V50 SPECIFICATION

Project	Autor	Date
PULSE V V50 Basic Specification	Marc Stockburger	12.04.2019

INHALT

General 2

UART 2

Frame 2

Timing 6

CRC16 6

Encryption 7

Example Case1 (Simple Telegram) 10

Example Case2 (Simple Telegram) 11

Example Case3 (Simple Telegram Encrypted) 12

Example Case4 (Tunnel Telegram Encrypted) 14

Example Case5 (Tunnel Telegram Encrypted) ..... **Fehler! Textmarke nicht definiert.**

V50 SPECIFICATION

General

„V50“ Interface frame specification. Here in special, the communication between the host controller and the radio module (Nordic Controller).

UART

- asynchron
- 57 600 baud
- 1Stop Bits
- Even Parity 8 Data Bits
- LSB first
- Big Endianness

Frame

Basic Structure

STX(8Bit)	Length L (8Bit)	Secure Info (8Bit)	Profile(16Bit)	DestNode(16Bit)	SourceNode(16Bit)	**Payload (L Bytes)**	CRC16 (16Bit)

„length“→payload length

„Secure Info“→ 0=no Encryption; 1=AES128 CCM Encryption (additional data);

„profile“→ contain the profile number, profile encryption type and the profile type attribute:

- **Bit 15 Tunnel Mode : 0 =Simple Communication; 1= Tunnel Mode (additional Data)**
- Bit14-13: Res (0)
- Bit12: Ack Wish
- Bit11-0 Profile number (see profile table)
    - Bit11 High→Query; Bit11 Low→Command

„destNode“→ Destination node (physical low level node).

- Bit10 Low →Bit15-11 Short dest. address of intern lumis
- Bit10 High→ no short dest. address at Bit11-13. Bit11-13=0 → Complete address will be insert at begin of data.

Additionally data:

“data length” (exist only in encryption mode): →data length.

“data” (only in encrypt mode): data

“padding byte” (exist only in encryption mode): rest bytes of modulo 16 (encryption data must be divisible by 16); all bytes 0x00

“request Info ” (exist only in tunnel Mode):

- Bit 3-Bit 0 : 0=Query; 1= Command; 2=Command Multi Tel Start; 3=Command Multi Tel Next; 4=Command Multi Tel Last;

“BLE Short Address" (exist only in tunnel Mode): 2Byte short Address

“MIC" (exist only in encrypt. Mode): 4Byte MAC

V50 SPECIFICATION

Simple Telegram

General exchange information's (like configurations, key exchange…) between BLE und Host (here unencrypted).

STX (8Bit)	Length (L) (8Bit)	Secure Info (8Bit)	Profile Tunnel (1Bit)	Profile Attribute (3Bit)	Profile number (12Bit)	DestNode (16Bit)	SourceNode (16Bit)	**Payload (L Bytes)**	CRC16 (16Bit)
0x55	paylength	0	0	attribute	**number**	address	address	**see below**	value

Payload:

Data (L Bytes)
Data……

-CRC16 over the complete telegram

General exchange information's (like configurations, key exchange…) between BLE und Host (here encrypted).

STX (8Bit)	Length L (8Bit)	Secure Info (8Bit)	Profile (16Bit)	DestNode (16Bit)	SourceNode (16Bit)	***Payload (L Byte)**	CRC16 (16Bit)
0x55	paylength	1	0000	address	address	**see below**	value

***Payload:**

Frame Counter (48Bit)	Sub-Profile Tunnel (1Bit)	Sub-Profile Attribute (3Bit)	Sub-Profil number (12Bit)	Sub-Length N	Data (N Byte)	Padding Byte (must be divisible by 16)	MIC (32Bit)
Value	0	attribute	number	data length	Data…….	0x00……	value

-CCM-AES128 Encrypted (must be divisible by 16)

V50 SPECIFICATION

-MIC: MAC over complete unencrypted message (without CRC16)

-CRC16 over complete encrypted message

Tunnel Telegram

Tunnel over BLE to communicate outside in the mesh. Always encrypted.

