CypherMatrix® als elektronische Signatur

(Ernst Erich Schnoor)

Der Informationsaustausch über digitale Netze (Intranet, Internet) ist grundsätzlich unsicher (Integritätsproblem, Authentizitätsproblem). Eine Lösung bietet hier die elektronische Signatur. Sie hat die Aufgabe, sowohl die Unversehrtheit elektronischer Dokumente (Nachrichten, Dateien) als auch den Absender bzw. Unterzeichner einer gesendeten Information eindeutig festzustellen und zu bestätigen.

Elektronische Signaturen werden eingeteilt in: [#1]

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

Die Durchführung ist im deutschen Signaturgesetz (SigG) als auch in den europäischen Richtlinien zur digitalen Unterschrift geregelt (EU VO 910/2014).

Für qualifizierte elektronische Signaturen schreibt das SigG feste Verfahrensschritte und Schlüsseltechniken vor. Die Funktionsweise ist recht kompliziert, aber im Hinblick auf die rechtliche Wirkung als eigenhändige Unterschrift gleich wohl erforderlich. In anderen Fällen bietet sich die im Folgenden beschriebene elektronische Signatur an. Das Verfahren ist wesentlich einfacher, aber dennoch absolut sicher. Generierung und Prüfung der Signatur erfolgen auf Basis des **CypherMatrix** Verfahrens [#2].

Das Verfahren wird mit **Python 3.7** im 'Terminal' oder unter 'IDLE' als >**teleCypher-Signatur.py**< aufgerufen. Das Verfahren verwendet einen proprietären Zeichensatz (256 bytes):

Zeichen:

ɛ ԴЕ丰ԴEṽ 庢ʟʟ ५ᵻж႟ʋO 𝖾 男ヽ◌̥ͦ ꊓ Ћ歹ᄈ 旁 ЦPɽX ᴌᴇ Π 匧 Rɦ ॐ Й允曰舆 Ɋ ᛇ ῥ'I ᄜ ϵ ᄌ ɱ 剩 Ц 冱

手ト㘶ᄖ 生ΛfЯ೩೩ 香 x ㅕ ᄔ bZ人ᄢ cmʅIo廴 ⸾ X'EedꞨMΔ ꧆ ২ 哫 ꧆ ৭ 扨 U风ৄঘ ᄅ 洞 ऄW¶ 叏 Ѓ ७ ᑭႶИ

ᄣ嗏 ҷॲY 㫖 SЪʅoÿg ⋿ Θ ᄞ◌̐八麦ᄙ ᒪi卄'Y ত Q'O૫N 㖶 ∞ 氷辶 ত χaΘ 叺 㪺 Ⅰ ʔ ᄡ ড L 湳 ᄿ キ ҷДэΘ

ᄙ Э ᄔ Ь ᄊ ꞵ ᄛ ʊ ᄇ Ы 豖ᄀвӪΨ 匽 支ӰV ㅇɧЙ米ㅁㅅ 㔚 ঢ়厂 凖 Աᄿ kƅ ㄷ ঐTΦY ক ৯ 㓭 ƱK ল Ʊp 剢瓦

Ziffern:

0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZÄÖÜß

äöüÞΓΔΘΛΞΠΣΦΨΩαβγδεζηθικλμνξπρςστυφχψωÈЁЄЉЊЋЌЍЎЏАЖЗИЙКбвгдежзийкл

Für den Zeichensatz könnten auch alle anderen Unicode-Zeichen eingesetzt werden, es müssen nur 256 Elemente sein (Variation der 8-bit Zeichen).

Signaturprogramm
(CypherMatrix-Verfahren)

Auswahl: Bereich ..S.. (Senden)
..T.. (Testen)
..K.. (Kontrolle)
..E.. (Einrichten)

..q.. (Beenden)

Bereich wählen > ...

