Technical Datasheet

TPR0637B

VAULTIC184 - SIGFOX SECURE ELEMENT

WISeKey

Table of Contents

1. Overview

WISeKey's VaultIC184 is a Secure Element (SE) designed to facilitate the introduction of security in Sigfox IoT devices conforming to the Sigfox "Companion Secure Element Interface Functional requirements" rev 1.6 (05/09/2018).

VaultIC184 is a tamper resistant silicon chip, based on a state-of-the-art secure microcontroller. In association with a Sigfox specific Application Programming Interface, it allows device manufacturers an easy integration of the chip. The VaultIC184 devices are delivered with preloaded Sigfox secure credentials.

The VaultIC184 secure element is intended to be used through an API embedded in a host MCU.

This document contains a quick overview of the VaultIC184 and the technical information needed to connect the VaultIC184 to a host MCU on an IoT device.

As the communication with the SE is done through the API, please refer to documents [R1] and [R2] for detailed functionality description.

1.1 VaultIC184 Features

1.1.1 Hardware

- **8/16 bits low power RISC CPU running at 36MHz**
- **Operating Ranges: from 1.62V to 5.5V**
- **16 KBytes of user non volatile memory**
  - **up to 50 years data retention**
  - **500.000 write/erase cycles at 25°C**
  - **200.000 write/erase cycles at 105°C**
- **ESD Protection ±4kV HBM on all pins**
- **ROHS compliant package QFN20.**

1.1.2 Software

- **Embeds secure firmware to:**
  - **Communicate with SE wrapper**
  - **Manage storage of secret assets**
  - **Authenticate messages**
  - **Verify downlink frames**
  - **Encrypt payload**
  - **Generate RC (Rollover Counter) synchronization frames**

1.1.3 Security

- **Dedicated Hardware for Protection Against SPA/DPA/SEMA/DEMA attacks**
- **Advanced Protection Against Physical Attacks, Including Active Shield**
- **Environmental Protection System (Voltage, Frequency, Temperature, Light Monitors)**
- **Secure Memory Management/Access Protection**

1.1.4 Interface

- **I^2C up to 400Kbps with true open drain pads**
- **7-bit addressing**
- **Programmable I^2C address**

1.1.5 Certification

- **Sigfox Verified™ (referenced S_0003_8A25_01)**

1.2 Tamper resistance

The proven technology used in VaultIC184 security module is already widespread and used in national ID/health cards, e-passports, bank cards (storing user Personal Identification Number, account numbers and authentication keys among others), pay-TV access control and cell phone SIM cards (allowing the storage of subscribers' unique ID, PIN code, and authentication to the network), where cloning must definitely be prevented. More than one billion of such microcontrollers have been already sold by WISeKey and successfully implemented in many secure systems.

WISeKey security modules will advantageously replace complex and expensive proprietary anti-tampering protection system. Their advantages include low cost, ease of integration, higher security and proven technology.

They are designed to keep contents secure and avoid leaking information during code execution. While on regular microcontrollers, measuring current consumption, radio emissions and other side channels attacks may give precious information on the processed data or allow the manipulation of the data. WISeKey microcontrollers' security features include voltage, frequency and temperature detectors, illegal code execution prevention, tampering monitors and protection against side channel attacks and probing. The chips can detect tampering attempts and destroy sensitive data on such events, thus avoiding data confidentiality being compromised.

These features make cryptographic computations secure in comparison with regular microcontrollers whose memories can be easily duplicated. It is much safer to delegate cryptographic operations and storage of secret data (keys, identifiers, etc.) to a WISeKey microcontroller.

