SBTEL - Symetric Burst Transport Encryption Layer

A Transport Layer with low latency for embedded system purpose

By Simon Diepold

SBTEL is a encrypted transportlayer which is usualy user over UDP oder TCP. It requires a setup phase over a secure channel to exchange a Symmetric key encryption and authentication.

I) SBTEL-Package Format

8B	4B	4B	1B-4KB	1B-4KB
Sender ID, UTF8 HEX	Data size in Bytes, UTF8, HEX	Signature size in Bytes, UTF8, HEX	Encrypted Data field	signature

Sender ID

At the beginning of the package ist a field with the size of 8 bytes which encodes in utf8 HEX digits (little endian) a sender ID. The sender ID is a uniqe identifier for the original sender of the package. Without a valid id, i key can not be matcht. If a SBTEL endpoint recieves a package with a unknown sender ID, it will be dropped imidiatly.

Data size

The Second field ist the size of the data area in bytes, again encoded in utf8 HEX (little endian) digits. Its maximum size is 4096 (0x1000) and it‘s minimum values ist 1. If the value is zero, the package will be dropped.

Signature size

The third field is the size of the signature field at the end of the package. The package will bei droped imidiatly if the sum of the fields does not fit to the size of the arrived package. Its maximum size is also 4096 (0x1000). If the value is zero, the package will be dropped.

The data field

1-17B	1B	Datasize-(PSN+1)
Package serial number (PSN)in HEX, UTF8	,	Payload

The data field consists of two fields, seperated by a utf8 comma. The first one is a serial number for the current package in the current communication channel. It is used to simplify debuging and prevent replay attacks if it is used as described in section II). The encoding is agian utf8 little endian hex code. The payload can have any desired format.

The signature is a digital signature of the entire package exept of itself. The signature can be assymetric or symmetric. The used algorythm needs to be configured in the setup phase on all communication partners. The signature is in raw independent bytes. The field does not perform any endianess operations.