STX (8Bit)	Length L (8Bit)	Secure Info (8Bit)	Profile (16Bit)	DestNode (16Bit)	SourceNode (16Bit)	**Payload (L Byte)**	CRC16 (16Bit)
0x55	paylength	0x01	0000	address	address	**see below**	value

Payload:

Frame Counter (48Bit)	Sub-Profile Tunnel (1Bit)	Sub-Profile Attribute (3Bit)	Sub-Profil number (14Bit)	Sub-Length N (8Bit)	BLE Short Node Dest (16Bit)	BLE Short Node Source (16Bit)	Key ID 32Bit	Reserve (8Bit)	Data (9+N Byte)	Padding Byte (Encrypt must be divisible by 16)	MIC (32Bit)
value	1	attribute	number	data length	adresse	adresse	id	info	data…	0x00….	value

-CCM-AES128 Encrypted (must be divisible by 16)

-MIC: MAC over complete unencrypted message (without CRC16)

-CRC16 over complete encrypted message

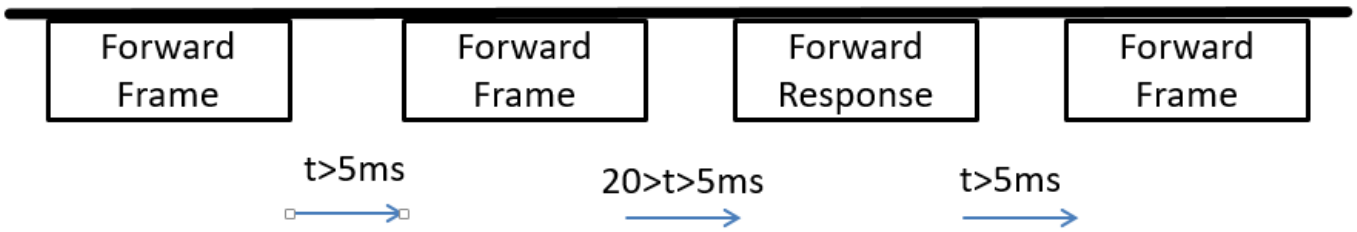
V50 SPECIFICATION

Timing

Frame Timing

Forward to Forward Tel.: >5ms

Forward to Response Tel.: <20ms and >5ms



Telegram or CRC error handling:

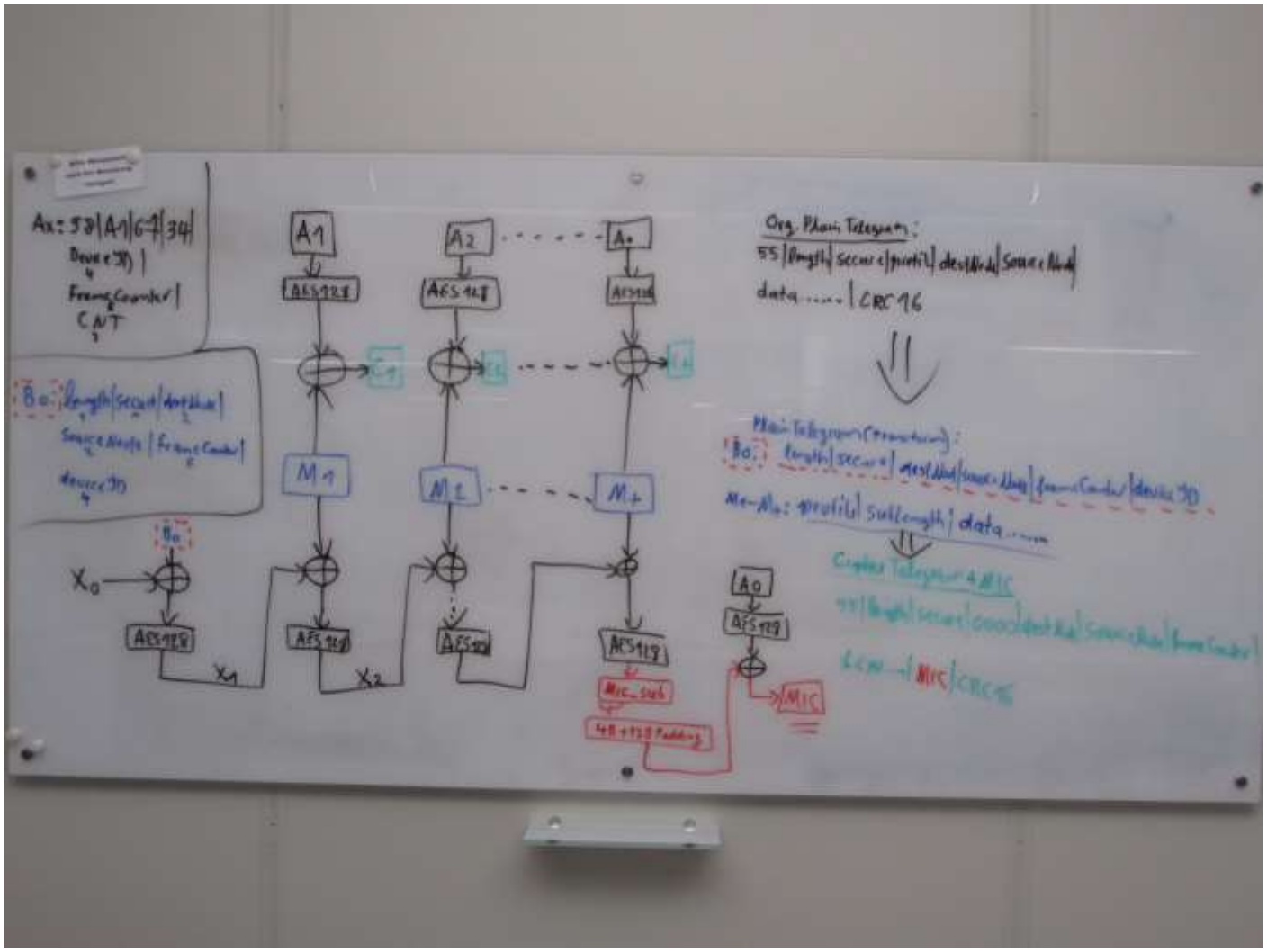
If no, wrong or nack response, try it max. 3 times. Than abort it for this time. Maybe change baud Rate back to default.