1.3 Sigfox assets storage

As defined in the sigfox specification for secure element, the VaultIC184 contains the credentials of the device (ID, secret key, PAC) and builds the requested frames according to the sigfox protocol.
Following the sigfox specification, these assets are stored and protected by the VaultIC184:

- Device ID
- Sequence counter
- Network Authentication Key (NAK)
- Encryption Key
- CTR part U^{20}
- Encryption flag
- Rollover counter

Depending on the criticity, the above assets are protected :

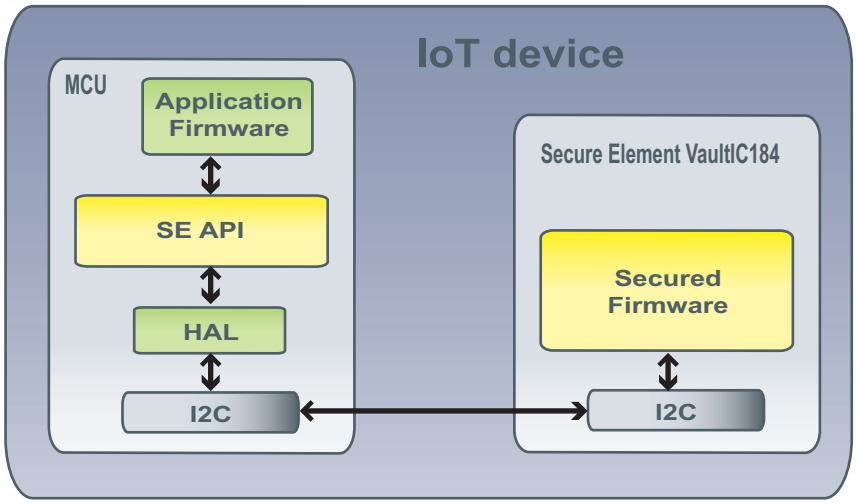
- against dumping
- against corruption (Integrity check)

Additionally, the communication bus (I^2C) is protected and the whole communication between the Host and the SE is encrypted thanks to a dedicated algorithm.

1.4 Software and Hardware Architecture

The VaultIC184 secure element includes a secured firmware and is intended to be used with a dedicated API (SE_API) embedded in a host MCU as shown on the diagram below.

Figure 1-1. Software and Hardware Architecture



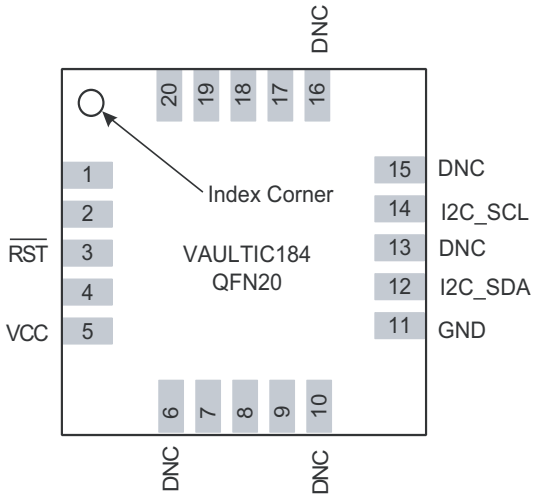
The SE (VaultIC184) and the SE API (host MCU code) are provided by WiseKey. The MCU HAL to interface with the I^2C is MCU dependant and has to be developed by the customer as explained in [R1].

2. Detailed Features

2.1 Pin & Package Configuration

2.1.1 Pinout for package QFN20

Figure 2-1. Pinout VaultIC184 - Package QFN20



2.1.2 Pin Configuration

Table 2-1. Pin List Configuration for QFN20 package

Designation	Pin number	Description
$\overline{\text{RST}}$	**3**	Reset
VCC	**5**	Power supply
-	**6**	Do not connect
-	**10**	Do not connect
GND	**11**	Ground (reference voltage)
I2C_SDA	**12**	I²C SDA
-	**13**	Do not connect
I2C_SCL	**14**	I²C SCL
-	**15**	Do not connect
-	**16**	Do not connect
Exposed pad	**Exposed pad**	Connect to GND

Caution

The pins defined as DNC (Do not connect) can be soldered on the QFN20 footprint, but they must not be connected to any signal (VCC or GND).
The pins that are not assigned can be floating or connected to GND

2.2 Communication Interface

The link between the VaultIC184 and the host MCU is done through an I²C bus as specified in [R3].

