SE050

SE050 Errata sheet

Rev. 1.0 — 14 October 2020 **Errata sheet**

640310

Document information

Information	Content
Keywords	SE050
Abstract	This document contains known issues with the SE050 and their workaround.

Revision History

Rev	Date	Description
640310	2020-10-14	Initial version

1 Product Information

The SE050 product identification can be obtained out by sending a dedicated command to the secure element.

The Plug & Trust Middleware (nxp.com) includes a utility called ‘se05x_GetInfo’ to retrieve detailed product information from the connected SE050 derivative. It is available as a Windows binary (binaries\ex\VCOM-se05x_GetInfo.exe) and in source code. The html documentation included with the Plug & Trust Middleware package (section ‘Demo & Examples’ > ‘SE05X Get Info example’) provides additional information on using and compiling the utility.

The information retrieved by se05x_GetInfo is a superset of what is required to determine whether an entry in the errata sheet is applicable to the product.

The exact product identification is covered by two parameters:

- The product OS configuration (Platform build ID) in the format JXXXXXXXXXXXXXXX. Example below : `J3R351021EEE0400`
- The version of the Applet in the format xx.xx.xx (major.minor.patch). Example below: 3.1.0

```
C:\<MW install Dir>\binaries\ex>VCOM-se05x_GetInfo.exe
COM<port>
App   :INFO :PlugAndTrust_v03.00.04_20200928
App   :INFO :Running se05x_GetInfo.exe
App   :INFO :Using PortName='COM<port>' (CLI)
Opening COM Port '\\.\COM<port>'
sss   :INFO :atr (Len=35)
      00 A0 00 00    03 96 04 03    E8 00 FE 02    0B 03 E8 08
      01 00 00 00    00 64 00 00    0A 4A 43 4F    50 34 20 41
      54 50 4F
App   :WARN :No SemsLite Applet Available.
App   :INFO :Running se05x_GetInfo.exe
App   :INFO :Using PortName='COM<port>' (CLI)
Opening COM Port '\\.\COM34'
sss   :INFO :atr (Len=35)
      00 A0 00 00    03 96 04 03    E8 00 FE 02    0B 03 E8 08
      01 00 00 00    00 64 00 00    0A 4A 43 4F    50 34 20 41
      54 50 4F
sss   :WARN :Communication channel is Plain.
sss   :WARN :!!!Not recommended for production use.!!!
App   :WARN :#####################################################
App   :INFO :uid (Len=18)
      04 00 50 01    43 E7 C2 90    7A BD 8B 04    42 0A 59 55
      00 00
App   :WARN :#####################################################
App   :INFO :Applet Major = 3
App   :INFO :Applet Minor = 1
App   :INFO :Applet patch = 0
App   :INFO :AppletConfig = 6FFF
App   :INFO :With ECDAA
App   :INFO :With ECDSA_ECDH_ECDHE
App   :INFO :With EDDSA
App   :INFO :With DH_MONT
App   :INFO :With HMAC
App   :INFO :With RSA_PLAIN
App   :INFO :With RSA_CRT
App   :INFO :With AES
App   :INFO :With DES
App   :INFO :With PBKDF
App   :INFO :With TLS
App   :INFO :With MIFARE
App   :INFO :With I2CM
App   :INFO :Internal = 010B
App   :WARN :###########################################
App   :INFO :Tag value - proprietary data 0xFE = 0xFE
App   :INFO :Length of following data 0x45 = 0x45
App   :INFO :Tag card identification data (Len=2)
      DF 28
App   :INFO :Length of card identification data = 0x42
App   :INFO :Tag configuration ID (Must be 0x01) = 0x01
App   :INFO :Configuration ID (Len=12)
      00 04 A1 F4    45 88 4F 17    E5 19 C0 69
App   :INFO :OEF ID (Len=2)
      A1 F4
App   :INFO :Tag patch ID (Must be 0x02) = 0x02
App   :INFO :Patch ID (Len=8)
      00 00 00 00    00 00 00 01
App   :INFO :Tag platform build ID1 (Must be 0x03) = 0x03
App   :INFO :Platform build ID (Len=24)
      4A 33 52 33    35 31 30 32    31 45 45 45    30 34 30 30
      BC 03 04 79    33 8D 18 10
App   :INFO :JCOP Platform ID = J3R351021EEE0400
App   :INFO :Tag FIPS mode (Must be 0x05) = 0x05
App   :INFO :FIPS mode var = 0x00
App   :INFO :Tag pre-perso state (Must be 0x07) = 0x07
App   :INFO :Bit mask of pre-perso state var = 0x00
App   :INFO :Tag ROM ID (Must be 0x08) = 0x08
App   :INFO :ROM ID (Len=8)
      2E 5A D8 84    09 C9 BA DB
App   :INFO :Status Word (SW) (Len=2)
      90 00
App   :INFO :se05x_GetInfoPlainApplet Example Success !!!...
App   :WARN :############################################
App   :INFO :cplc_data.IC_fabricator (Len=2)
      47 90
App   :INFO :cplc_data.IC_type1 (Len=2)
      D3 21
App   :INFO :cplc_data.Operating_system_identifier (Len=2)
      47 00
App   :INFO :cplc_data.Operating_system_release_date (Len=2)
      00 00
App   :INFO :cplc_data.Operating_system_release_level (Len=2)
      00 00
App   :INFO :cplc_data.IC_fabrication_date (Len=2)
      91 69
App   :INFO :cplc_data.IC_Serial_number (Len=4)
      00 03 23 95
App   :INFO :cplc_data.IC_Batch_identifier (Len=2)
      36 73
App   :INFO :cplc_data.IC_module_fabricator (Len=2)
      00 00
App   :INFO :cplc_data.IC_module_packaging_date (Len=2)
      00 00
App   :INFO :cplc_data.ICC_manufacturer (Len=2)
      00 00
App   :INFO :cplc_data.IC_embedding_date (Len=2)
      00 00
```

```
App   :INFO :cplc_data.IC_OS_initializer (Len=2)
      01 42
App   :INFO :cplc_data.IC_OS_initialization_date (Len=2)
      0A 30
App   :INFO :cplc_data.IC_OS_initialization_equipment (Len=4)
      30 33 32 33
App   :INFO :cplc_data.IC_personalizer (Len=2)
      00 00
App   :INFO :cplc_data.IC_personalization_date (Len=2)
      00 00
App   :INFO :cplc_data.IC_personalization_equipment_ID (Len=4)
      00 00 00 00
App   :INFO :cplc_data.SW (Len=2)
      90 00
App   :INFO :ex_sss Finished
```