CRC16

Datasheet	Polynomial
CRC-16 (CRC-CCITT)	0x1021
CRC32 (IEEE 802.3)	0x04C11DB7

V50 SPECIFICATION

Encryption



B0: DeviceDestAddress (4Bytes) | Length (1Byte)| SecureInfo(1Byte) | DestNode(2Byte)| SourceNode(2Byte)|FrameCounter(6Bytes)

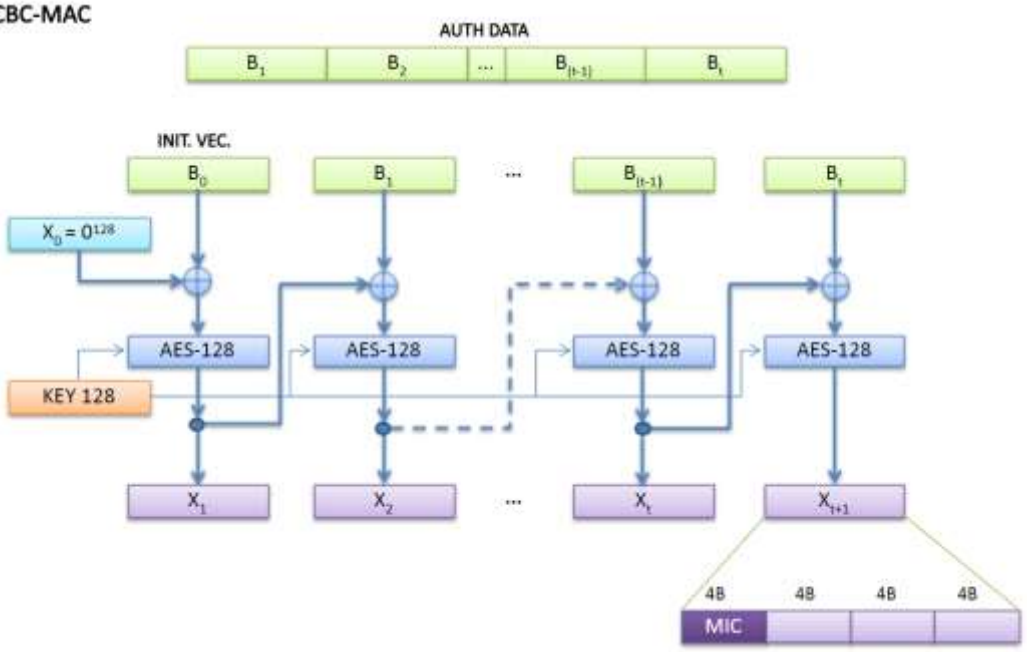
A0,A1…..: 0x98|0xA1|0x67|0x34|DeviceDestAdress (4Byte) | Frame Counter (6Byte) | CNT (2Byte)

