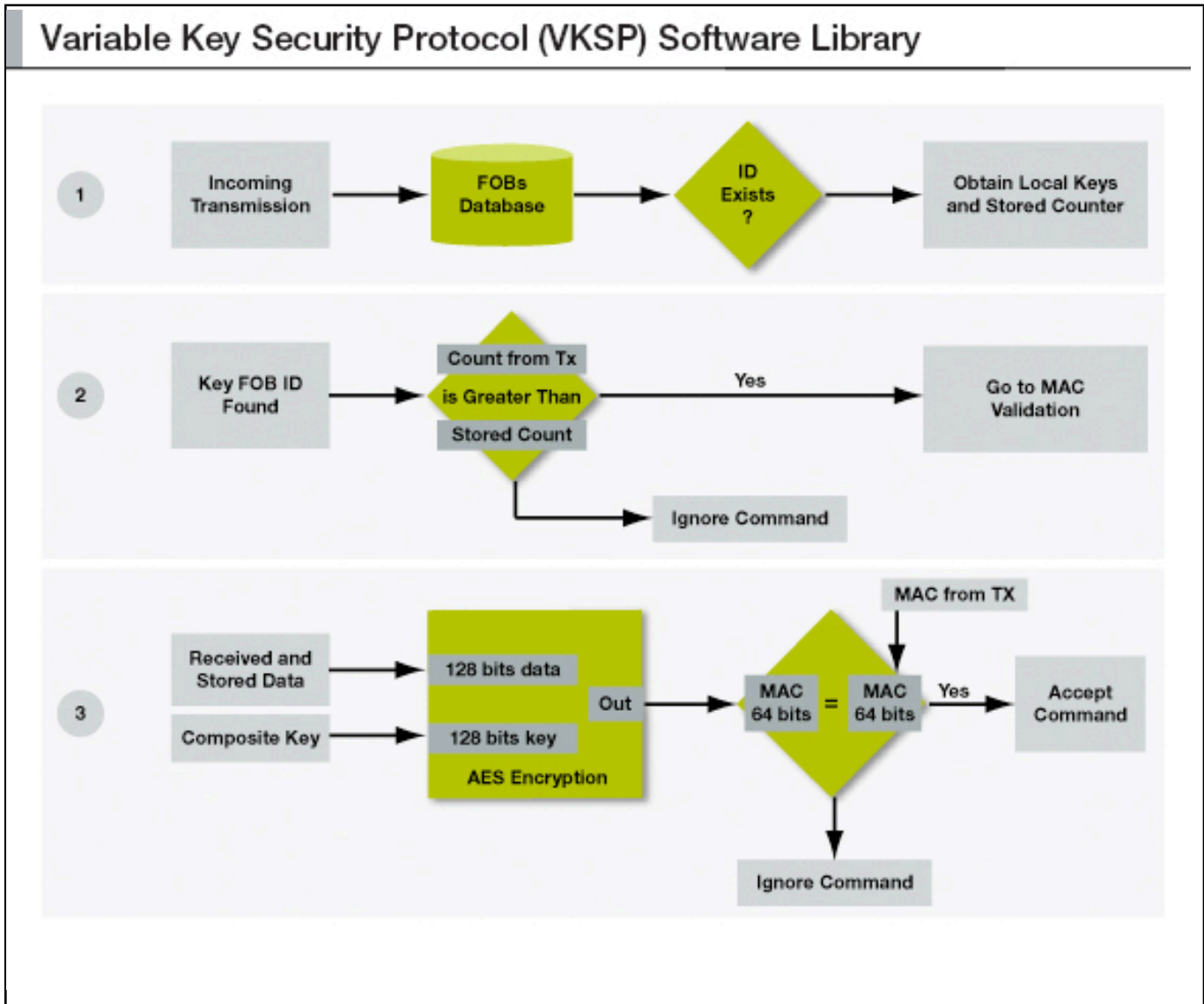# Variable Key Security Protocol (VKSP) Software Library
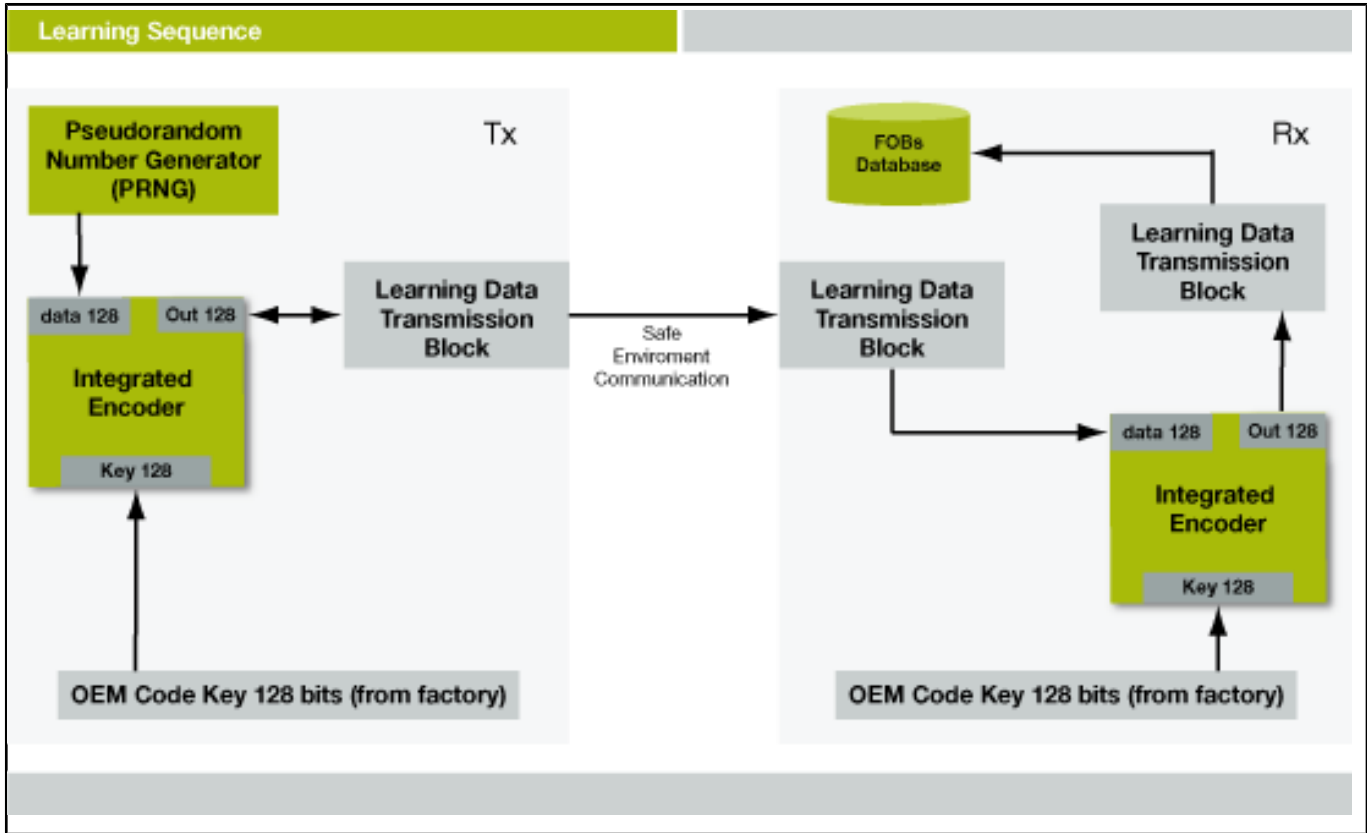
VKSP

