Swissbit TSE SMAERS Firmware - Guidance Manual

Version 1.3.3, 2019-12-13

Table of Contents

Chapter 1. Introduction

This document is the Guidance Manual for the Swissbit TSE SMAERS Firmware. It comes in one of three form factors, which are depicted in Figure 1. It is meant to become a component of an Electronic Cash Register (ERS) to protect the ERS' transaction data as required by [KSV], [FCG], [BSI-TR-03153], and [PP-SMAERS]. Each Swissbit TSE contains the Swissbit TSE SMAERS Firmware and a Cryptographic Service Provider. Please note that it is sometimes tricky to distinguish whether a certain description is applicable specifically to the Swissbit TSE SMAERS Firmware or rather to the Swissbit TSE. As the Swissbit TSE SMAERS Firmware is part of the Swissbit TSE, all guidance and recommendations given with respect to the Swissbit TSE also apply to the Swissbit TSE SMAERS Firmware. When using a Swissbit TSE, the interaction is always with the Swissbit TSE SMAERS Firmware, which then uses its cryptographic service provider to create cryptographic signatures of the transaction logs, which the Swissbit TSE SMAERS Firmware protects.

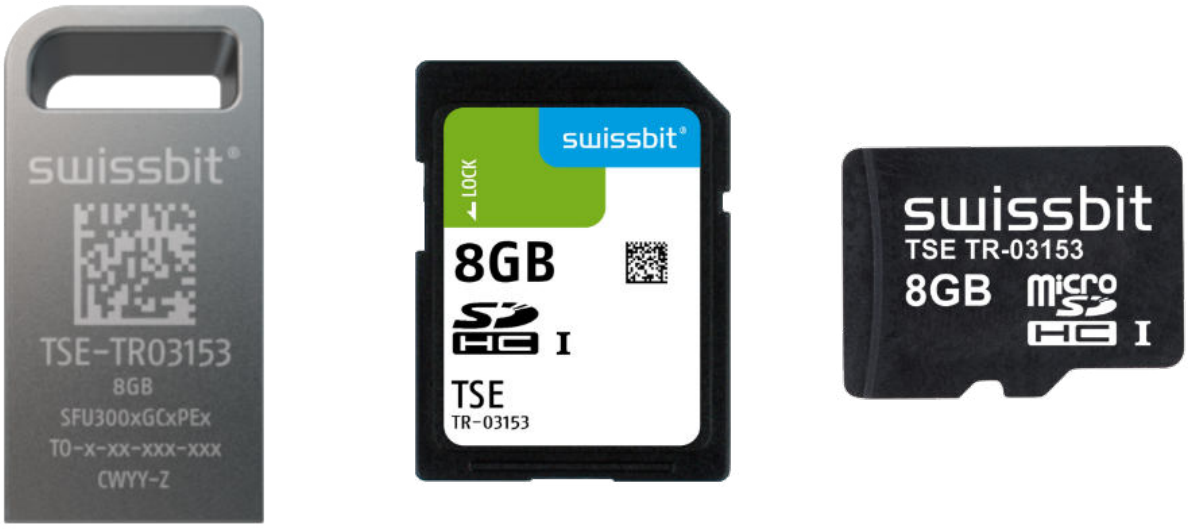

Figure 1. Different form factors of the Swissbit TSE

To successfully integrate and use the Swissbit TSE into Electronic Cash Registers, this document contains all required information including references to other documents, which cover, for example, the details of the user interface.

To allow a legal usage of the Swissbit TSE SMAERS Firmware according to [KSV] and [FCG], it will be certified according to [BSI-TR-03153]. In addition, it will be certified according to Common Criteria with the security target [ST-TSE]. This security target claims strict conformance to [PP-SMAERS].

1.1. Audience

Considering the life cycle of the Swissbit TSE, three roles play a major role:

- Swissbit, as producer of the Swissbit TSE and Swissbit TSE SMAERS Firmware within
- the ERS-Manufacturer, integrating the Swissbit TSE into the ERS or reselling Swissbit TSE to ERS-Users
- the ERS-User (Steuerpflichtige), using the ERS and thereby the Swissbit TSE and TOE. As taxpayer, the ERS-User is obliged by legal regulations to use a certified TSE.

This Guidance Manual is written and maintained for ERS-Manufacturers of Swissbit TSE into Electronic Cash Registers (ERS). The Guidance Manual for the ERS-users of the Swissbit TSE will then be provided by the ERS-manufacturer. So the ERS-Users' Guidance Manual has to be written by the audience of this document and is not covered by this document. This document does however contain guidance and specific information for the integrator that has to be forwarded to the ERS-User (which makes the separation sometimes hard to follow).