X0=0^128

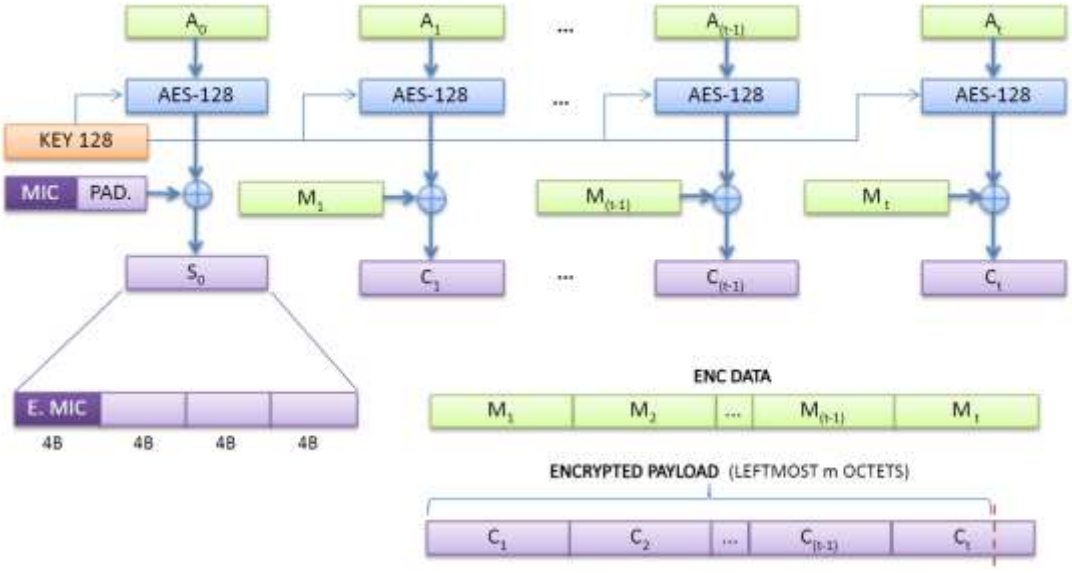
V50 SPECIFICATION

CCM Principe

AES-CBC-MAC



AES-CTR



Quelle:

https://player.slideplayer.com/15/4625158/

Frame Counter (4Bytes)

If(Rx FrameCounter > FrameCounter) FrameCounter=Rx FrameCounter

else invalid

V50 SPECIFICATION

Example Case1 (Simple Telegram)

Description: Activate LED Flash on BLE module

- Host intern Lumi 1.
- acknowledge yes
- Interface between BLE and Host: UART 1

1)Host → BLE: Command set module LED

STX (8Bit)	Length (8Bit)	Secure Info (8Bit)	Profile Tunnel (1Bit)	Profile Attribute (3Bit)	Profile table (12Bit)	DestNode (16Bit)	SourceNode (16Bit)	**Payload (L Bytes)**		CRC16 (16Bit)
0x55	2	no	no	ACK	statusLedModule (0x062)	UART1	Host Intern Lumi 1	**LED Flash (slow)**		Value
0x55	0x02	0x00	0x1062			0x0020	0x1000	0x20	0x14	??

2)BLE→Host: Acknowledge

STX (8Bit)	Length L (8Bit)	Security Info (8Bit)	Profile Tunnel (1Bit)	Profile Attribute (3Bit)	Profile table (12Bit)	DestNode (16Bit)	SourceNode (16Bit)	**Payload (L Bytes)**	CRC16 (16Bit)
0x55	1	No	no	-	Ack (0x0A1)	Host Intern Lumi1	UART1	**ACK Message**	Value
0x55	0x01	0x00	0x00A1			0x1000	0x0020	0x00	?????

Example Case2 (Simple Telegram)

Description: Query BLE module rotary switch's

- Host general: Query Rotary Switch on BLE module.
- Rotary Switch: S1=10; S2=12; S3=9; S4=4
- Interface between BLE and Host: UART 5

1)Host → BLE: Query module rotary switch's values

STX (8Bit)	Length L (8Bit)	Security Info (8Bit)	Profile Tunnel (1Bit)	Profile Attribute (3Bit)	Profile table (12Bit)	DestNode (16Bit)	SourceNode (16Bit)	**Payload (L Bytes)**	CRC16 (16Bit)
0x55	1	No	No	no	queryRotarySwitch Module (0x80A)	UART5	General	**Data**	value
0x55	0x01	0x00	0x080A			0x0060	0x0000	0x00	0x629B

2)BLE→Host: Send rotary switch values

STX (8Bit)	Length L (8Bit)	Security Info (8Bit)	Profile Tunnel (1Bit)	Profile Attribute (3Bit)	Profile table (12Bit)	DestNode (16Bit)	SourceNode (16Bit)	***Payload (L Bytes)**	CRC16 (16Bit)
0x55	4	no	No	No	rotarySwitch Module (0x064)	General	UART5	**Data….**	Value
0x55	0x01	0x00	0x0064			0x0000	0x0060	See below	??

