>teleCode< als erweiterte Signatur

(Ernst Erich Schnoor)

Mit dem „CypherMatrix“ Verfahren lassen sich viele Probleme in der digitalen Informations-Technik einfach bearbeiten und lösen, so auch eine erweiterte Signatur, vom Autor mit >teleCode< bezeichnet. Im Vergleich mit dem im Artikel des Autors "Signatur.pdf" beschriebenen Verfahren einer erweiterten digitalen Signatur ist das folgende Verfahren einfacher, ohne Bild und Unterschrift, aber dennoch sicher gestaltet.

Entsprechend der datentechnischen Gestaltung werden folgende Signaturen unterschieden:

einfache elektrische Signatur,
fortgeschrittene elektronische Signatur und
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 hinreichender Sicherheit - bietet sich folgendes Verfahren als digitale Signatur an:

Basisfunktion: CypherMatrix Verfahren

Generierung und Verifizierung der Signatur erfolgen mit dem Hashwert des Dokuments (Nachricht, Datei, Information) und dem Hashwert der persönlichen Daten des Senders (Signierender) auf der Basis des "CypherMatrix" Verfahrens als dynamische Hashfunktion.

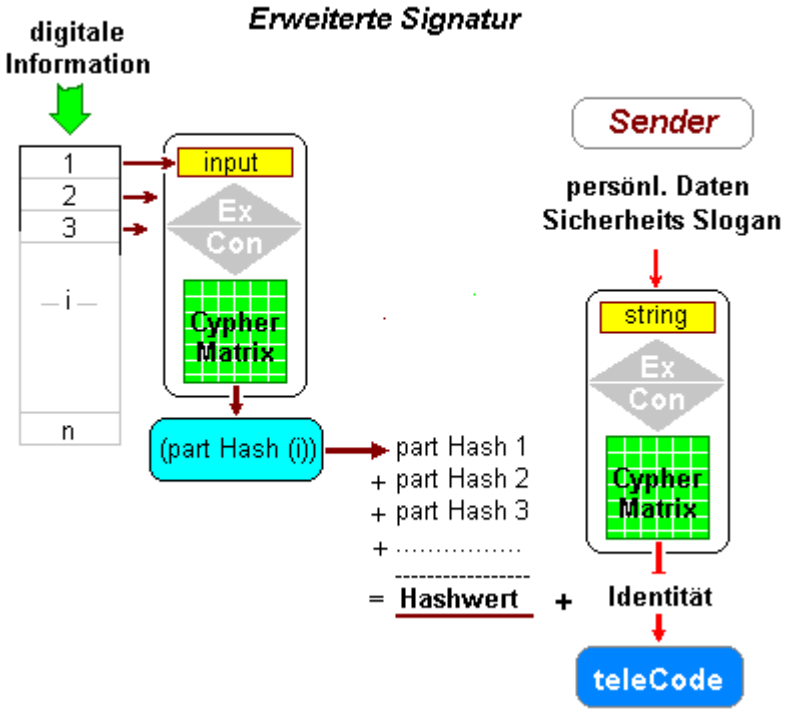
Das Verfahren teilt digitale Zeichenfolgen (Dateien, digitale Nachrichten, Programme, "e-mail"-Kommunikation, Domain-Content, Identifikationsdaten sowie private und öffentliche Schlüssel) in Blöcke fester Länge (z.B: **60** Bytes). Jeder Block wird als Eingangs-Sequenz einer kollisions-freien Einweg-Hashfunktion unterworfen. 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.

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.

1. Hashwerte als Grundlage

Zum signieren einer digitalen Information (Nachricht, Datei) werden der Hashwert der zu **signierenden Information** und der Hashwert der **persönlichen Daten** des Senders addiert und in einem digitalen Wert als Signatur („**teleCode**“) zusammengefasst.

