine temporäre oder permanente Verbindung zwischen zwei Partnern ein. Dafür werden die internen Parameter des Programms als **Unikat** eingestellt (z.B: Blocklänge = **72** Bytes, Zahlensystem zur Basis **68** und Expansionsfaktor Basis **75**). Der empfangende Partner (Gegenstation, Geschäftspartner, Niederlassung, Internet-Shop, Bank) richtet die **Internet-Datenbank** ein. Der sendende Partner speichert **User-Code** und **User-Referenz** in dieser Datenbank und kann dann jederzeit eine Nachricht mit der errechneten **Signatur** an den Empfänger schicken. Der Empfänger prüft die Integrität der erhaltenen Nachricht und die Authentizität des Senders. Aussenstehende Personen können in den Ablauf der **CypherLine** nicht eindringen, da ihnen die Daten des Absenders nicht bekannt und außerdem alle gespeicherten und übertragenden Daten sicher verschlüsselt sind.

2. CypherCircle

Die Anzahl der Beteiligten lässt sich auf einen größeren Personenkreis erweitern, wie beispielsweise in einem "Intranet": **"CypherCircle"**. Der Ablauf des Verfahrens vollzieht sich wie im Falle CypherLine. Lediglich die internen Parameter zur Steuerung des Verfahrens werden

individuell eingestellt (**Unikat**). Einer der Beteiligten muss die Datenbank installieren, verwalten und dem Zugriff der anderen am Ring beteiligten Partner vorhalten.

3. teleCypher

Wird die Zahl der beteiligten Partner datentechnisch nicht begrenzt und das Programm allen interessierten Anwendern im **Internet** zur Verfügung gestellt, kann das Verfahren als eine einfache digitale **Signatur** verwendet werden , wie oben im Einzelnen beschrieben. Der Betreiber des **Signatur-Portals** übernimmt die Funktion der traditionellen Zertifizierungsstelle. Um Missbrauch auszuschließen kann der Betreiber eine Teilnahme am Verfahren nur zulassen nach eigener Prüfung der persönlichen Daten eines Anwenders oder nach Bestätigung durch einen Notar.

Bemerkungen

Vervielfältigungen und Übersetzungen dieser Ausführungen sowie Verwendungen des beschriebenen Verfahrens oder einzelner Teile davon, die über bloße Testzwecke hinausgehen, bedürfen der ausdrücklichen Genehmigung des Autors. Kritik, Anregungen, Verbesserungen zu den Verfahren, sowie geeignete Partner zur Entwicklung eines kommerziellen Programms sind jederzeit willkommen.

Ihre Nachricht wird erbeten per e-mail an:
eschnoor@multi-matrix.de

München, im November 2009