

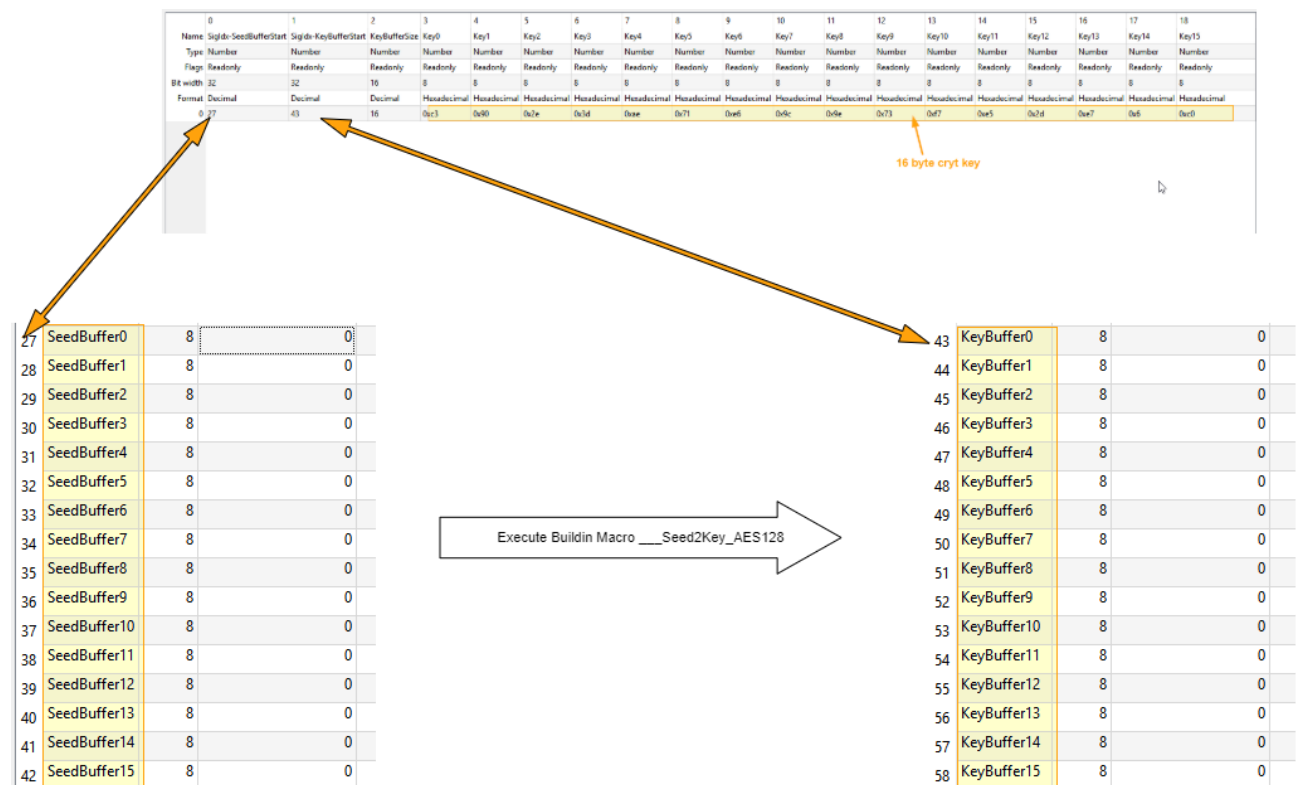
## Table of Content

Objective .....	2
Device requirements .....	2
SDF requirement.....	2
System table @@SYSTAB_SEED2KEY_AES128 .....	3
Column 0 SigIdx-SeedBufferStart.....	3
Column 1 SigIdx-KeyBufferStart.....	3
Column 2 KeyBufferSize .....	3
Column 3...18 Key Bytes0...15 .....	3
BuildInMacro __Seed2Key_AES128.....	4
Document revision history.....	5

## Objective

Since firmware version 6.23 B5 of Baby-LIN/Harp firmware, there exists a buildin macro, to encrypt a 16 Byte seed given in a virtual signal array SeedByte0...SeedByte15, into a 16 Byte key which will be placed in virtual signal array KeyByte0...KeyByte15.

The encryption key will be defined in a new system table @@SYSTAB\_SEED2KEY\_AES128



The parameter of BuildIn Macro \_\_\_\_Seed2Key\_AES128 allows to select row to use if system table would hold multiple rows (e.g. with different crypt keys).

## Device requirements

To use the Buildin macro \_\_\_\_Seed2Key\_AES128 with a Baby-LIN device, these things are required:

1. Installed firmware must be 6.23 B5 or later.
2. The SDF file must be extended to have specific system table, and macros and virtual signal.

## SDF requirement

To use Buildin macro \_\_\_\_Seed2Key\_AES128 in an SDF application, some specific elements must be added to the SDF file.