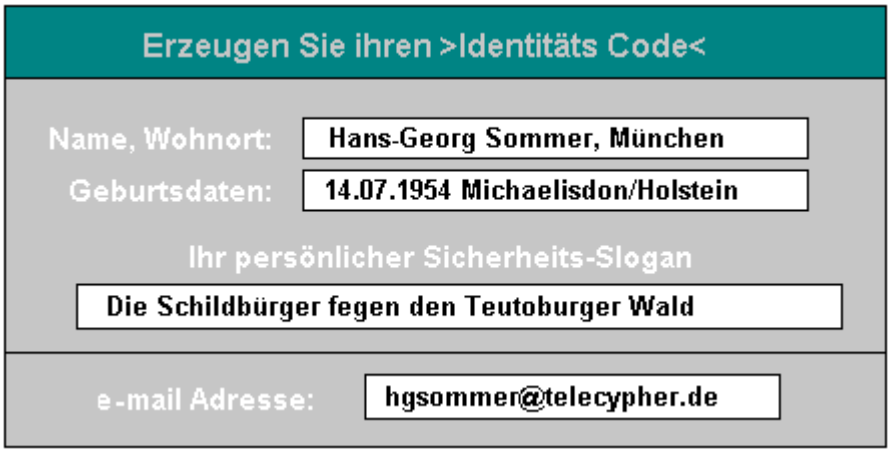
Die folgende Skizze zeigt die Zusammenhänge:



2. Daten des Anwenders

Bei der Installation des Programms sind die persönlichen Daten des Anwenders (Name und Wohnort, die Daten seiner Geburt: Datum und Geburtsort), sowie ein persönlicher Sicherheits-Slogan und seine e-mail Adresse einzugeben. Aus diesen Daten generiert das Verfahren einen Hashwert als **„Identität“ (ID)** des Anwenders. Dazu folgendes Beispiel:

(alle Namen und Daten sind frei erfunden)



	Basis 62	hexadezimal	dezimal
Hashwert „**Identität“ ID:**	**2f75Nz0ig**	210D7CA049BFA	581468946734074

Als **Sicherheits-Slogan** dienen am Besten lustige, zusammenhanglose, widersprüchliche und von anderen Personen möglichst nicht nachvollziehbare Textpassagen (von mindestens 24 Bytes Länge) , wie zum Beispiel:

Bruno der Braunbär aus Bregenz im Breisgau
7 Nordlichter wandern über den großen Belt
blue flamingos flying to Northern Cumberland

Den Sicherheits-Slogan können Sie nach der Eingabe wieder vergessen. Er wird später nicht mehr benötigt und soll vor allem als Ergänzung dienen zu den persönlichen Daten von bekannten Anwendern oder mit kurzen Namen und wenigen Angaben.

3. Zu signierende Information

Als Beispiel dient die Textdatei „**HESSE.TXT**“ mit 742 Bytes

Als Siddhartha den Hain verließ, in welchem der Buddha, der Vollendete, zurückblieb, in welchem Govinda zurükblieb, da fühlte er, dass in diesem Hain auch sein bisheriges Leben hinter ihm zurückblieb und sich von ihm trennte.
Dieser Empfindung, die ihn ganz erfüllte, sann er im langsamen Dahingehen nach. Tief sann er nach, wie durch ein tiefes Wasser ließ er sich bis auf den Boden dieser Empfindung hinab, bis dahin, wo die Ursachen ruhen, denn Ursachen erkennen so schien ihm, das eben ist Denken, und dadurch allein werden Empfindungen zu Erkenntnissen und gehen nicht verloren, sondern werden wesenhaft und beginnen auszustrahlen, was in ihnen ist.

Hermann Hesse, Siddhartha, Eine indische Dichtung, Montagnola 1953

Das Verfahren errechnet den Hashwert der Datei: „**Hesse.txt**“ mit:

	Basis 62	hexadezimal	dezimal
Hashwert Datei**:**	**C2SEfKg0UR**	243067FB2C8D3AF	162981157045588911