1.2. Scope

This document gives you, the ERS-Manufacturer, a general idea of the usage of a Swissbit TSE SMAERS Firmware. Details of the user interface are documented in the document Swissbit TSE SMAERS Firmware Functional Specification **[ADV_FSP]**. Besides, this document guides you to develop your guidance manuals for the ERS-Users of the Swissbit TSE (and of your ERS accordingly). To properly use Swissbit TSE some security aspects have to be considered. These aspects are documented here and it is your responsibility to ensure, that these needs are fulfilled. Ignoring these points might create security issues leading to an illegal usage of the Swissbit TSE accordingly.

1.3. Additional Documents

Besides this Guidance Manual, there are additional documents covering various aspects of the Swissbit TSE. Please make sure to also consider these documents:

- Swissbit TSE SMAERS Firmware Functional Specification **[ADV_FSP]**
- Swissbit TSE Data Sheet
- Verpackungsprüfanweisung **[Verpackungsprüfanweisung]**
- Swissbit TSE SMAERS Firmware Common Criteria Security Target **[ST-TSE]**

Chapter 2. The Swissbit TSE

The Swissbit TSE consists of a controller chip, flash memory and a cryptographic service provider. It comes either as SD-Card, Micro SD-Card, or USB-token. Within the Swissbit TSE there is the Swissbit TSE SMAERS Firmware, which is the Creative Common certified component of the Swissbit TSE. Swissbit TSE SMAERS Firmware consists of the software of the Swissbit TSE and parts of its controller chip.

Figure 2 give a high-level overview over these components.

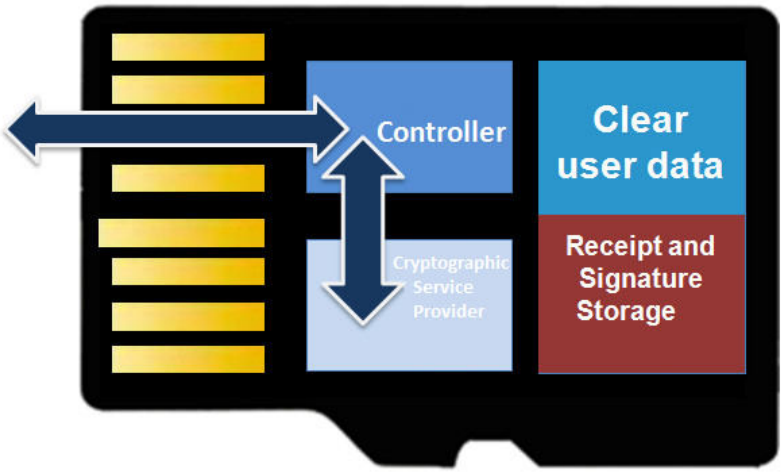

Figure 2. Architecture of the Swissbit TSE

Figure 2 splits up the flash memory of the Swissbit TSE into the Tar-archives, which hold the ERS's signed transaction logs. This part is named *Receipt and Signature Storage*. In addition, the other part *Clear user data* can be used to store additional documents, for example the Swissbit TSE's Guidance Manual.

The next section File Based Command Interface, gives an idea how the Swissbit TSE shall be used. Setup / Preparative procedures details the steps required to setup a Swissbit TSE, i.e. to make it operable. this is followed up by information on the operational phase of the Swissbit TSE, its PIN values and their handling as well as the time management, which the ERS has to do. Finally, the last section Operating the Swissbit TSE covers aspects of the life span of the Swissbit TSE .

2.1. File Based Command Interface

The Swissbit TSE SMAERS Firmware offers one user interface to the ERS. If the (micro) SD-Card or USB-Token is connected to the ERS it offers a *file-system interface*. Figure 3 shows the files, which the Swissbit TSE SMAERS Firmware presents in its file-system interface in a Windows Explorer.

Figure 3. The file interface of the Swissbit TSE SMAERS Firmware in a Windows Explorer

Note that the files and their content depend on the internal state of the Swissbit TSE SMAERS Firmware. In general, the file TSE_INFO.DAT contains status information of the device, the TSE_TAR.* files contain the stored transaction and system logs of the Swissbit TSE SMAERS Firmware and TSE_COMM.DAT is used to transfer commands to the Swissbit TSE SMAERS Firmware and receive the devices replies.

