Spezifikation des Basic Serial Protocol (BSP)	
Version	3
Datum	06.04.18
Index	

1 Übersicht

Das BSP dient zur Übertragung eines beliebig großen binären “Blobs” über eine etablierte Verbindung. Dabei ist das Ziel eine zuverlässige Datenübertragung zu gewärleisten.

Kommunikation erfolgt durch Austausch von Paketen zwischen zwei Klienten. Die zu übertragenden Daten werden von Klient #1 dem Sender-Program übergeben, welches diese in einem Datenpaket verpackt und verschickt. Das Empfänger-Program vom Klient #2 quittiert den Empfang des Datenpaketes mit dem verschicken eines Antwortpaketes an den Sender und übergibt die entpackten Daten an Klient #2.

2 Verpflichtungen

2.1 Empfänger

1. Der Empfänger ist verpflichtet jedes empfangene Datenpaket zu validieren und zu quittieren.
2. Der Empfänger muss sicherstellen, dass ein valides Datenpaket, das mehr als einmal empfangen wird, nur einmal an den Klienten übergeben wird. Trotzdem muss jedes eingegangene Datenpaket quittiert werden.

2.2 Sender

1. Der Sender ist verpflichtet darauf zu achten, dass der Empfänger zeitnah das verschickte Datenpaket quittiert und ggf. das Datenpaket erneut zu verschicken.
2. Der Sender ist verpflichtet ein Datenpaket, das nicht als OK quittiert wurde erneut zu verschicken.
3. Der Sender darf kein Datenpaket verschicken sofern nicht das vorherige Datenpaket quittiert wurde.

3 Datenpakete

Das Datenpaket besteht neben den zu übertragenden Daten (*raw data*) aus Metadaten, die dem Konrollfluß sowie Fehlererkennung dienen. Um das Verhältnis von *raw data* zu Metadaten zu maximieren werden zwei verschiedene Datenpakete genutzt, abhängig von der Länge der *raw data*: Small Data Packet (SDP) und Large Data Packet (LDP).

	SMD	LDP
Länge von *raw data*	1 - 15 Bytes	16+ Bytes
Länge von Metadata	5 Bytes	10 Bytes
Füllbytes	0 - 14 Bytes	0 Bytes
Gesamte Paketgröße	20 Bytes	-

3.1 Small Data Packet

Ein SDP hat eine Länge von exakt 16 Bytes und besteht aus einem 4 Byte Header und einem 12 Byte payload. Der payload enthält die *raw data* sowie (wenn notwendig) “Füllbytes” um die Länge des payloads auf exakt 12 Bytes zu bringen. Im Detail ein SDP ist wie folgt aufgebaut:

	Größe	Beschreibung
Header	2 Bytes	Packet Type *Siehe Appendix A*
	1 Byte	Packet ID *Siehe Appendix B*
	4 bits	2er Komplement der Länge der *raw data*
	4 bits	Länge der *raw data*
	1 Byte	XOR Checksum *Siehe Appendix D*
Payload	1 - 15 Bytes	*raw data*
	0 - 14 Bytes	Füllbytes (dürfen beliebige Werte haben)

3.2 Large Data Packet

Um *raw data* von mehr als 15 Bytes zu verschicken werden LDPs benutzt. Dabei kann ein einzelnes LDP bis zu 65.536 Bytes transportieren. Bei größeren Mengen von *raw data* wird diese in mehrere Fragmente partioniert und in mehrern LDPs verschickt.

Ein einzelnes LDP besteht aus zwei verschiedenen Sub-Paketen. Zuerst wird ein Control Packet (CP) verschickt, gefolgt von einem Raw Data Packet (RDP).

3.2.1 Control Packet

Ein CP hat eine Länge von exakt 10 Bytes und ist wie folgt aufgebaut:

Größe	Beschreibung
2 Bytes	Packet Type *Siehe Appendix A*
1 Byte	Packet ID *Siehe Appendix B*
2 Bytes	Länge des *raw data*-Fragments - 1
4 Bytes	CRC32 Checksum für das *raw data*-Fragment
1 Byte	XOR Checksum für das CP *Siehe Appendix D*

Wenn der Empfänger den korrekten Empfang des CP quittiert hat wird das zweite Sub-Paket verschickt.

3.2.2 Raw Data Packet

Das RDP besteht aus einem *raw data*-Fragment ohne Metadaten. Daher ist ein RDP zwischen 1 und 65.536 Bytes lang. Auch ein RDP muss quittiert werden. Sollte ein RDP erneut Übertragen werden müssen, muss immer erst das dazugehörige CP noch einmal gesendet (und quittiert) werden.

3.2.3 Cyclic Redundancy Check (CRC32)

Zur Überprüfung der Integrität übertragender RDPs werden CRC32 Checksums nach ISO-3309 verwendet. *Siehe Appendix C*

4 Das Antwortpaket

Jedes empfangene (Sub-)Paket wird vom Empfänger durch das senden eines Antwortpaketes (AP) quittiert. Ein AP ist exakt 5 Bytes groß und ist wie folgt aufgebaut:

Größe	Beschreibung
2 Byte	Packet Type *Siehe Appendix A*
1 Byte	Packet ID *Siehe Appendix B*
1 Byte	XOR Checksum *Siehe Appendix D*
1 Byte	Füllbyte

Die Packet ID ist die ID des Datenpaketes auf das sich das AP bezieht. Im Falle eines RDP (welches keine Packet ID hat) ist die Packet ID im AP gleich 0x00.