4. Erzeugung der Signatur

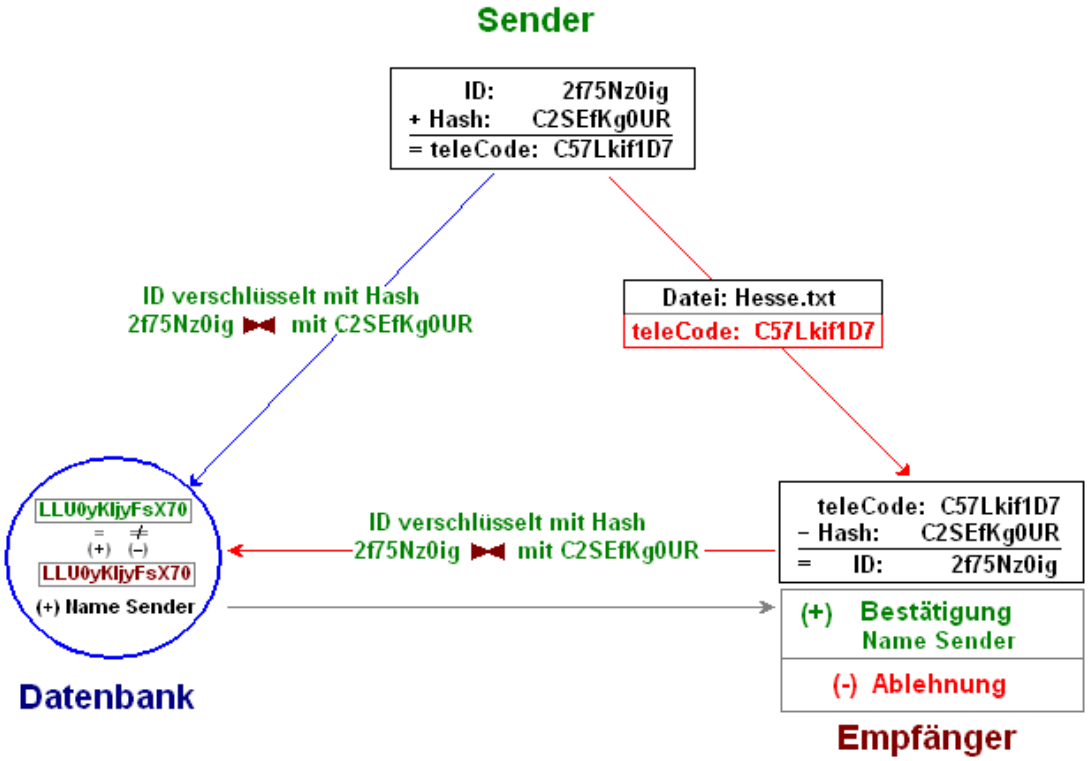
Das Programm erzeugt den „**teleCode**“ (Signatur) für die Datei „HESSE.TXT“ durch Addition des Hashwertes (**Hash**) für die Datei und des Hashwertes für die „Identität“ (**ID**) des Anwenders (Sender) wie folgt:

	Basis 62	hexadezimal	dezimal
ID Anwender:	**2f75Nz0ig**	210D7CA049BFA	581468946734074
+ **Hash**wert Datei:	**C2SEfKg0UR**	243067FB2C8D3AF	162981157045588911
= **teleCode:**	**C57Lkif1D7**	24517577CCD6FA9	163562625992322985

Der Sender schickt die Datei „HESSE.TXT“ zusammen mit dem „**teleCode**“ als Signatur an den Empfänger. Gleichzeitig schickt der Sender seine „Identität“ (**ID**) verschlüsselt mit dem **Hash**wert der Datei als Kontrollinformation an die Datenbank:

2f75Nz0ig ►◄ C2SEfKg0UR = **LLU0yKljyFsX70**

Schematisch vollzieht sich folgender Ablauf:



(►◄ Zeichen für Verschlüsselung mit CypherMatrix)

Zum Testen der Signatur muss der Empfänger natürlich das gleiche Programm verwenden.