2 Errata Overview

Table 1. Functional problems table

Functional problems	Short description	Platform build ID	Applet and Applet version affected	Detailed description
Secure element / I^2C lock-up in case of erroneous APDU sequence	I^2C.1	J3R351021EEE0400 and J3R3510264571100	All SE050 variants (A,B,C,D) are affected	Section 3.1
SE050 get unresponsive after sending empty I^2C frame	I^2C.2			Section 3.2
Security reset during startup	I^2C.3			Section 3.3
Timings for the edges on the I^2C bus	I^2C.4			Section 3.4
The IoT Applets attestation feature can attempt to return a message larger than its response buffer	APP.1			Section 3.5
SE050 IoT applet session close	APP.2			Section 3.6
Specified maximum attempts read as 0x00 in attested read of UserID object	APP.3			Section 3.7
PRF function fails for master secret when used with SHA384	APP.4			Section 3.8
Incomplete UserID check on VerifySesionUserID	APP.5		SE050 applet up to version 3.1.0	Section 3.9
HKDF can be used in Extract-And-Expand mode as well as in Expand-Only mode	APP.6		All SE050 variants (A,B,C,D) are affected	Section 3.10
Read with attestation using a key with Origin EXTERNAL	APP.7			Section 3.11
SE050 goes to security reset when invalid EC key is used	JOS.1			Section 3.12
SCP03 - maintenance of the encryption counter for APDUs without C-DATA	JOS.2			Section 3.13

3 Functional problems details

3.1 I^2C.1: Secure element / I^2C lock-up in case of erroneous APDU sequence

3.1.1 Introduction

T1oI2C and UM11225 [1] protocols rely on alternating Command-APDU response-APDU data pairs. Before the secure element receives a new Command-APDU the previous Response-APDU needs to be fetched entirely.

3.1.2 Problem

In scenarios where the command response sequence is not respected by the host side, e.g. sending 2 command-APDUs subsequently to the secure element (without fetching the response APDU) the secure element may start permanent clockstretching until it is being power cycled.

