JUSTIZ
JUSTIZRESSORT
Bundesministerium für Justiz

Elektronischer Rechtsverkehr (ERV)

Prüfzeichenberechnung für CYBERDOC und ARCHIVIUM

Dateiname: FB_Archiv_Prüfzeichenberechung

Version: 1.0 vom 13.06.2007

Ersteller: Franz Jambrich (franz.jambrich@brz.gv.at)

1 Dokumentinformation

1.1 Inhaltsverzeichnis

1.2 Änderungsverlauf

Version	Datum	Ersteller	Kommentar
1.0	13.06.2007	Jambrich	erste veröffentlichte Version

2 Einleitung

2.1 Zweck des Dokuments

Der Zweck dieses Dokuments ist die Beschreibung des verwendeten Prüfsummenalgorithmus zur Berechnung des Prüfzeichens von CYBERDOC- und ARCHIVIUM-Dokumenten und dessen Anwendung auf die UrkundenID.

Das Prüfzeichen besteht aus 2 Zeichen.

Inhaltlich wurden viele Teile aus den Schriftstücken "Spezifikation Konsistenzprüfung der Archivium Dokumentenarchivs Zugriffscodes V1.0" und "Spezifikation Konsistenzprüfung des Cyberdoc Zugriffscodes V1.2" der Firma Siemens übernommen.

2.2 Begriffsbestimmungen und Abkürzungen

CRC	Cyclic Redundancy Check – Zyklische Redundanzprüfung
CN	Common Name – Ein Teil des Antragstellernamens enthält den Konstanten Wert: "UZS-BMJ.BRZ.GV.AT"

3 Prüfsummenalgorithmus

Als Prüfsummenalgorithmus kommt eine Prüfsumme zum Einsatz.
Dieser Wert hat die Länge eines Bytes.
Bei einer 1 Byte Prüfsumme ergeben das 2 Zeichen aus 0-9 und A-F,
z.B. für 0x3f „3F“ oder 0xa0 „A0“.

3.1 Implementierung

Hier eine C Funktion, die eine bereits vordefinierte Wertetabelle benützt.

```
BYTE CRC8(BYTE crc, LPBYTE pbData, DWORD cbData)
{
    BYTE pbLookAhead[256] = {
        0x00, 0x07, 0x0E, 0x09, 0x1C, 0x1B, 0x12, 0x15,
        0x38, 0x3F, 0x36, 0x31, 0x24, 0x23, 0x2A, 0x2D,
        0x70, 0x77, 0x7E, 0x79, 0x6C, 0x6B, 0x62, 0x65,
        0x48, 0x4F, 0x46, 0x41, 0x54, 0x53, 0x5A, 0x5D,
        0xE0, 0xE7, 0xEE, 0xE9, 0xFC, 0xFB, 0xF2, 0xF5,
        0xD8, 0xDF, 0xD6, 0xD1, 0xC4, 0xC3, 0xCA, 0xCD,
        0x90, 0x97, 0x9E, 0x99, 0x8C, 0x8B, 0x82, 0x85,
        0xA8, 0xAF, 0xA6, 0xA1, 0xB4, 0xB3, 0xBA, 0xBD,
        0xC7, 0xC0, 0xC9, 0xCE, 0xDB, 0xDC, 0xD5, 0xD2,
        0xFF, 0xF8, 0xF1, 0xF6, 0xE3, 0xE4, 0xED, 0xEA,
        0xB7, 0xB0, 0xB9, 0xBE, 0xAB, 0xAC, 0xA5, 0xA2,
        0x8F, 0x88, 0x81, 0x86, 0x93, 0x94, 0x9D, 0x9A,
        0x27, 0x20, 0x29, 0x2E, 0x3B, 0x3C, 0x35, 0x32,
        0x1F, 0x18, 0x11, 0x16, 0x03, 0x04, 0x0D, 0x0A,
        0x57, 0x50, 0x59, 0x5E, 0x4B, 0x4C, 0x45, 0x42,
        0x6F, 0x68, 0x61, 0x66, 0x73, 0x74, 0x7D, 0x7A,
        0x89, 0x8E, 0x87, 0x80, 0x95, 0x92, 0x9B, 0x9C,
        0xB1, 0xB6, 0xBF, 0xB8, 0xAD, 0xAA, 0xA3, 0xA4,
        0xF9, 0xFE, 0xF7, 0xF0, 0xE5, 0xE2, 0xEB, 0xEC,
        0xC1, 0xC6, 0xCF, 0xC8, 0xDD, 0xDA, 0xD3, 0xD4,
        0x69, 0x6E, 0x67, 0x60, 0x75, 0x72, 0x7B, 0x7C,
        0x51, 0x56, 0x5F, 0x58, 0x4D, 0x4A, 0x43, 0x44,
        0x19, 0x1E, 0x17, 0x10, 0x05, 0x02, 0x0B, 0x0C,
        0x21, 0x26, 0x2F, 0x28, 0x3D, 0x3A, 0x33, 0x34,
        0x4E, 0x49, 0x40, 0x47, 0x52, 0x55, 0x5C, 0x5B,
        0x76, 0x71, 0x78, 0x7F, 0x6A, 0x6D, 0x64, 0x63,
        0x3E, 0x39, 0x30, 0x37, 0x22, 0x25, 0x2C, 0x2B,
        0x06, 0x01, 0x08, 0x0F, 0x1A, 0x1D, 0x14, 0x13,
        0xAE, 0xA9, 0xA0, 0xA7, 0xB2, 0xB5, 0xBC, 0xBB,
        0x96, 0x91, 0x98, 0x9F, 0x8A, 0x8D, 0x84, 0x83,
        0xDE, 0xD9, 0xD0, 0xD7, 0xC2, 0xC5, 0xCC, 0xCB,
        0xE6, 0xE1, 0xE8, 0xEF, 0xFA, 0xFD, 0xF4, 0xF3};

    for (DWORD i=0; (i < cbData); i++)
         crc = pbLookAhead[(crc ^ pbData[i]) & 0xff];
    return(crc);
}
```

3.2 Ablauf

Der CRC8 wird über den Common Name (CN) und die Dokumentenkoordinaten gebildet. Der CN sowie die Dokumentenkoordinaten dürfen keine führenden oder nachfolgenden Leerfelder (Leerzeichen, Tabulator, Zeilenvorschub, vertikaler Tabulator oder Seitenvorschub) enthalten.

Zusammensetzung der Dokumentenkoordinaten:

- CYBERDOC: Registrierungsnummer
  laufende Nummer (ohne führende Null)
  Geschäftszahl
  Urkundentyp
- ARCHIVIUM: Archivierungsnummer

3.3 Beispiele

- CYBERDOC:

CN	UZS-BMJ.BRZ.GV.AT
Registrierungsnummer	N120006
laufende Nummer	1
Geschäftszahl	298
Urkundentyp	P

  UZS-BMJ.BRZ.GV.ATN1200061298P ergibt Prüfzeichen 7B

- ARCHIVIUM:

CN	UZS-BMJ.BRZ.GV.AT
Archivierungsnummer	20070611AATAE0005

  UZS-BMJ.BRZ.GV.AT20070611AATAE0005 ergibt Prüfzeichen 5E