5 Ausnahmesituationen

5.1 Unbekannter Packet Type

Wenn ein Paket mit einem Packet Type empfangen wird, der nicht in der Tabelle in Apendix A aufgeführt ist, ist diese unbekannte Type-ID zu analysieren. Weicht sie in nur einem bit von einem der aufgeführten Werte ab ist anzunehmen, dass diese Type-ID gemeint war. In diesem Fall kann die empfangene Type-ID korrigiert werden und der Rest des Paketes normal eingelesen werden. Kann der ursprüngliche Packet Type nicht rekonstruiert werden, dann wird ein Reset Packet (RP) an den Sender geschickt. Daraufhin sind alle ankommenden Daten zu verwerfen bis die Reset Acknowledge Sequence (RAS) *Siehe Appendix E* empfangen wird.

5.2 Reset Packet

Das Empfangen eines RP signalisiert einen schwerwiegenden Datenverlust bei der Übertragung und bedeutet, dass keine Pakete bis zur Wiederherstellung der Kommunikation mehr verschickt werden dürfen. Wenn eine Quittierung für ein verschicktes Datenpaket noch aussteht ist dieses als verloren anzusehen und erneut zu senden. Wenn auf das letzte

versandte AP kein Datenpaket gefolgt hat ist dieses AP ebenfalls erneut zu verschicken. Die Kommunikation wird wieder hergestellt durch das zweimalige Versenden der RAS.

5.3 Failed Checksum in einem AP

Sollte ein AP den Checksum Test nicht bestehen, dann gilt das Paket, auf das sich das AP bezieht, als nicht erfolgreich übertragen und muss noch einmal gesendet werden.

5.4 Wiederholtes Empfangen eines validen Paketes

Sollte ein Paket empfangen werden, was bereits vorher in einem validen Zustand empfangen wurde (zB durch eine Korruption eines AP), dann ist der Inhalt des Pakets zu ignorieren und (im Falle eines Datenpakets) zu quittieren.

6 Appendices

A Packet Type

Ein Packet Type ist eine 2 Byte Sequenz die die Inhalt eines Pakets kategorisiert. Es bildet den Anfang von jedem Paket (abgesehen von DPs, die keinen Packet Type haben) und sind im Big Endian Format. Es gibt 6 verschiedene Paket-Typen:

Wert	Paket	Erläuterung
81 A5	Small Data Packet	
42 96	Control Packet (SUPER)	Das folgende RDP ist nur ein Teil der zu übertragenden *raw data*; es folgen noch weitere LDPs
24 C9	Control Packet (LAST)	Das folgende RDP enthält das letzte *raw data*-Fragment.
18 7C	Answer Packet (OK)	Datenpaket ist empfangen und valide.
36 13	Answer Packet (ERR)	Datenpaket ist beschädigt und muss noch einmal versandt werden.
70 B1	Reset Packet	Es gab einen schwerwiegenden Kommunikationsfehler und die beiden Klienten müssen sich erst synchronisieren bevor die Kommunikation wieder aufgenommen werden kann.

B Packet ID

Beim Senden eines Datenpaketes (SDP und CP) gibt der Sender diesem eine numerische ID. APs halten die ID des Paketes auf das sie sich beziehen. RDP haben keine Packet ID. Die vergebenen IDs dürfen nicht 0 sein und fangen daher bei 1 an und werden für jedes weitere **versandte** Paket um 1 erhöht. Da für das Packet ID nur ein Byte reserviert ist wird nach erreichen der ID 255 wieder bei 1 angefangen. Beide Klienten müssen mindestens die letzten 20 gesendeten Pakete und die IDs der letzten 20 empfangen Pakete gespeichert halten.

C Cyclic Redundancy Check (CRC32)

Die Integrität eines jeden RDP wird durch einen CRC sichergestellt. Dabei wird vom Sender ein 32 bit Wert errechnet und im CP verschickt. Beim Empfangen des RDP errechnet der Empfänger ebenfalls einen Wert basierent auf dem empfangenen RDP. Diese beiden Werte sind identisch wenn das Paket korrekt übertragen wurde. Die Errechnung des CRC Wertes erfolgt nach ISO 3309. Dabei wird folgendes CRC Polynom genutzt:

$$f(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Der CRC Wert wird vor der Berechnung mit 1sen initialisiert und nach der Berechnung invertiert. Im CP wird der CRC Wert im Big Endian Format gespeichert.

D XOR Checksum

Die XOR Checksum beschreibt einen 1 Byte großen Wert der durch die Verknüpfung mit XOR aller anderen Bytes im Paket entsteht. Dies hat zur Folge, dass wenn mal alle Bytes in einem Paket (inklusive der XOR Checksum) durch XOR verknüpft der Wert 0x00 heraus kommt. Ist das Ergebnis dieser Berechnung *nicht* 0x00, dann wurde der Inhalt des Paketes im Transport beschädigt.

E Reset Acknowledge Sequence

Die RAS ist die Folgende Byte-Sequenz:

```
91 0D 91 0D 91 0D 91 0D 91 0D 91 0D 91 0D 91 0D
```

Im Falle einer empfangenen RAS wird so lange weitergelesen, bis etwas anderes als eine Sequenz von `91 0D` gelesen wird.

F Glossar

Acronym	Bedeutung
BSP	Basic Serial Protocol
SDP	Small Data Packet
LDP	Large Data Packet
CP	Control Packet
RDP	Raw Data Packet
CRC	Cyclic Redundancy Check
AP	Answer Packet
RP	Reset Packet
RAS	Reset Achnowledge Sequence