5. Testen der Signatur

Der Empfänger errechnet den **Hash**wert der erhaltenen Datei „HESSE.TXT“ und zieht den **Hash**wert von dem erhaltenen „**teleCode**“ ab. Das Ergebnis entspricht der **Identität (ID)** des Senders:

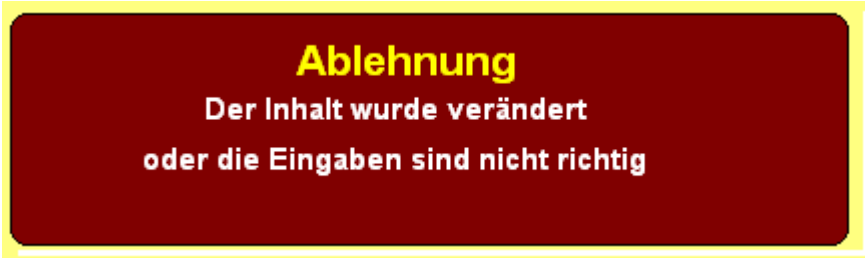
	Basis 62	hexadezimal	dezimal
teleCode:	**C57Lkif1D7**	24517577CCD6FA9	163562625992322985
- **Hash**wert Datei:	**C2SEfKg0UR**	243067FB2C8D3AF	162981157045588911
= **ID** Anwender:	**2f75Nz0ig**	210D7CA049BFA	581468946734074

Der Empfänger verschlüsselt den errechneten Wert „**ID** Anwender“ mit dem errechneten **Hash**wert der Datei „HESSE.TXT“ und schickt das Ergebnis an die Datenbank zum Abgleich mit den dort gespeicherten Daten.

2f75Nz0ig ►◄ C2SEfKg0UR = **LLU0yKljyFsX70**

Stimmt der verschlüsselte Kontrollwert mit dem in der Datenbank gespeicherten Wert überein, erhält der Empfänger eine Bestätigung über die Übereinstimmung mit der Originaldatei und den Namen des Senders zurück (+),

anderenfalls wird der Test abgelehnt (-).



6. Die Datenbank

Wer als Anwender mit der Datenbank in Verbindung treten will, sei es als **Sender** Daten hinterlegen oder als **Empfänger** Daten abgleichen, muss vorher einen Antrag auf Mitgliedschaft stellen, seinen **Referenz-Code** festlegen und an die Datenbank schicken. Nur mit Eingabe des Referenz-Codes ist ein digitaler Kontakt möglich. Ein Eindringen von nicht autorisierten Personen wird so ausgeschlossen.

Der Referenz-Code wird bereits bei der Installation des Programms aus der **Hashfunktionsfolge** der persönlichen Daten des Anwenders abgeleitet.

Referenz-Code = **Nib66TQSW0xl**

Als Zuordnung zum registrierten Anwender wird in der Datenbank seine Identität **(IC)** mit seinem **Referenz-Code** verschlüsselt:

2F75Nz0ig ►◄ Nib66TQSW0xl = **OCBJ47TXlmR87rATtDU**

Bei jedem Zugriff ist daher der Referenz-Code des Anwenders erforderlich. Er wird unverzüglich in der Datenbank abgeglichen. Bei fehlender Übereinstimmung wird der Zugriff verweigert.

7. Angriffszenarien

Für einen Angreifer eröffnen sich folgende Angriffziele:

a) Dem Empfänger eine geänderte digitale Information zu unterschieben mit behaupteter Signatur des ursprünglichen Absenders oder
b) einfach Daten zu ändern und Verwirrung zu stiften.

Information und Signatur werden offen übertragen. Der Angreifer kann den Hashwert einer geänderten Information (Datei) errechnen, den gefundenen **ID** Wert des ursprünglichen Absenders mit dem Hashwert der gefälschten Information verschlüsseln und versuchen, das ganze als Kontrollinformation an die Datenbank zu senden. Da jedoch der Angreifer den Referenz-Code des ursprünglichen Senders nicht kennt, wird der Zugriff verweigert und das Vorhaben muss scheitern.

Mit der Angriffsposition als „**man in the middle attack**“ könnte ein Angreifer ferner versuchen, sich zwischen

a) Sender und Enpfänger,
b) Sender und Datenbank oder
c) Datenbank und Empfänger

zu setzen und die Beteiligten zu täuschen. Die Möglichkeiten b) und c) versprechen keinen Erfolg, da die Datenbank im Fall b) nur über den Referenz-Code des Senders und im Fall c) nur über den Referenz-Code des Empfängers angesprochen werden kann. Im Fall a) könnte der Angreifer den Datenaustausch zwischen den Beteiligten abfangen und durch seine falsche Information ersetzen. Das kann aber in keinem Fall zu einer nachprüfbaren Signatur führen, da der erforderliche Referenz-Code unbekannt ist. Eine bloße Kenntnis der **Identitäten (ID)** der Beteiligten (Sender und Empfänger) ist dagegen unbedenklich, nur der jeweilige **Referenz-Code** eines Beteiligten darf nicht bekannt werden.