The I²C communication interfaces of the VaultIC184 can manage the following features:

- Clock line up to 400 kbps
- Clock stretching capability
  If the VaultIC184 is not ready to receive data on the I²C bus (due to internal storage, cryptographic operations...), the SCL line will be hold to the low level until next data can be received.
- 7-bit addressing
- I²C device address configurable
  The default configuration for the I²C address is 0x5F which can match any application when only one I²C slave is connected to the bus. But if needed (for example another I²C slave is connected on the bus with the same address) it is possible to change the VaultIC184 address with a specific command and update the SE API in the MCU host with this new address.

The number of devices that can be connected to the bus is only limited by the bus capacitance limit of 400 pF and the 7-bit slave address space. A detailed specification of the electrical characteristics of the I²C is given in “I²C characteristics” on page 9 where two different sets of specifications are presented: one relevant for the Standard Mode (bus speeds below 100 kHz), and one relevant for the Fast Mode (bus speed up to 400 kHz).

2.3 Supported commands

The commands supported by the VaultIC184 (transiting on the I²C bus) are only accessible through the certified Sigfox SE API provided by WiseKey.

Using the SE API, the following commands (needed for Sigfox protocol) are available:

- SE_API_init
- SE_API_open
- SE_API_close
- SE_API_get_version
- SE_API_secure_uplink_message
- SE_API_verify_downlink_message
- SE_API_get_device_id
- SE_API_get_initial_pac
- SE_API_set_rc_sync_period

Additionally a few set of command is available to get information on or to configure the VaultIC184:

- SE_API_EXT_Get_Info
- SE_API_EXT_Set_SCP_Key
- SE_API_EXT_Status_Error_Handler
- SE_API_EXT_Set_SE_Resp_Delay
- SE_API_EXT_Change_I2C_Address

The way to use these commands is fully explained in [R1]

3. Electrical characteristics

3.1 Maximum Ratings

Table 3-1. Absolute Maximum Ratings

Symbol	Parameter	Min.	Max.	Units
V_{MAX}	Maximum Voltage	0	7.5	V
T_A	Operating Temperature	-40	+105	°C
E_{EEPROM}	EEPROM Endurance for write/erase cycles		500 000 (1)	cycles
$t_{DataRetention}$	EEPROM Data Retention Virgin		50	Years
ESD	Electrostatic Discharge on all pins		±4 (HBM)	kV
Lup	Latch-up		+/- 100	mA

1. At a temperature of 25°C.

Caution

Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

3.2 AC/DC Characteristics (1.62V - 5.5V range; T= -40°C to +105°C)

3.2.1 General

Table 3-2. AC/DC Characteristics and supply monitor

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{CC}	Functional Supply Voltage		1.62		5.5	V
V_{MAX}	Voltage Monitor: High Level Detection		5.5			V
V_{MIN}	Voltage Monitor: Low Level Detection				1.62	V
T_{MON} Max	Temperature Monitor: High Level Detection		105			°C
T_{MON} Min	Temperature Monitor: Low Level Detection				-40	°C

Table 3-3. RST pad characteristics (1.62V - 5.50V range; T= -40°C to +105°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{IH}	Input High Voltage - RST		0.7*V_{CC}		V_{CC}+0.3	V
V_{IL}	Input Low Voltage - RST		-0.3		0.3*V_{CC}	V

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
I_{IH}	Leakage High Current - RST	$V_{IN} = V_{IH}$	-10		10	µA
I_{IL}	Leakage Low Current - RST	$V_{IN} = V_{IH}$	-40		10	µA
R_{RST}	Pin Pull-up RST			220		KΩ