Die Bereiche >Senden< und >Kontrolle< sind für den **Signatar** (Sender) zum Generieren der Signatur und Versenden an den Empfänger bestimmt.

Mit dem Bereich >Testen< kann der Empfänger die erhaltene Signatur testen und die Identität des Senders und die Authentizität der Information prüfen.

Einrichten

Zum Einrichten des Programms werden die persönlichen Daten des Senders (Signatars) wie folgt eingegeben:

Bereich wählen: E

Das Programm wird eingerichtet! Bitte folgende Daten eingeben:

Startsequenz: Sven Hedin hat am Nordpol seine Taschenlampe verloren

Name: Karl-Otto Berger

PLZ Wohnort: 10178 Berlin

Strasse Nr: Heinrich-Heine-Str.12

E-mail: karlotto@email.com

Passport Nr: 19283746-CFA-32

Die Startsequenz sollte ungewöhnlich sein und mindestens 36 Zeichen betragen. Aus den Daten wird ein geheimer Hashwert ermittelt (***1LzDiwHpl***), der verschlüsselt und in der Datei: „**Usercode.txt**" gespeichert wird. Der Wert setzt sich aus Ziffern des Zahlensystems zur Basis 62 zusammen.

Er dient in allen Bereichen zur Identifikation des Senders und ist bei jedem Start des Programms erforderlich.

Bei wiederholtem Aufrufen des Bereichs Einrichten kommt folgende Einschaltung:

Das Programm ist bereits installiert! Soll es überarbeitet und neu eingerichtet werden?

Nein = ..n.. / Ja = ..j.. / Beenden ..q..>

Die Daten können geändert werden. Nur der Name des Anwenders wird aus Sicherheitsgründen beibehalten. Dies um zu verhindern, dass ein Bösewicht den Namen des bisherigen Senders für ein verändertes Objekt missbrauchen könnte.

Senden

Als Beispiel soll die Datei „Ballin.txt“ (1 KB reiner Text) signiert werden.

Eingabe des Bereichs: S

Eingabe des zu prüfenden Objekts

Signierte Datei: Ballin.txt

Nach dechiffrieren der Datei: >Telecode.txt< wird ausgegeben:

Benutzer: Karl-Otto Berger

Eingabe des Objekts: Ballin.txt

Signatur:

SӝѲ 剃 ୨ ড়'YЛ ꟷ吣八ɱd ∃ ꟷ ɩ 嗦 Ѳ ꟷ 'O八hЖ 吣ୣVɗ ʟʟ Q曰歹ʗQχJKФЧ श Ƅआर्ग ꟷ kɘQ୨手Я¬ 叓ᑭ止Op'HΨШ⽇纟 纟 沰台 ɿɲЙQɮ ६ OOɱУ ꝛꝛ允n¬XѲ'ER 刲 g ⊑ ক Y 呉滳ि pΨɯ风୨ ꝛꝛ Ʊ 叺Ⴑ Л 滳 c ꟷ ᑭ ज़ ૪ ㅂ 剃 ʊЧ ꟷ 沰曰曰৵

Die Signatur ist in der Datei: >Telecode.txt< gespeichert

Die Datei zusammen mit dem Objekt an den Empfänger senden

Das Verfahren ermittelt den Hashwert des Objekts (***335779b0333***). Zur Erfassung aller Daten verbindet das Programm die Daten des Anwenders (*Karl-Otto Berger/10178 Berlin/Heinrich-Heine-Str.12/ karlotto@email.com*) mit dem Hashwert der Anwender-Daten (*1LzDiwHpl*) und dem Hashwert des Objekts (*335779b0333*). Die zusammengefassten Daten werden verschlüsselt und in der Datei Telecode.txt als >**Signatur**< zum Empfänger gesendet. Startcode und Hashwert (*1LzDiwHpl*/335779b0333) bleiben als Rückbehalt für spätere Verwendung ('Ballin.txt.arv') beim Sender im Bereich >Kontrolle<.