In case clock stretching is enabled (by default on types A,B,C,D) and the first 4 bytes of the second APDU will be received within 560 µs the secure element will start clock stretching SCL permanently (which will also interfere with other devices on the same I^2C bus) until the SE050 is power cycled.

In case clock stretching is disabled usually a R-block response indicating an error from the secure element will be answered on the second APDU (which will be recovered by regular protocol handling).

3.1.3 Workaround

Ensure the response is fully read from the secure element before sending the next command-APDU. This is especially important when the host is reset independently of the secure element or used in multi-threaded/multi-processing applications. Independently of the secure element, ensure the host/SE command response sequence is synchronized.The deadlock in case of a host reset can be prevented by ensuring to send a read command to the secure element after starting up the host. The deadlock, when occurred, can be resolved only by a power cycle.

Note: *Workaround to avoid independent host rest scenario is implemented in all NXP Plug & Trust Middleware releases covering SE050. In multi-processing cases the AccessManager from NXP Plug&Trust has to be used. Multi-threaded access is handled for RTOS and Linux from version 03.00. Multi-process access control is planned to be available Q1/2021.*

3.2 I^2C.2: SE050 get unresponsive after sending empty I^2C frame

3.2.1 Introduction

In scenarios of detecting I^2C ICs on the bus using an empty I^2C frame containing only the address the SE050 will block the I^2C bus.

3.2.2 Problem

When sending an empty I^{2}C frame which contains only the slave address but no data (I^{2}C Start, SE050-Slave-Address, I^{2}C Stop Condition) the SE050 will start permanent clockstretching after receiving six additional bytes.

3.2.3 Workaround

Ensure every acknowledged I^{2}C frame addressed to SE050 contains at least one byte of data or ensure the capability to power cycle the SE050 on V_{cc} (e.g. send to Deep Power Down and wake up again using toggling the ENA pin as described in UM11225 [1]).

Note: *The NXP Plug & Trust MW does not send such probing requests.*

3.3 Security reset during startup

3.3.1 Introduction

I^{2}C lines SDA and SCL have to be pulled high via a pullup resistor to have the default state high. SE050 detects that the I^{2}C on startup if the interface is active based on the level of SDA/SCL.

3.3.2 Problem

In case of an interface soft reset S-Block JCOP will restart an interface detection. If any of SDA or SCL are default low on host side the interface detection will not be able to detect the active interface and will trigger an security reset after ~1 s. The device will only lock itself permanently when multiple error events are happening in a row. Any successful selection of the applet will reset the error condition in the SE050.

3.3.3 Workaround

Leave I^{2}C lines in default state high as mandated by the I^{2}C standard (UM10204, see [3]). Especially in case the host sends a Interface soft reset S-Block request set both I^{2}C lines to high state for at least 1 ms or wait until the host receives Interface soft reset S-Block response before sending new I^{2}C requests

3.4 I^{2}C.4: Timings for the edges on the I^{2}C bus

3.4.1 Introduction

UM10204 (see [4]) defines timings for the edges on the I^{2}C bus.

3.4.2 Problem

During data transfer SDA is only allowed to change when SCL is low. UM10204 allows timing down to 0ns difference. SE050 needs SCL to change before SDA with a small margin.

3.4.3 Workaround

Ensure to switch SCL before SDA with the timings as defined in the SE050 datasheet (see [4]) section 14.3, "I2C Bus Timing Specification".

3.5 APP.1: The IoT Applets attestation feature can attempt to return a message larger than its response buffer

3.5.1 Introduction

The IoT Applet according to its specification [2] is limited to a maximum Response-APDU length of 1024 bytes.

3.5.2 Problem

When the resulting Response-APDU becomes larger than this limit, including protocol and session overhead, the error code SW_CONDITIONS_NOT_SATISFIED is returned instead.

This is a limiting factor in the attestation use case. The attested data and its appended signature can result in this behavior. The attestation signature length depends on the algorithm used for the attestation.

3.5.3 Workaround

Ensure that the maximum response length stays under 1024 bytes by e.g. avoiding cryptographic algorithms with very large signature length for attestation. Example: use ECC instead of RSA3K, RSA4 for attestation.

3.6 APP.2: SE050 IoT applet session close

3.6.1 Introduction

SE050 supports users sessions which can be opened and closed separately in order to maintain parallel connections of different users to the SE050.

3.6.2 Problem

After calling closeSession without session (in the default session) the applet will respond with error code 6985. All following commands will all return error 6985 altough they get executed.