Last Updated: Apr 8, 2022

The Variable Key Security Protocol (VKSP) Software Library from NXP® is a one-way authentication algorithm with a 128-bit key. It is ideal security for applications which require remote operation, such as remote keyless entry (RKE) systems or garage door openers.

VKSP Block Diagram Block Diagram

Variable Key Security Protocol (VKSP) Software Library

1

Incoming Transmission → FOBs Database → ID Exists ? → Obtain Local Keys and Stored Counter

2

Key FOB ID Found → Count from Tx is Greater Than Stored Count

— Yes → Go to MAC Validation

→ Ignore Command

3

Received and Stored Data → 128 bits data

Composite Key → 128 bits key

AES Encryption

Out → MAC 64 bits = MAC 64 bits ← MAC from TX

Yes → Accept Command

→ Ignore Command

VKSP Block Diagram Block Diagram

Learning Sequence

Pseudorandom Number Generator (PRNG)

Tx

data 128 | Out 128

Integrated Encoder

Key 128

Learning Data Transmission Block

Safe Enviroment Communication

Learning Data Transmission Block

OEM Code Key 128 bits (from factory)

FOBs Database

Rx

Learning Data Transmission Block

data 128 | Out 128

Integrated Encoder

Key 128

OEM Code Key 128 bits (from factory)

View additional information for Variable Key Security Protocol (VKSP) Software Library.

Note: The information on this document is subject to change without notice.

www.nxp.com