Detailed information on the file structure and all available commands can be found in the functional specification **[ADV_FSP]**, which Swissbit made available to you. Please note the ERS must not change the file system structure and ensure the file system remains valid. The ERS shall cleanly unmount the TSE prior to removal from the ERS.

2.2. Delivery of Swissbit TSE to you

Swissbit delivers Swissbit TSE to you. The delivery process has to ensure, that the Swissbit TSE reach you unmodified and not tampered with. To do so, the delivery is tracked and Swissbit did share the document **[Verpackungsprüfanweisung]** prior to delivery with a signed email. Make sure to successfully verify that email before providing the **[Verpackungsprüfanweisung]** inhouse further. If the verification fails or the document did not reach you, please contact your Swissbit Sales Contact immediately. Please make sure that the corresponding employees, which accept the delivery of the Swissbit TSE on your side, are aware of this document and use it to check the integrity of the parcel! If the stickers are damaged or broken do **not** accept the delivery and immediately contact your Swissbit Sales Contact to arrange an exchange of the possibly tampered Swissbit TSE!

When the Swissbit TSE successfully reached you, it comes with a cryptographic service provider that already contains one cryptographic key, which it uses to sign the ERS-User's transaction data. It also already contains a certificate, which will be used to verify the signatures and enables third parties to verify, that indeed a genuin certified CTSS was used to create the signed transaction logs. Finally, each Swissbit TSE comes with individuell initial PIN and PUK values, that can be derived as documented in section **Initial PIN Values and PIN Handling**.

Besides [Verpackungsprüfanweisung], Swissbit will deliver the document swissbit TSE - Functional Specification (ADV_FSP) [ADV-FSP] to you and list of revocation passwords. Each Swissbit TSE has a revocation password, that allows to revoke the certificate of that specific TSE if it is required (for example in case the TSE gets stolen or lost). Make sure that you received these information per encrypted email.

2.3. Setup / Preparative procedures

Before a Swissbit TSE can be used in an Electronic Cash Register, a few steps have to be executed. These steps shall be executed by the ERS-Users, so you, as ERS-Manufacturer have to guide your customers to do so.

First, the initial PINs have to get changed. Then, *Admin* has to log in and configure the ERS's serial number, such that the Swissbit TSE is able to identify the ERS. Afterwards, *Admin* or *TimeAdmin* have to set the time of the Swissbit TSE. The sequence of commands, that has to be executed can be found in *Application Note: TSE Setup* in the functional specification [ADV_FSP] of the Swissbit TSE. In addition, Figure 4 shows the sequence of commands, which has to be used to make the Swissbit TSE operational. Note that Swissbit offers (on request) the **Swissbit TSE Host Library** which implements the sequence of commands as setup function.