Table 3-4. Power consumption

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
I_{uplink}	Average supply current running `SE_API_secure_uplink_message` command	Vcc=3.3V Pup_{SCL} = 1.2KΩ Pup_{SDA} = 1.2KΩ		9.12		mA

3.2.2 I²C characteristics

3.2.2.1 SCL / SDA pads

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{IL}	Input low level voltage				$0.3*V_{CC}$	V
V_{IH}	Input high level voltage		$0.7*V_{CC}$			V
V_{OL}	Low level output voltage	$2.7V < V_{CC} < 5.5V$ I_{OL}=3mA			0.4	V
		$1.62V < V_{CC} < 1.8V$ I_{OL}=2mA			$0.2*V_{CC}$	V
I_{OL}	Low level output current	V_{OL} = 0.4V	3			mA
		V_{OL} = 0.6V	6			mA

3.2.2.2 Timings

Table 3-5. I²C Timings parameters in Standard-Mode (f_{SCL} = 100kHz)

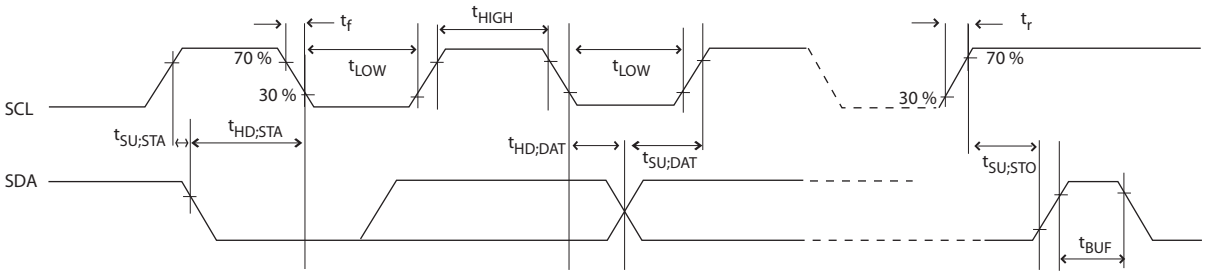
Symbol	Parameter	Condition	Min.	Max.	Units
f_{SCL}	SCL Clock Frequency		0	100	kHz
$t_{SU;STA}$	Set-Up Time for a (repeated) START Condition	f_{SCL} = 100kHz	4.7		µs
$t_{HD;STA}$	Hold Time (repeated) START Condition	f_{SCL} = 100kHz	4.0		µs
t_{LOW}	Low Period of the SCL Clock	f_{SCL} = 100kHz	4.7		µs
t_{HIGH}	High period of the SCL clock	f_{SCL} = 100kHz	4.0		µs
$t_{HD;DAT}$	Data hold time	f_{SCL} = 100kHz	0		µs
$t_{SU;DAT}$	Data setup time	f_{SCL} = 100kHz	250		ns
$t_{SU;STO}$	Setup time for STOP condition	f_{SCL} = 100kHz	4.0		µs

Symbol	Parameter	Condition	Min.	Max.	Units
$t_{VD;DAT}$	Data valid time	f_{SCL} = 100kHz		3.45	µs
$t_{VD;ACK}$	Data valid acknowledge time	f_{SCL} = 100kHz		3.45	µs
t_{BUF}	Bus free time between a STOP and a START condition	f_{SCL} = 100kHz	4.7		µs

Table 3-6. I²C Timings parameters in Fast-Mode (f_{SCL} = 400kHz)