3.6.3 Workaround

In case of an error returned from closeSession re-select the applet resp. restart the MW. When starting the MW the applet always gets selected first.

Note: *NXP Plug & Trust MW prevents sending closeSession when no session is open starting from version 03.00*

3.7 APP.3: Specified maximum attempts read as 0x00 in attested read of UserID object

3.7.1 Introduction

Authentication objects can get an authentication attempts counter set to limit the amount of failed authentications. The value of this counter is available in the object attributes which can be read using an attested read.

3.7.2 Problem

The authentication attempts counter of the object attributes is not reported for UserID on an attested read (the attribute value remains 0).

3.7.3 Workaround

In case reading the counter value is needed, use an AESkey object for authentication instead.

3.8 APP.4: PRF function fails for master secret when used with SHA384

3.8.1 Introduction

With TLSPerformPRF the wanted DigestMode can be selected

3.8.2 Problem

Only DigestModes DIGEST_SHA and Digest_SHA256 are available on SE050.

3.8.3 Workaround

No workaround. SE050 APDU Specification 2.12 contains corrected specification. SE051 will provide support for more DigestMode parameters.

3.9 APP.5: Incomplete UserID check on VerifySesionUserID

3.9.1 Introduction

UserID checks if it matches a stored value in order to open a session.

3.9.2 Problem

Up to applet version 3.1.0 the check of the UserID is incomplete and can pass even if wrong value is supplied.

3.9.3 Workaround

Don't rely on UserID when using Applet version 3.1.0 or ensure to use at minimum applet version 3.1.1.

3.10 APP.6: HKDF can be used in Extract-And-Expand mode as well as in Expand-Only mode

3.10.1 Introduction

APDU specification 2.3 and earlier versions mentioned that HKDF can be used in Extract-And-Expand mode as well as in Expand-Only mode.

3.10.2 Problem

HKDF Expand-Only mode cannot be used on SE050, only HKDF Extract-And-Expand implemented as specified in RFC5869, see [5].

3.10.3 Workaround

No workaround.

3.11 App.7: Read with attestation using a key with Origin EXTERNAL

3.11.1 Introduction

Attested read can be used to sign data returned from the IoT Applet. Within the SE050 APDU specification up to version 2.11 it is mentioned that an attested read cannot be performed with keys having ORIGIN_EXTERNAL.

3.11.2 Problem

An attested read can be performed with any origin.

3.11.3 Workaround

No Workaround (needed). To have trust in a key for attestation it anyway needs to be trusted via e.g. an externally signed certificate like included in SE050C.

3.12 JOS.1: SE050 goes to security reset when invalid EC key is used

3.12.1 Introduction

Customers can insert new ECC keys into the SE050 IoT applets. This keys need to be valid in order to be usable.

3.12.2 Problem

ECC Keys that are inserted into the SE050 IoT applet that do not following the rules for the key length are accepted by SE050. When the key is used a system reset is triggered which leads to the observation that the response is lost.

3.12.3 Workaround

ECC keys that get inserted into the SE050 IoT Applet need to be sent in the exact byte length of the selected curve (see APDU spec [2]). This problem is solved on SE051 product types.

3.13 JOS.2: SCP03 - maintenance of the encryption counter for APDUs without C-DATA

3.13.1 Introduction

Platform SCP is utilizing SCP03. In this protocol the encryption counter is utilized as part of the creation of the cryptograms.

3.13.2 Problem

When C-APDUs, not containing command data, are sent to the SE050 IoT Applet within a platform SCP session, the encryption counter is not increased. This leads to an interruption of the communication on subsequent APDUs due to the missing increment of the encryption counter.

3.13.3 Workaround

As workaround it is proposed to append command data to the APDU (e.g. a case 4 APDU). This will lead to a correct maintenance of the encryption counter. This workaround is implemented in Plug&Trust MW.

4 References

1. UM11225, SE05x T=1 Over I2C Specification. Available on NXP website.
2. AN12413, SE050 IoT applet APDU Specification. Available on NXP website.
3. UM10204, I^{2}C-bus specification and user manual. Available on NXP website.
4. 5049xx, SE050 data sheet. Available on NXP website.
5. RFC5869, HMAC-based Extract-and-Expand Key Derivation Function (HKDF). Available under the link.

5 Legal information

5.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

5.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

5.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 14 October 2020
Document identifier: ES_640310
Document number: 640310