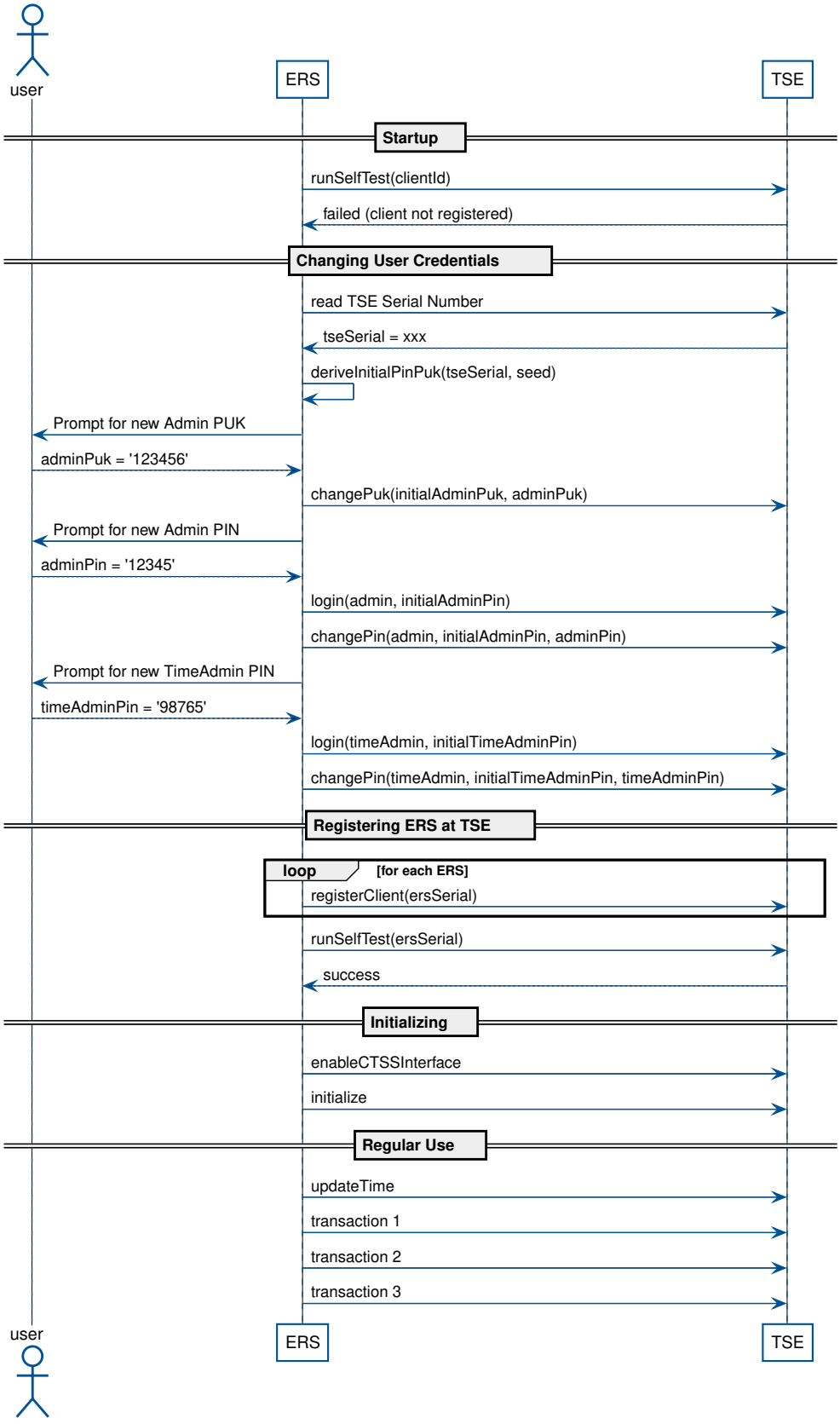

Figure 4. Sequence of commands to make Swissbit TSE SMAERS Firmware operational

The **Swissbit TSE Host Library** also implements the derivation method, which is required to compute the initial PIN and PUK-values for you.

In addition, the section **Initial PIN Values and PIN Handling** has some more information what the initial PIN values are and what has to be considered, when the PINs get changed. The section **Time management** of this document has additional information covering, what has to be considered, when the time of the Swissbit TSE SMAERS Firmware is updated. Note that the ERS has to have a correct reference time to do so!

Finally, it is crucial that you ensure, that the user of the Swissbit TSE registers the TSE at the Finanzamt. This is specified in the *Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen*, § 146a (4), **[FCG]**. To do so, the Finanzamt will provide a form (amtlich vorgeschriebener Vordruck) that has to be filled by the ERS-User. Swissbit suggest you to provide a software module in your ERS to collect all required information from the user and from the Swissbit TSE and print them. In addition, your guidance manual has to guide the user to register the Swissbit TSE in time. This way, the user is easily able to fill out the form and register the Swissbit TSE as required. The list of data, which have to be provided is listed in **[FCG]**.

In addition to the initialization of the Swissbit TSE itself and its registration, it is crucial that the device reaches its ERS-User in an unmodified form. Finally, the user has to provide a secure operational environment for the Swissbit TSE to protect its integrity. These two aspects have to be realized by your delivery process of the Swissbit TSE to the user and your guidance manuals, which advise the user how to set up the operational environment to protect the Swissbit TSE. More details on these topics can be found in the Chapter **Operational Environment and Delivery to ERS-Users** of this document.

2.4. Operating the Swissbit TSE

After the preparative procedures have been executed successfully, the Swissbit TSE is operational. This means, the Electronic Cash Register can save transaction data on the Swissbit TSE. In this phase there is almost no interaction between the ERS-User and the Swissbit TSE required.

The ERS itself has to update the time of the Swissbit TSE as documented in Section **Time management**. To do so, the ERS stores the *TimeAdmin PIN*, as documented in Section **Initial PIN Values and PIN Handling**. In addition, the guidance documents that you (the ERS-Manufacturer) deliver to your customer (the ERS-User) has to explain to the ERS-User how to backup transaction logs from the Swissbit TSE and how to delete the transaction logs after successful export by using the *Admin PIN*.

