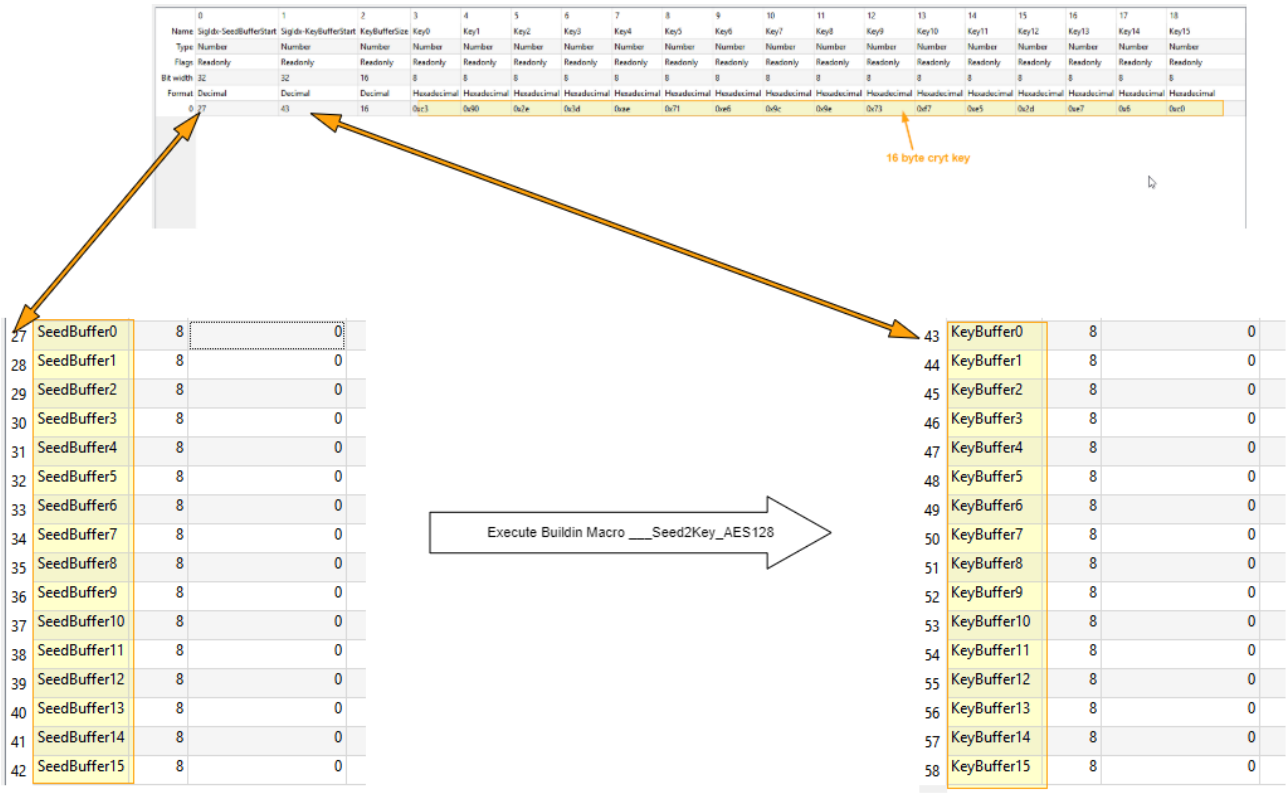
Table of Content

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

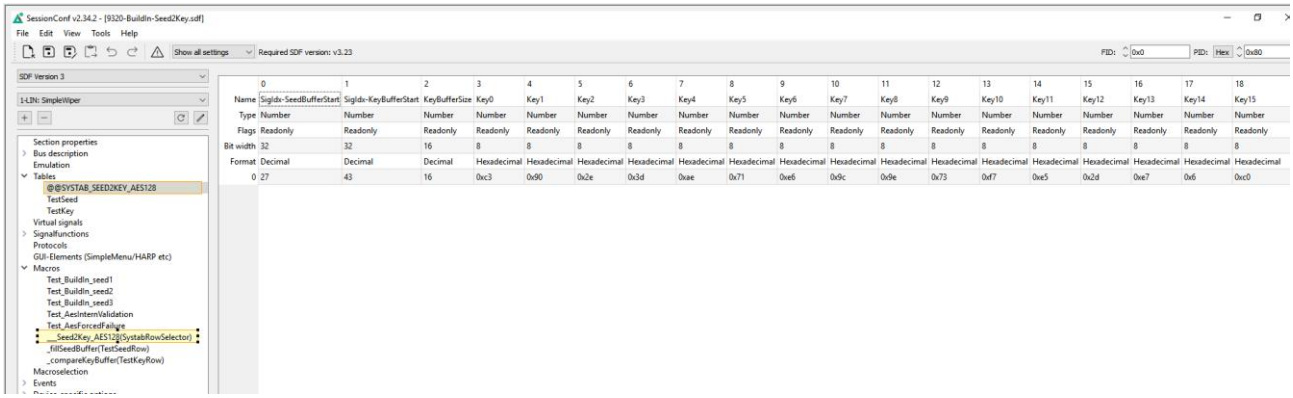
The SDF will typically contain a protocol service to get Seed from ECU and to write Key to ECU.