Sollte ein Hacker versuchen, in die Datenbank einzudringen, würde er allenfalls folgendes vorfinden:

Gespeicherte Mitglieder:

radLJGRzt7IOI5N6/IlcAre3cI3WslzyNFrlWAPdBBu5cBU25Fghe09BDO&I5Cjup
ALy5U#xrRK80OPMc/&GGteIZLX3PhnReCZBH22gq0UXhAfYEquwr5J3Rl2Mi2bC7V
7#bIT#tSbe0jGm8O/fcCyPsQhiAbB2n68nnZgE3FPH40RJ#Ed8GtVtKgfEuVVO#IN

3#mIbjlINkDyB&vW/cwL7K4cxeL7VkUnxtq7jrfYeb9bttqfJL#ZF3K&txQX3nFPy
Csix3NZaVkBhDj7B/KLIH2UgZy7lu7XuNBeA06d8cGOIOn4Rj0HP#YL1zcWQR4ZyY
….....

Gespeicherte Vorgänge:

pK0HeisG157ty2P4/W3SJwYSQi2AgUIF&mNikfPgAuFfoci0sIEiq9r7NNqg5TAj7
2QcDMf&pRZseV&Pu/d8ohTVCxIldoPl01qvdvzcpXpiHT6FR2LNpHCFCeLBnPUUMZ
JlVFwHOM0u04zGC5/&VBk59eSSBW9KVIBN7&g8RNm9bb6bplBEhA&KUIJvXWCTRAM
hykXJOL&Rh3ypkFI/e5b6bmJJ1MdMr#da#DJrwB30zSc7rqWo&781BQKMMhUovrYS
&GMfbk9hOt7VGVOc/xBOIHLp6kq#mzq7wZ#sDkR&6vBTFqFVGfaHpJkc#EzwkfTbO
2QV3y9ROuE&BWxPu/ls8hTE9RapgHAYH4SvjnGfueissAJsrYMamk13CeLBnPUUMZ
LmzczaOLxqc6a0dz/5sZVd17rie&QvB06cJ0WF6tVIz2yivsH5sQRilfz#rrMDze1
LofIQo8XbMuxJUDQ/hqNXVI4uRNNUQd27UEFb7F0WzHtmG2USQOFcYaKi&jNHt1KV
ej4Q&JJxswoo3WBP/&xi5FxNQsJlaAHgmbtIWRufVhOP2ieU15xMFATDsq8UcaJcC
….....

Die in der **Internet Datenbank** gespeicherten Daten – sowohl die **Mitglieder** als auch die **Vorgänge –** sind mit dem **CypherMatrix** Verfahren verschlüsselt. Dabei werden für jeden Vorgang unterschiedliche „start sequenzen“ (Schlüssel) verwendet. Die Schlüssel können jeweils nur aktuell von den berechtigten Anwender selbst generiert werden.

Mit XOR-Verknüpfung und Bit-Konversion vollzieht sich eine Umwandlung der Klartextzeichen vom Bytesystem zur Basis 8 (**8 bit**) in verschlüsselte Geheimzeichen im Bytesystem zur Basis 6 (**6 bit**: Alphabet mit 64 Zeichen). Das Verfahren – erläutert im Artikel: Verschlüsseln mit >CypherMatrix< - ist kollisionsfrei und sicher.

Zum Testen eines DEMO-Programms kann das Programm „teleCode.exe“ von der Internetseite

http://www.telecypher.net/ZUSENDEN.HTM

herunter geladen werden. Zusendungen und Rückfragen bitte über die e-mail Adresse des Autors:

eschnoor@multi-matrix.de

München, im November 2010