In this case make sure that the user is aware that the data can not be restored on the device and that it is the user's responsibility to store the data for the required amount of time! The commands which are required to implement these features are documented in **[ADV_FSP]** and your ERS software has to

wrap them according to your customers' needs.

In addition, the operational user guidance which you deliver to the user has to cover the aspects of the protection of the Swissbit TSE, which are listed in Chapter **Operational Environment and Delivery to ERS-Users**.

2.5. Initial PIN Values and PIN Handling

The Swissbit TSE has three PINs:

- The Admin PIN
- The Admin PUK
- The TimeAdmin PIN

Each Swissbit TSE comes with different initial PIN values. These values can be derived from the Swissbit TSE serial number and a seed specific to the ERS integrator, that you shared with Swissbit. The derivation scheme to compute the actual initial PINs (and PUK) values can be found in *Application Note: Initial PUKs and PINs* of the document **[ADV_FSP]**. Note that the initial values have to be changed before the Swissbit TSE SMAERS Firmware gets operational.

Chapter **Setup / Preparative procedures** covers details of this initialization process.

If you decide to change the PIN (and PUK) values prior to delivery to your customers, make sure (by a corresponding implementation in your software in the Electronic Cash Register), that the ERS-User has to change the PIN (and PUK) values again. It is not adequate that you are aware of the PIN (and PUK) values of a Swissbit TSE, which is in use by an ERS-User!

Finally, do not store the values of the Admin PIN or PUK within the software of your electronic cash register! These values are credentials of the owner of the Swissbit TSE and should be known to him/her only. Ensure that the ERS-User is aware of this by documenting it accordingly in the ERS-User's guidance manual. In addition, add remarks that ensure, that the ERS-User is aware of his/her surrounding while changing PINs to prevent somebody else watching the new PIN values being entered by the ERS-User.

Storing the TimeAdmin PIN in the ERS software is acceptable though. This PIN is required to update the time of the Swissbit TSE and is required multiple times each day.

2.6. Time management

The Swissbit TSE has to maintain an internal clock to be able to determine timestamps for various events. To do so, the ERS has the responsibility to correct the time of the Swissbit TSE. The maximal

timespan between two time-correction events can be found in the file TSE_INFO.DAT of the Swissbit TSE's file interface. It is given by the field *MaxTimeSynchronizationDelay*. The document **[ADV_FSP]** contains all required details on this and explains which command needs to be used to correct the time of the Swissbit TSE.

To operate the Swissbit TSE, it is crucial that the time is set as required. Be aware, this means that the ERS has to maintain a correct time! So you have to ensure, that the reference time, which gets set, is correct.

Finally note, that you should not correct the time of the Swissbit TSE too often. Setting the time results in internal log messages, which creates (when the audit data of CSP are fetched internally) a signature of the cryptographic service provider of the Swissbit TSE. This means, updating the time too often reduces the number of transactions, that can be stored in the Swissbit TSE!

2.7. Life Span of a Swissbit TSE

Two aspects determine the life span of a Swissbit TSE:

- the number of signatures, its cryptographic service provider computed and
- the validity of the certificate of the cryptographic service provider.

The cryptographic service provider is able to create twenty Million (20.000.000) signatures. When a Swissbit TSE SMAERS Firmware has created this amount of signatures it is strongly suggested to replace it.

The validity of the certificate depends on the point of time, when the certificate was created. This happens as part of the production process and the Swissbit TSE SMAERS Firmware does not support to switch certificates after production.

Both information, the number of created signatures and the validity of the certificate can be read from the file TSE_INFO.DAT, which the Swissbit TSE provides via its file interface. The functional specification **[ADV_FSP]** has details on this information.

For common usage, the Swissbit TSE has more than enough memory to store all transactions, which will be made in its life time. In special cases, especially if each transaction contains a lot transaction data, it might be the case, that the Swissbit TSE runs out of memory. Again, the file TSE_INFO.DAT contains information about the TSE's capacity and the current size of Logs. If the current size comes too close to the capacity, either the TSE should be replaced or the log files should be exported and stored safely. Afterwards, the Swissbit TSE Logs can be deleted on the TSE by the Administrator and the TSE be used further. Again, the functional specification **[ADV_FSP]** has details on the data format of TSE_INFO.DAT and on the commands, that are required to export and delete the Logs of the

Swissbit TSE.

2.8. Updates of the Swissbit TSE

For various reasons it might be required, that ERS-Users have to install update packages of the Swissbit TSE. Note that these will be rare events, but if ERS-Users fail to install updates intime, they will run into legal problems, because Swissbit TSEs, which did not install the required updates are not used as required by the certification processes.