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 alogorithm.



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 (KeedByte0)

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.

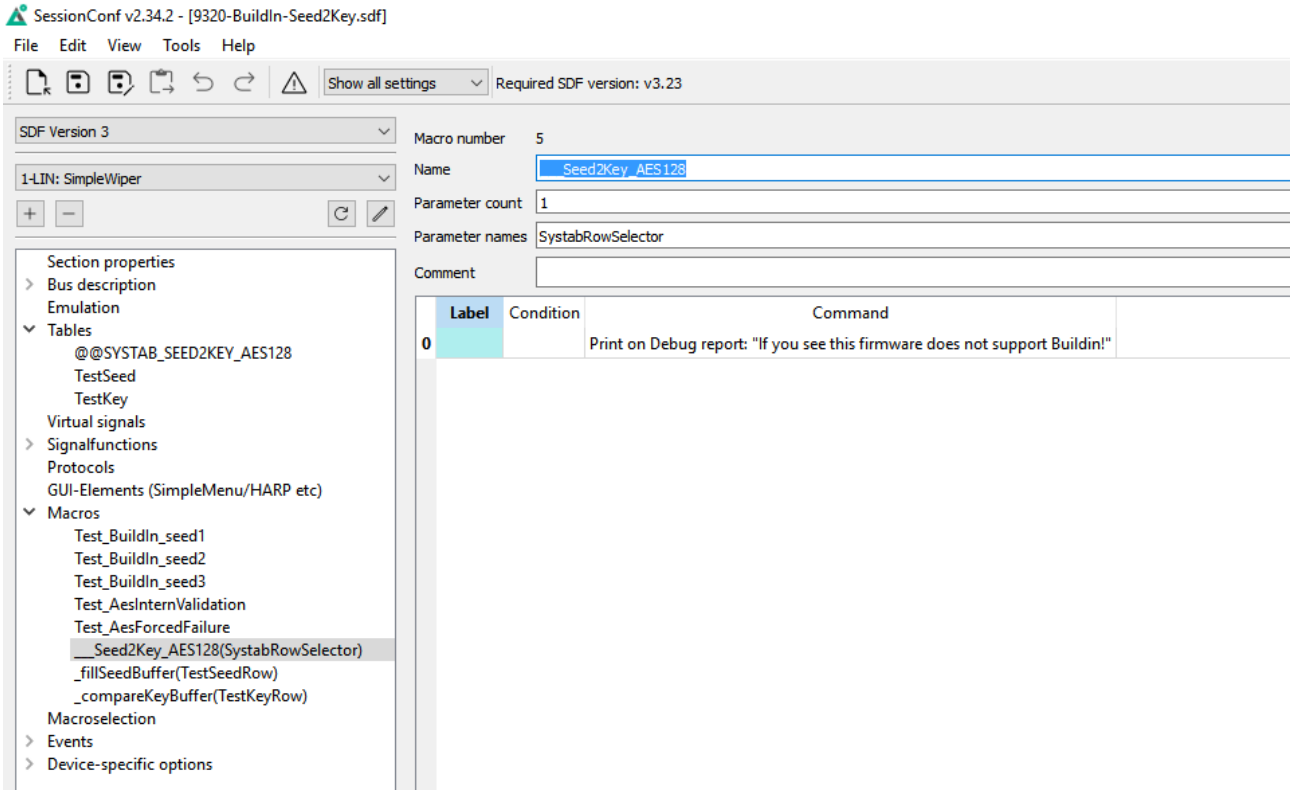
During parsing the reserved name will be recognized and the macro will be used as an entry point to call an internal firmware function.

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).



Document revision history

Date	Revision	Action	by	Comment
20.06.2023	A		al	Initial revision