*Payload:

Data0	Data1	Data2	Data3
0x0A	0x0C	0x09	0x04

Example Case3 (Simple Telegram Encrypted)

Description: Query Key1

- BLE Module: Query Key1 from SE Element.
- Interface between BLE and Host: UART 3
- Frame Counter act Value 0x001105795678

1)BLE → Host: Query Key

STX (8Bit)	Length L (8Bit)	Secure Info (8Bit)	Profile Tunnel (16Bit)	DestNode (16Bit)	SourceNode (16Bit)	***Payload (L Bytes)**	CRC16 (16Bit)
0x55	22	AES128-CCM	Encrypted	SE-Element	General	**Data….**	value
0x55	0x16	0x01	0x0000	0x0002	0x0040	See below	??

*Payload:

Frame Counter (48Bit)	Sub-Profile Tunnel (1Bit)	Sub-Profile Attribute (3Bit)	Sub-Profile number (12Bit)	Sub-Length N (8Bit)	Data (N Bytes)	Padding Bytes (Encrypt must be divisible by 16)	MIC (32Bit)
counter	No	0	queryKEY1 (0x810)	0x01	0x00	12x 0x00	???
0x001105795678	0x0810			0x01	0x00	12x0x00	

-CCM-AES128 Encrypted (shown data are not encrypted)

-MIC: MAC over complete unencrypted message (without CRC16)

-CRC16 over complete encrypted message

V50 SPECIFICATION

2)Host→BLE: Send Key1

STX (8Bit)	Length L (8Bit)	Secure Info (8Bit)	Profile (16Bit)	DestNode (16Bit)	SourceNode (16Bit)	**Payload (L Bytes)**	CRC16 (16Bit)
0x55	16	AES128-CCM	encrypted	UART	SE-Element	**Data….**	value
0x55	0x10	0x01	0x0000	0x0040	0x0002	See below	??

*Payload

Frame Counter (48Bit)	Sub-Profile Tunnel (1Bit)	Sub-Profile Attribute (3Bit)	Sub-Profile (12Bit)	Sub-Length N (8Bit)	Data (N Bytes)	Padding Bytes (Multiplier 16Bytes)	MIC (32Bit)
counter	no	No	SEKey1 (0x0E0)	0x10	KEY (16Bytes)	13 x 0x00	???
0x001105795679	0x80E0			0x10	……	13x0x00	

-CCM-AES128 Encrypted

-MIC: MAC over complete unencrypted message (without CRC16)

-CRC16 over complete encrypted message

-“Sub-Length”: from “Data” to last “Padding Byte”.

Example Case4 (Tunnel Telegram Encrypted)

Description: Set working art template

- BLE Module: Set new template from Host intern Lumi4
- Interface between BLE and Host: UART 3
- Frame Counter act Value 0x001105823566
- BLE own Short Node: 0x0045; Radio incoming from BLE short Node:0x0011

1) BLE → Host: Set new working art template

STX (8Bit)	Length L (8Bit)	Secure Info (8Bit)	Profile (16Bit)	DestNode (16Bit)	SourceNode (16Bit)	***Payload (L Bytes)**	CRC16 (16Bit)
0x55	??	yes	encrypted	Host Intern Lumi 4	UART3	**Data….**	value
0x55	??	0x0x01	0x0000	0x8000	0x0040	See below	??

***Payload**

Frame Counter (48Bit)	Sub-Profile Tunnel (1Bit)	Sub-Profile Attribute (3Bit)	Sub-Profile number (12Bit)	Sub-Length (8Bit)	BLE dest Short Node	BLE source Short Node	BLEKey ID(32Bit)	Res.	Data (N Bytes)	Padding Bytes (Multiplier 16Bytes)	MIC
counter	Yes	no	setWorking artTemplate (0x065)	0x53	adresse	adresse	key	0x00	……..	……..	????
0x00110 5823566	0x8065			0x53	0x0045	0x0011	????	0x00	……	……	

-CBC-AES128 Encrypted

-MIC: MAC over complete unencrypted message (without CRC16)

-CRC16 over complete encrypted message

-"Sub-Length":from "BLE dest Short Node" to last "Padding Byte".