Swissbit implemented the following three methods to ease the distribution of updates:

2.8.1. Implementing online check if Update is Required

If the ERS, which the TSE is integrated into, has the capabilities to check for TSE Updates, Swissbit strongly suggests to implement such a functionality. Here Swissbit offers a REST-API to check what the current version of the Swissbit TSE Software is. You either have to compare the corresponding version with the version, being announced in TSE_Info.dat, or you provide the TSE_Info.dat to the REST-API and the application will parse it and check if an update is required. The Rest-API then also provides the URL of the update to install.

Then the functionality of the ERS has to download the update and prompt the ERS-User to install it.

2.8.2. Registering email addresses of ERS-Users

Not all ERS are constantly able to check for updates, so Swissbit offers to register an email-address (for each TSE), which will receive update notifications. Note that the addresses will not be used for other purposes. Swissbit strongly suggests to either inform your TSE-Users to register an email-address at Swissbit, or you should create a list of email-addresses of the TSE-Users and relay the update information to them. Note that in this case you have to document towards your customers how they have to download and install updates. This has to be part of the guidance documents of your ERS. The email-addresses can be registered at **http://swissbit.com/tse/**.

Note that Swissbit will always inform you on published updates per email!

2.8.3. Notifying ERS-Users to check for Updates

Both ways to to distribute updates for Swissbit TSEs can fail. Therefore it is required, that the ERS-User checks periodically for updates on their own. You have to inform the ERS-User on this requirement and you have to provide a place to check for updates. If you do not provide such a place/webpage, you have to direct your ERS-Users to the corresponding Swissbit-page: **http://swissbit.com/tse/**.

Chapter 3. Operational Environment and Delivery to ERS-Users

The security concept of the Swissbit TSE requires, that the Swissbit TSE operational environment protects it against physical manipulation. The Swissbit TSE does not have a hardened casing, which prevents tampering! This means, to ensure the integrity of the Swissbit TSE and to operate it legally according to **[KSV]** and **[FCG]**, you have to ensure the Swissbit TSE protection in its operational environment and during the delivery from you to the ERS-User of the Swissbit TSE.

3.1. Delivery to ERS-Users

The delivery of the Swissbit TSE to the ERS-User has to ensure, that the Swissbit TSE reaches its destination unmodified. In addition, the recipient of the Swissbit TSE has to be put into the position to easily decide if the Swissbit TSE was (possibly) modified or arrived untampered. To reach this goal, you have to create a delivery process, that fulfills this needs.

The same also applies to the delivery of the Swissbit TSE from Swissbit to you. Section **Delivery of Swissbit TSE to you** and the document **[Verpackungsprüfanweisung]** give some insight, how Swissbit secures this delivery. Crucial aspects here are the packaging and sealing of the parcel with stickers in combination with the fast delivery time and tracking of the parcel.

To design a delivery process that fits the Swissbit TSE's and your needs, analyze carefully how the Swissbit TSE arrives at the ERS-User. A Swissbit TSE which is build into an electronic cash register, which is sealed, is to some extend protected by the register's case. Opposing, a Swissbit TSE sent on its own per mail is crucially vulnerable, so you have to add security measures here to properly protect the Swissbit TSE!

Finally, design the delivery process in such a way, that you can be sure to be informed about lost or possibly modified Swissbit TSE and report them as lost or tampered with their serial number in time! This way Swissbit can revoke the certificates of these Swissbit TSE and ensure that data logs of these TSE will not be accepted.

Be aware that you can request the Certificate Authority to revoke certificates of Swissbit TSE. To do so, please contact the Certificate Authority directly.

If a Swissbit TSE get lost, are reported lost from your customers or if they might have been manipulated, revoke the certificate to prevent abuse. To do so, Swissbit delivered revocation passwords for all TSEs to you. Note that you are responsible to provide the ERS-Users with a possibility to revoke their certificates. So either provide the revocation passwords to them or provide a service, which they can use to revoke the certificates with.

Swissbit also offers an online verification service to check tar archives of signed transaction logs from

the Swissbit TSE. Here, a tar file is uploaded and the contained signatures are verified, including the chain of certificates. Also revocation information are taken into account. Note that the functionality is also available as REST-Interface, so you can create a branded online service with the same functionality easily. Alternatively you can integrate the corresponding functionality into the cash register itself, if it has online connectivity. This way the function of the CSP can be verified and it can be made sure, that the certificate of the checked Swissbit TSE is not revoked.