Symbol	Parameter	Condition	Min.	Max.	Units
f_{SCL}	SCL Clock Frequency		0	400	kHz
$t_{SU;STA}$	Set-Up Time for a (repeated) START Condition	f_{SCL} = 400kHz	0.6		µs
$t_{HD;STA}$	Hold Time (repeated) START Condition	f_{SCL} = 400kHz	0.6		µs
t_{LOW}	Low Period of the SCL Clock	f_{SCL} = 400kHz	1.3		µs
t_{HIGH}	High period of the SCL clock	f_{SCL} = 400kHz	0.6		µs
$t_{HD;DAT}$	Data hold time	f_{SCL} = 400kHz	0		µs
$t_{SU;DAT}$	Data setup time	f_{SCL} = 400kHz	100		ns
$t_{SU;STO}$	Setup time for STOP condition	f_{SCL} = 400kHz	0.6		µs
$t_{VD;DAT}$	Data valid time	f_{SCL} = 400kHz		0.9	µs
$t_{VD;ACK}$	Data valid acknowledge time	f_{SCL} = 400kHz		0.9	µs
t_{BUF}	Bus free time between a STOP and a START condition	f_{SCL} = 400kHz	1.3		µs

Figure 3-1. I²C timings chronogram



Note

Parameters t_f and t_r depend on the Host.

3.3 Power-on sequence

To start the chip, the Vcc shall be first applied.

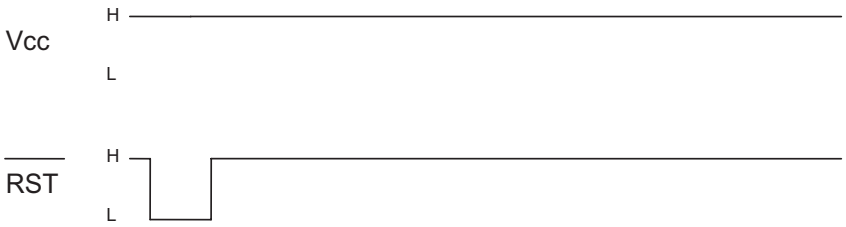
Optionally, the $\overline{RST}$ signal can be held low by the master while Vcc goes to high level. In this case, the CPU will start when the $\overline{RST}$ is released to high level.

A Power-on Reset internal circuitry ensures that the CPU is not started until Vcc has reached a minimum level.

3.4 Reset sequence

A chip reset is generated by a low level on the $\overline{RST}$ pin: the $\overline{RST}$ pin must be held low for at least 2 µs.

Figure 3-2. External reset sequence



3.5 Typical Applications

3.5.1 Typical application without VCC control

This schematic fits well IoT devices without severe power consumption constraints.

In this case, the reset pin of the Secure Element has to be controlled, to be able to recover from a security error detection.

Figure 3-3. VaultIC184 connection without VCC control

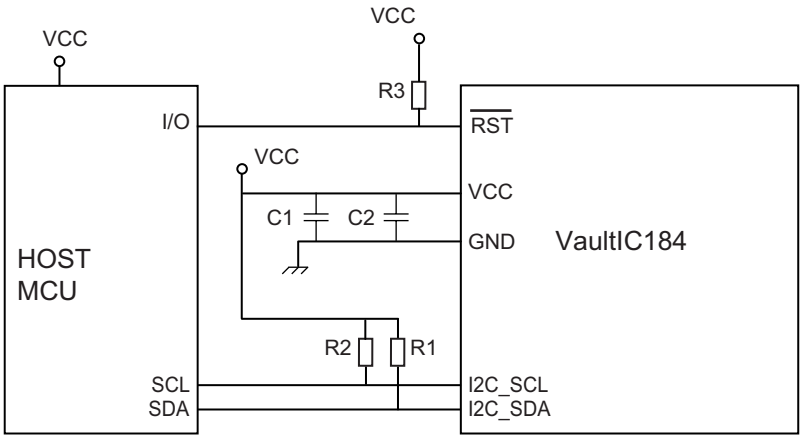


Table 3-7. External components, Bill of Materials

Reference	Description	Typ.Value	Comment
R1, R2	Pull-Up Resistors	2.2 kΩ	Dependant of I^2C charge
R3	Pull-Up Resistor	10 kΩ	Recommended
C1	Power Supply Decoupling Capacitor	4.7 µF	Recommended
C2	Power Supply Decoupling Capacitor	10 nF	Recommended

