KUDELSKI SECURITY

Sigfox

Security Assessment on Devices

Framework and Lab deliveries

KUDELSKI SECURITY

31.03.2017

DOCUMENT PROPERTIES

Version:	1.0
File name:	Sigfox - Security Assessment on Devices - Framework and Lab deliveries v1.2.docx
Publication date:	31.03.2017
Confidentiality Status:	Confidential
Document Owner:	Jullian Stéphane
Document Recipient:	Melia Telemaco
Document Status:	Proposal
Client Company Name:	Sigfox

TABLE OF CONTENTS

TABLE OF TABLES

EXECUTIVE SUMMARY

This document is intended for the manufacturers of devices who are partners of Sigfox and whose chipset implements security features required by Sigfox. Kudelski Security Laboratories will perform security assessments based on these requirements and the targeted security level.

The purpose of this document is to provide to those partners a detailed description of the framework and material required by Kudelski Security for the different security assessments scenarios.

The Device Manufacturer should check that a candidate device follows the best current security practices issued by Sigfox before submitting to a security assessment.

INTRODUCTION

In order to execute the test scenarios needed during the security evaluation of the device, Kudelski Security requests the Device Manufacturer to provide some test materials, including documents, hardware and software items. All these test materials shall be provided by the Device Manufacturer (DM), and the list is presented into this document:

- List of Material for Security assessment on Sigfox devices (section 2):
  - Generic Documents (1.2)
  - Security Documents (1.3)
  - Hardware samples(1.4)

Using this document together with the Sigfox security guidelines, the Device Manufacturer will be able to prepare the security assessment phase and to provide Kudelski Security Labs with all the necessary "ready-to-use", test application, tools and hardware samples, allowing the stake holders to execute the security assessment in a quick and efficient way.

SECURITY ASSESSMENT LEVELS

Depending on the security assessment scenarios the list of mandatory material may vary.

At the publication date for this document, the different security levels are:

- Basic - Minimum security level
    - 5 MD security evaluation effort
    - Mandatory level for Sigfox modules without secure elements
- Medium - Intermediate security level
    - 15 MD security evaluation effort
    - Complementary tests as Fault by Glitch or Simple Side Channel could be performed by the security lab.
- Advanced - Custom security evaluations
    - Aimed at critical applications with a secure element. Advanced techniques could be used like Fault (Laser/EM) or Side channel attacks. Attack scenarios will be defined on a case by case basis with the Device Manufacturers.
    - Software security code audit on critical applications could be performed by the security lab.
- CSPN – Security certification delivered by ANSSI (French security certification authority)
    - 35 MD evaluation effort
    - KS security labs will execute the security tests so as to get this security certification. A pre-assessment phase could be proposed to the Device Manufacturer so as to estimate the security level before starting this certification.
    - KS lab could provide support to the Application providers or Device Manufacturers so as to write the Security Target document needed for the CSPN certification.

1. LIST OF MATERIAL FOR SECURITY ASSESSMENT

This section describes the overall material, per scenario, needed to complete the security evaluation activities. This material includes the documents to be provided in order to fulfil the various assessment phases such as generic documents, security documents and some other documents, to be exchanged between Kudelski Security Laboratories and the Device Manufacturer.

Apart from these documents the Device Manufacturer shall provide the hardware items (described in Section 2.4) and tools (described in Section 2.6) used during the security evaluation.

1.1. Prerequisites for the Security Assessment on Devices

Before entering the security evaluation phase, it is mandatory that the following steps have been completed:

- The “Best Current Practice Document” document has been fully understood by the Device Manufacturer. All needed technical and security related documentations as specified in the next sections have been provided to KS.
- The complete answers to the questions presented in the “Technical & Test Material Questionnaire” have been provided to Kudelski Security labs.
- A meeting between the KS Security Lab and the Device Manufacturer has been held to rule out misunderstandings on the answers provided in the “Technical & Test Material Questionnaire”. This meeting will also cover the implementation of the security mechanisms.

1.2. Generic Documents

The following table describes the list of required generic documents as per the Sigfox device security levels. DM stands for Device Manufacturer, KS for Kudelski Security.

Asset Name	Doc source	Security assessment scenario		
		Basic	Medium	Advanced
Device datasheet	DM	Yes	Yes	Yes
Device user manual	DM	Yes	Yes	Yes
Device architecture overview	DM	Yes	Yes	Yes
Debug Interfaces	DM	Yes	Yes	Yes
Technical & Test material Questionnaire	DM	Yes	Yes	Yes

Table 1 - Generic documents

1.3. Documents for Secure Element

The following table describes the list of the required documents as per the certification scenarios. SE stands for Secure Element, CC for Common Criteria, CM for Chipset Manufacturer.