1. System table @@SYSTAB\_SEED2KEY\_AES128

2. BuildInMacro \_\_\_\_Seed2Key\_AES128 must be defined
3. Virtual signal Arrays SeedByte0..15 must be defined
4. Virtual signal Arrays KeyByte0...15 must be defined

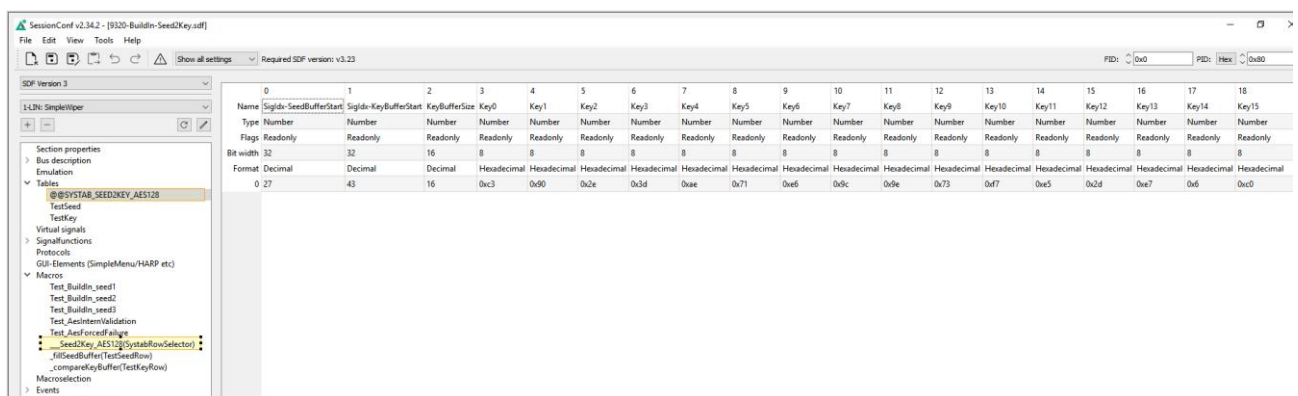
The SDF will typically contain a protocol service to get Seed from ECU and to write Key to ECU.

These both services will use the virtual signal arrays SeedByte1..16 and KeyByte1...64 in their signal mappings for the response resp, request payload.

## System table @@SYSTAB\_SEED2KEY\_AES128

This table tells the build in macro where the virtual signal arrays SeedByte0...15 and KeyByte0...15 are located.

It also holds the crypt key used for the applied AES128-BCB algorithm.



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Name	SigIdx-SeedBufferStart	SigIdx-KeyBufferStart	KeyBufferSize	Key0	Key1	Key2	Key3	Key4	Key5	Key6	Key7	Key8	Key9	Key10	Key11	Key12	Key13	Key14	Key15
Type	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number	Number
Flags	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly	Readonly
Bit width	32	32	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
Format	Decimal	Decimal	Decimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal	Hexadecimal
	0 27	43	16	0xc3	0xd0	0x2e	0x3d	0xae	0x71	0xae	0xdc	0xde	0x73	0xd7	0xe5	0x2d	0xe7	0x6	0xc0

*Column 0 SigIdx-SeedBufferStart*

Signal Index of first signal forming the virtual signal array for Seed (SeedByte0)

*Column 1 SigIdx-KeyBufferStart*

Signal Index of first signal forming the virtual signal array for Key (KeyByte0)

*Column 2 KeyBufferSize*

This tells the size of the KeyByte Array, which will be written by Buildin macro

*Column 3...18 Key Bytes0...15*

This columns hold the 16 Bytes of the encryption key used.

## BuildInMacro \_\_\_\_Seed2Key\_AES128

This new special BuildIn Macro will be assigned as an empty macro with parameter description and a specific name.

During parsing the reserved name will be recognized and the macro will be used as an entry point to call an internal firmware function.

So, this why it is important to assign the macro with exactly this name "\_\_\_\_Seed2Key\_AES128" with three leading '\_' characters!

It then be called from within the SDF by a gosub macro command.

You might add print command, which will be executed only, when the name was written incorrect, or if the firmware installed does not yet support this build in macro.

This might help to make such a kind of problem visible in SimpleMenu Report Monitor (or in MB-II Logfile).

SessionConf v2.34.2 - [9320-BuildIn-Seed2Key.sdf]

File Edit View Tools Help

Show all settings Required SDF version: v3.23

SDF Version 3

1-LIN: SimpleWiper

Macro number 5

Name Seed2Key\_AES128

Parameter count 1

Parameter names SystabRowSelector

Comment

Label	Condition	Command
0		Print on Debug report: "If you see this firmware does not support Buildin!"

Section properties

- Bus description
- Emulation
- Tables
  - @SYSTAB\_SEED2KEY\_AES128
    - TestSeed
    - TestKey
  - Virtual signals
- Signalfunctions
- Protocols
- GUI-Elements (SimpleMenu/HARP etc)
- Macros
  - Test\_BuildIn\_seed1
  - Test\_BuildIn\_seed2
  - Test\_BuildIn\_seed3
  - Test\_AesInternValidation
  - Test\_AesForcedFailure
  - Seed2Key\_AES128(SystabRowSelector)
  - \_fillSeedBuffer(TestSeedRow)
  - \_compareKeyBuffer(TestKeyRow)
- Macroselection
- Events
- Device-specific options

## Document revision history

Date	Revision	Action	by	Comment
20.06.2023	A		al	Initial revision