3.5.2 Typical application with VCC control

If the power consumption of the IoT device is a priority, the following schematic should be used:

Figure 3-4. VaultIC184 connection with VCC control

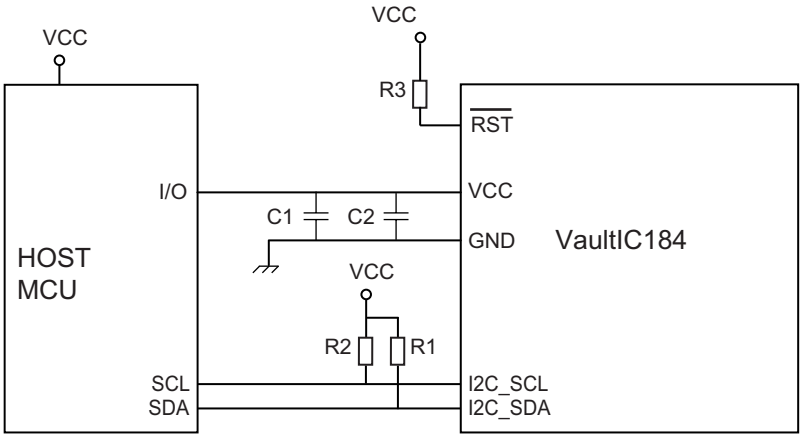


Table 3-8. External components, Bill of Materials

Reference	Description	Typ.Value	Comment
R1, R2	Pull-Up Resistors	2.2 kΩ	Dependant of I^2C charge
R3	Pull-Up Resistor	10 kΩ	Recommended
C1	Power Supply Decoupling Capacitor	4.7 µF	Recommended
C2	Power Supply Decoupling Capacitor	10 nF	Recommended

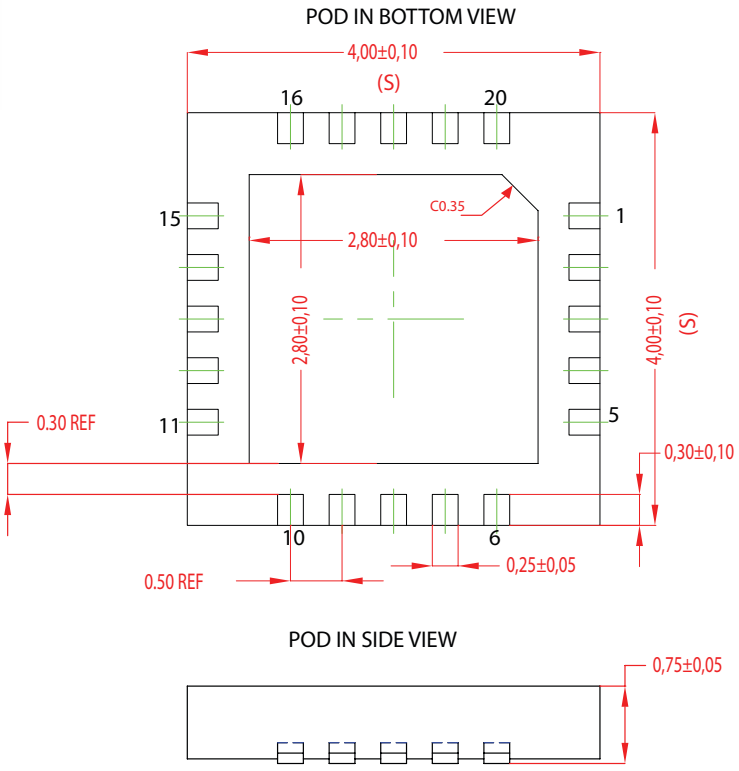
Caution

In this schematic, the I/O of the host MCU must be able to provide the required current for the VaultIC184, otherwise a specific VCC command transistor or power management device must be used.