Asset Name	Doc source	Security assessment scenario		
		Basic	Medium	Advanced
SE Security Architecture Overview	DM	-	Yes	Yes
SE datasheet	DM	-	-	Yes
CC certified SE TOE document	CM	-	-	Yes

Table 2 - Security documents

1.4. Hardware Items

The hardware items include the test devices and the debug interface probes. It also includes any specific item required for the test platform environment.

1.4.1. Samples for security assessment

It is sufficient and even desirable to have devices for security evaluation in a “small form factor”. Devices can be provided in a standalone board or final device form.

The minimum number of test device is mentioned in the table below:

Asset Name	Security assessment scenario		
	Basic	Medium	Advanced
Number of devices	3	5	10

Table 3 - Number of samples for the security lab

As some of the attacks carried out in the Advanced security evaluation case could require direct access to the chip’s surface or as some of the security evaluation tests can be destructive, the security lab could need a certain number of spare devices as well.

1.4.2. Generic configuration of devices

The hardware revision, software revision should be clearly identified and related information provided in the technical questionnaire. The devices provided to the KS lab should be provided in production configuration.

A simple test application allowing communication with Sigfox infrastructure should be available on the tested samples and these devices should be registered and recognized by the Sigfox infrastructure.

KS labs should be able to have access to messages transmitted / received by the test devices using the Sigfox portal.

1.4.3. Specific configuration of devices

The Advanced security evaluations scenario could require modifications of the devices to access trigger signals, change power supplies, etc. Such a specific configuration will be discussed with the Device Manufacturer when defining the evaluations scope.

In order to prepare these modifications and to identify difficulties before the proper security evaluation phase, Kudelski Security evaluation team may need access to dummy devices in advance.

1.4.4. Debug Interface Probe / JTAG

In order to test all Debug Interface protections or upload and execute test application software, KS needs an appropriate Debug Interface probe including the device manufacturer software for each available debug port.

Such probe should include:

- All the necessary hardware to connect the Host PC to the test device.
- The drivers and software components needed to use the debug probe with the Host Virtual Machine

Note: KS supports the following OS: Windows XP Pro, Windows 7, Windows 10, GNU Linux Ubuntu distribution, GNU Linux Fedora distribution.

2. SECURITY ANALYSIS FRAMEWORK

This section details the projected workflow at KS Labs for each level of security assessment scenario.

2.1. Security evaluation common framework

1. A KS commercial standard offer for a Basic / Medium / Advanced security assessment is accepted by the Device Manufacturer.
2. A NDA is signed between Kudelski Security and the Device Manufacturer.
3. The device has received a functional certification by Sigfox.
4. A planning for the security assessment is defined between KS lab and the Device Manufacturer.
5. A meeting will take place between the Device Manufacturer and KS lab to answer questions and ensure that all items listed in section 1 are available.
6. All documents and device samples are sent one week before the start of the security assessment phase to KS lab.
7. Paper analysis phase: All documents provided will be analysed by KS lab.
8. Functional tests are performed on devices, to check the standard interfaces and API.
9. Basic security level:
    a. Simple security manipulations will be performed, it could include:
        i. Non-volatile memory (NVM) content extraction
        ii. Tests on debug interfaces (JTAG, USB…)
        iii. Physical manipulations on device board
        iv. Other tests

10. Medium security level:
    a. Complementary tests to Basic level will be performed, possibly including:
        i. Simple Power Analysis
        ii. Glitch analysis
    b. A status meeting will be scheduled mid-test.

11. Advanced security level:
    a. Complementary tests to Basic level will be performed, possibly including:
        i. Side channel: Simple Power Analysis, Differential Power Analysis, Electromagnetic field measurements
        ii. Fault injection: Electrical glitch, Laser fault injection, Electromagnetic fault injection
        iii. Hardware analysis: Circuit edit, Reverse Engineering, Probing
    b. A status meeting will be scheduled mid-test.

12. A report is published summarizing the test findings and describing suggested mitigation means.

13. An optional post-analysis meeting can be scheduled if the client has any further question.

DOCUMENT HISTORY

Version	Status	Date	Authors	Comments
v.1.0	Proposal	**31.03.2017**	**Stephane Jullian**	Initial version

Reviewer	Position	Date	Document Version
Dominique Le Floch	Principal Security Engineer	31.03.2017	V1.0
Gerrit Holtrup	Senior Security Engineer	31.03.2017	V1.0

Approver	Position	Date	Document Version
Benoit Gerhard	Head of Security Evaluation and Attacks		

DOCUMENT RECIPIENTS

Name	Position	Contact Information
David Fernandez	Project Manager	David.Fernandez@Sigfox.com

KUDELSKI SECURITY CONTACTS

Name	Position	Contact Information
MELIA Telemaco	Business Development Manager	Telemaco.melia@kudelskisecurity.com

REFERENCES

[1] A new reference
[2] Document Title / Author / Date
[3] Yet another reference
[4] …
[5] Dsdsd
[6] Sdsdsd
[7] sdsd

ACRONYMS

Acronym	Stands for	Definition

ANNEXES

Just add annexes to your convenience.