Testen

Der Empfänger der Information hat zusammen mit der zu prüfenden Datei (Objekt) auch die Datei >**Telecode.txt**< als Signatur erhalten. Der Telecode wird entschlüsselt . Zur Abstimmung der Signatur werden der Usercode (*1LzDiwHpl)* und der Hashwert des Objekts (*335779b0333*) direkt ermittelt und mit den im >Telecode< entaltenen Daten verglichen.

Bereich wählen > T

Eingabe des zu prüfenden Objekts

Signierte Datei: Ballin.txt

Datei >Telecode.txt< lesen [ENTER]

Absender:

Karl-Otto Berger

10178 Berlin

Heinrich-Heine-Str.12

karlotto@email.com

Übereinstimmung ! Keine Änderungen

Eine zusätzliche Prüfung der Daten mit folgendem Aufruf:

Soll die Integrität des Absenders geprüft werden ?

Nein = ..n.. / Ja = ..j.. / Beenden ..q..> j

gewählt: j

Signatar = Karl-Otto Berger

>Ballin.txt.bac< an Karl-Otto Berger senden (karlotto@email.com)

Die Datei 'Ballin.txt.bac' wird an den Signatar zurück geschickt und dort zusätzlich einer abschließenden Kontrolle unterzogen.

Kontrolle

Bei Übereinstimmung der Daten werden sowohl die Authentizität der Signatur als auch die Identität des Signatars analysiert.

Bereich wählen > K

Eingabe des zu prüfenden Objekts: Ballin.txt

Signatar: Karl-Otto Berger

Das Programm ist zur Kontrolle bereit !

1LzDiwHpl/335779b0333 == 1LzDiwHpl/335779b0333

Die Integrität des Signatars wird bestätigt !

Die Information per >E-mail< an den Empfänger zurückschicken !

Sollten die Daten Zweifel erregen, kann der Empfänger in Abstimmung mit dem Sender die Ursache von Abweichungen suchen und daraus die Konsequenzen ziehen. Im Falle fehlender Übereinstimmung zeigt das Programm folgende Information:

Signatar: Karl-Otto Berger

Die Daten des Signatars stimmen nicht überein !

Die Integrität wird nicht bestätigt. Der Vergleich geht fehl !

Die Information per >E-mail< an den Empfänger zurückschicken !

Sicherheit

Mit diesem Signaturverfahren wird jede gefälschte Signatur und/oder jedes noch so geringfügig geändertes Objekt erkannt. Die Sicherheit des Verfahrens ist im wesentlichen von der Verschlüsselung mit folgenden Eigenschaften geprägt (CypherMatrix Verfahren):

1. Proprietärer Zeichensatz (ausgewählte Unicode Zeichen),
2. 'One-time-chain' als kontinuierliche „one-time-pads' [#3] und
3. eine systematische Abstimmung zwischen Signatar und Empfänger.

Außerdem kann der Signatar - wenn ein Dritter versuchen sollte, seine Identifikation zu missbrauchen - jederzeit seine persönliche Startsequenz ändern ohne das die übrigen Daten beeinflusst werden.

Bemerkungen

Wer das Verfahren testen möchte, kann ein Probeexemplar beim Autor per e-mail anfordern (eschnooor@multi-matrix.de). Für die Verwendungen des beschriebenen Verfahrens oder einzelner Teile davon, die über bloße Testzwecke hinausgehen, gilt die CMLizenz.

Kritik, Anregungen, Verbesserungen zu dem Verfahren, sowie geeignete Partner zur Entwicklung eines kommerziellen Programms sind jederzeit willkommen.

München, im August 2019

Ernst Erich Schnoor

[#1] Wikipedia – Elektronische Signatur

[#2] www.teleCypher.net/Matrix-Generator.pdf

[#3] www.teleCypher.net/Algorithmus-CypherMatrix.pdf