4. Package characteristics

4.1 Package outline

Figure 4-1. QFN-20 package outline



NOTES:

1. ALL DIMENSIONS ARE IN mm. ANGLES IN DEGREES
2. COPLANARITY APPLIES TO THE EXPOSED PAD AS WELL AS THE TERMINALS. COPLANARITY SHALL NOT EXCEED 0.08 mm.
3. WARPAGE SHALL NOT EXCEED 0.10 mm.
4. PACKAGE LENGTH/ PACKAGE WIDTH ARE CONSIDERED AS SPECIAL CHARACTERISTIC.(S)
5. REFER JEDEC MO-220.

4.2 Product Marking

Figure 4-2. QFN20 marking

VaultIC versionning
XXXXXX : Lot Number
YYWW : Date Code

Note

Engineering samples may be marked VIC407 instead of VIC184

5. Ordering information

5.1 Legal

A **Non-Disclosure Agreement** must be signed with WISeKey.

An **Export License** for cryptographic hardware/software must be granted.

5.2 Quotation and Volume

For minimum order quantity and annual volume, please contact your local WISeKey sales office.

5.3 Part Numbers

Reference		Description
VAULTIC184E-001-Z1T		Sigfox Secure Element part in QFN20 package
Reference	**Application**	**Description**
VAULTIC-STK12-184ZA	Sigfox Security	Starter Kit for Sigfox Secure Element in QFN20 package

5.4 Starter Kit

The Sigfox Starter Kit provides an easy path to test and integrate a high level of security in a Sigfox module.
Contents:

- 1 demonstration board with a VaultIC184 Secure Element packaged in QFN20
- 1 board with a host MCU (used to communicate with the VaultIC184)
- 1 USB cable
- 1 USB-key containing a support documentation set (getting started, application notes, reference design), some demo applications to get an insight into the VaultIC184 features.

Please refer to [R2] for full description of the starter kit and the way to use it.

Figure 5-1. Sigfox Starter kit - Contents.

Definitions and abbreviations

AES	Advanced Encryption Standard algorithm
CPU	Central Processing Unit
Cryptographic key	A bit string used as a secret parameter by a cryptographic algorithm. To prevent a key from being guessed, keys need to be generated truly randomly and contain sufficient entropy.
EEPROM	Electrically Erasable Programmable Read-Only Memory
HAL	Hardware Abstract Layer - Hardware specific software used to link hardware and software
Host	Entity that communicates (directly or not) with the device.
I^2C	Inter Integrated Circuit Bus
Integrity	The property that received data has not been altered
Master	The device that initiates and terminates a transmission. The Master also generates the clock for synchronous interface.
MCU	MicroController Unit
NAK	Network Authentication Key
OS	Operating Systems
Provisioning	Activity consisting in loading/generating user credentials, cryptographic keys, identifiers into an equipment
SE	Secure Element
Slave	The device addressed by a master
Wrapper	Set of functions used to encapsulate more complex and/ or lower level functions

Referenced Documents

[R1] Sigfox SE API integration - compiled HTML file (.chm) present in the Kit
[R2] TPR0645 Getting started with VaultIC184 - PDF file present in the kit
[R3] UM10204 - I^2C-bus specification and user manual - Re. 6 - 4 April 2014

Datasheet Revision History

- **Rev. TPR0637B- 09Mar20**
  - Change document access from WCP to GBU
  - Update ESD protection, typical applications schematics, package marking
  - Minor corrections
- **Rev. TPR0637A - 14Feb20**
  - First Release

Headquarters

WISeKey
Arteparc de Bachasson - Bat A
Rue de la Carrière de Bachasson
CS 70025
13590 Meyreuil - France
Tel: +33 (0)4-42-370-370
Fax: +33 (0)4-42-370-024

Product Contact

Web Site
www.wisekey.com

Technical Support
dl_e-security@wisekey.com

Sales Contact
sales@wisekey.com