3.2. Operational Environment

To operate the Swissbit TSE and the Swissbit TSE SMAERS Firmware according to the assumptions, which had to be made to create a security architecture for the device, the Swissbit TSE Common Criteria Security Target **[ST-TSE]** lists five security objectives for the operational environment of the Swissbit TSE SMAERS Firmware:

3.2.1. OE.CSP

The Swissbit TSE Common Criteria Security Target **[ST-TSE]** requires for Swissbit TSE SMAERS Firmware a Cryptographic Service Provider (CSP) in the Operational Environment of the Swissbit TSE SMAERS Firmware. This CSP is part of the Swissbit TSE, so it is always present.

3.2.2. OE.Transaction

The Swissbit TSE Common Criteria Security Target **[ST-TSE]** requires that the operational environment of the Swissbit TSE SMAERS Firmware shall verify the transaction log. This is not achieved by the Swissbit TSE itself. To allow the operational environment to do so, Swissbit offers the online verification service, which is explained in section **Delivery to ERS-Users**. This allows you, the ERS-Manufacturer, to implement a verification mechanism and enables the ERS-User to do the verification on their own.

3.2.3. OE.SUCP

The Swissbit TSE Common Criteria Security Target **[ST-TSE]** requires Swissbit to issue updates of the software of the Swissbit TSE SMAERS Firmware with protection mechanisms. The Swissbit TSE will reject all updates, which do not contain such protection mechanisms, so all installable Update Code Packages will be protected as required by **[ST-TSE]**.

3.2.4. OE.ERS and OE.SecOEnv

The Swissbit TSE Common Criteria Security Target **[ST-TSE]** requires the operational environment of the Swissbit TSE to protect the device accordingly. This requirements originates in the document

Swissbit TSE Common Criteria Security Target [ST-TSE] in section *Security objectives for the operational environment*. The two objectives, which your ERS has to fulfill are:

> **OE.ERS:** Trustworthy electronic record-keeping system The taxpayer shall use correctly an electronic record-keeping system that provides separately, correctly, completely and in real time all Transaction Data that are legally required for generation of Log messages to the TOE. The electronic record-keeping system shall support its testing as external entity by the TOE. The electronic record-keeping system shall produce receipt including besides the transaction data the points in time when the transaction is started, completed or terminated, and the transaction number provided by the certified security device (i.e. the CSP).

and

> **OE.SecOEnv:** Secure operational environment The operational environment shall protect the electronic record-keeping system and the certified technical security system including the TOE against manipulation, perturbation and misuse. It protects the integrity of the communication between the electronic record-keeping system and the TOE.

Note that the TOE in these quotes is the Swissbit TSE SMAERS Firmware and CSP refers to the cryptographic service providers. Both together form the Swissbit TSE. While it is your responsibility to build your ERS to fulfill **OE.ERS**, you also have to make sure that the operational environment of your ERS, which contains one Swissbit TSE, fulfills **OE.SecEnv**.

To do so, one aspect is, where the Swissbit TSE is located in your ERS. If it is inside the ERS case which is closed with screws and security seals, you already have some physical protection layer around the Swissbit TSE, which helps to achieve the requirements of **OE.SecEnv**. In case of a Swissbit TSE USB, which is located in an outer USB-Slot of the ERS, you have to do more. As a good starting point the Swissbit TSE should be removed and locked away, when the ERS is not operating. In addition, it should be regularly checked, if it is directly connected to the ERS.

Note that there are also other options of connecting a Swissbit TSE to the ERS. The document [ST-TSE] lists possibilities how to use a TSEs in a remote fashion and how to secure connection. In addition, it might be possible to wrap a Swissbit TSE in some form changer. The form changer shall be implemented to store neither clientIDs nor any other authentication secret on behalf of the ECR, therefore exclusively a conversion of access protocol and/or form takes place. For example, a Swissbit TSE in the Micro SD Formfactor could be wrapped in an USB dongle with or without additional logic put in front of the TSE while the TSE module is removable from the form changer.

Some further aspects to consider are the following ones:

- Who has (physical) access to the ERS?
- Is the ERS monitored by employees at all times?
- Is there a (physical) separation between customers and ERS?
- Do customers directly interact with the ERS or is all interaction tunneled through employees?

Depending on the answers to this questions, you have to develop guidelines for the ERS-Users of the Swissbit TSE in your guidance manual, which ensure that the operational environment of your ERS and the Swissbit TSE is secured accordingly to the requirements above.

