Freischaltcode / Rezeptcode – Berechnungsregel Prüfziffer

Stand:	30.07.2020
Gültig ab:	30.07.2020
Version:	1.0.0

Inhaltsverzeichnis

1 Berechnungsregel Prüfziffer

Base32Check1

Für die Base32-Kodierung wird das Alphabet laut RFC 4648, Abschnitt 6 verwendet.

Beispiele Base32Check1-Prüfsumme

Base32 Encoding	Check Digit
""	'A'
"A"	'A'
"AB"	'Q'
"ABCDEFGHIJKLMNO"	'R'

Berechnungsbeispiel

Im Folgenden wird die Prüfsumme für die Base32-Kodierung "ABCDEFGHIJKLMNO" (15 Zeichen) berechnet.

Voraussetzungen

Das gewählte primitive Polynom p := {1, 17, 8, 5, 3} und die entsprechenden Potenzen von p^0 bis p^30.

Berechnung

Zunächst wird für jedes Zeichen der Base32-Kodierung der 0-basierte Index "A" im Base32-Alphabet berechnet. Entsprechend beginnend mit 0 für den Buchstaben "A" und endend mit 31 für die Ziffer 7:

Base32-Zeichen	**Index**
A	0
...	...
Z	25
2	26
...	...
7	31

Für jede Position i im 0-basierten Index der Base32-Kodierung wird die Formel j := (i + 1) mod 31 berechnet. Im gewählten Beispiel gilt a = i. Als nächstes wird für jedes Tupel (a, j) die Matrixmultiplikation v := (a) * p^j berechnet. Bei p^j handelt es sich um eine Matrixpotenz. Von dem sich aus der Matrixmultiplikation ergebenden Vektor v wird nur das erste Skalar verwendet. Der Skalarindex beginnt wieder mit 0, also v0.

Zwischenschritte für gewähltes Beispiel

Base32-Zeichen	a = i	j	v0
A	0	1	0
B	1	2	6
C	2	3	23
D	3	4	21
E	4	5	11
F	5	6	29
G	6	7	18
H	7	8	13
I	8	9	29
J	9	10	31
K	10	11	15
L	11	12	14
M	12	13	21
N	13	14	15
O	14	15	8

Im nächsten Schritt werden die sich ergebenden v0 -Werte XOR verknüpft. Für das gewählte Beispiel ergibt sich s = 28. Als nächstes wird die Länge der Base32-Kodierung l zu einem weiteren Index verarbeitet: k := (30 - l) mod 31. Falls das Ergebnis negativ ist, wird einfach 31 dazu addiert. Für das gewählte Beispiel ergibt sich k = 15. Als nächstes wird wieder die Matrixmultiplikation v := (s) * p^k berechnet, und wieder wird nur das erste Skalar v0 davon verwendet. Für das gewählte Beispiel ergibt sich v0 = 17. Zu guter Letzt wird das Prüfzeichen an dieser Indexposition im Base32-Alphabet herausgesucht. Für das gewählte Beispiel ergibt sich damit das Prüfzeichen R.