Chapter 4. Certificates of the Swissbit TSE

The Swissbit TSE comes with one certificate, which can be used to verify the signatures in the tar-archives, which the Swissbit TSE produces. The validity of the certificate determines the life span of the Swissbit TSE. It can not be updated. Usually the certificate of the Swissbit TSE is valid for 3, 5, or 7 years each with added 6 months to cover the period from production to installation and usage.

The certificate is issued by the Certificate Authority **TSE-CA**, which is a sub-CA of the certificate authority **TSE Root CA**. Both CAs are maintained by T-Systems International. The certificate of **TSE Root CA** can be obtained from the certification report of the Common Criteria Certification of the Swissbit TSE SMAERS Firmware.

The CA maintains Certificate Revocation Lists, which list all certificates, that have been revoked for some reason. Certificates are listed on this list at least until 10 years of the end of their validity period. To revoke a certificate, Swissbit created a revocation password. Using this password the CA allows to revoke the certificate.

Chapter 5. Verification of TAR-Archives and Signatures of the Swissbit TSE

The following two sections specify how to verify signatures of the Swissbit TSE and how to verify Tar-archives.

5.1. Verification of Signatures

Note that the signature of the TSE have to be verified using a hybrid model, which works as follows:

- Extract the root CA certificate from the certification report of the Common Criteria Certification of the Swissbit TSE SMAERS Firmware. This is the trust anchor to verify the signatures.
- Verify, that signature of the TBS was generated with the certificate **cert_tse**
- Verify, that the **cert_tse** was valid, when the signature was created, i.e.
    - The point of time of signature creation is in the validity period of **cert_tse**, the Sub-CA certificate, and Root-CA certificate which issued **cert_tse**.
    - Assure, that **cert_tse** was not revoked at the signature creation time, using CRL mechanisms.
    - Verify that **cert_tse** was issued by the Sub-CA, including a revocation check of the Sub-CA's certificate
    - Verify that the Sub-CA's certificate was issued by the Root-CA
- Check that the validity of **cert_tse** did not end more than 10 years ago

This allows to successfully verify signatures for 10 years after the end of the validity period of **cert_tse**. The lifespan of **cert_tse** matches the lifespan of the TSE in the field. After the TSE's end of life it is required to be able to verify transaction data for 10 additional years. The hybrid model for signature verification allows to do so, while it ensures, that the signature was valid at creation time following the shell model.

Note that **[DSFinV-K]** describing in section 3.1.2.5 the examination process requirements for fiscal audit records TSE signature certificates need to be valid at the time of signature creation and not necessarily at the time of signature verification. Therefore aforementioned certificate lifetime does not have to be extended by this 10 year period and the hybrid verification model above is covered by this specification.

5.2. Verification of Tar-Archives

To check a Tar-archive, which was exported from a Swissbit TSE, proceed as follows:

- Extract **cert_tse** from the archive.
- Verify all signatures of all log messages in the tar archive following section **Verification of Signatures** of this document
- Check that the order of the log messages is plausible, i.e. verify that signature counter, transaction counter, and time stamps make sense:
    - check that there is no gap in the increasing sequence of the transaction numbers
    - check that not too many or too big gaps are present in the increasing sequence of signature counter values. Note that single signatures can got lost from time to time, for example due to power loss of the TSE in a critical moment. Still, no value can be present twice!
    - check that the time stamps of the signature are plausible. Not that there might be log messages in the tar archive, which can change the time in both direction. I.e. if a settime-event is in the log, the sequence of time stamps might be not increasing after the settime-event.

If any of these steps fails, the examinant has to analyze deeper why this is the case.

Chapter 6. Related Documents

- [ADV_FSP] swissbit TSE - Functional Specification (ADV_FSP), Version 1.2.11
- [BSI-TR-03153] Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, TR-03153, Version 1.0.1
- [DSFinV-K] Digitale Schnittstelle der Finanzverwaltung für Kassensysteme (DSFinV-K 2.0), Version 2.0, **https://www.bzst.de/DE/Unternehmen/Aussenpruefungen/DigitaleSchnittstelleFinV/digitaleschnittstellefinv_node.html**
- [FCG] Fiscal Code of Germany in the version promulgated on 1 October 2002 (Federal Law Gazette [Bundesgesetzblatt] I p. 3866; 2003 I p. 61), last amended by Article 6 of the Law of 18. July 2017 (Federal Law Gazette I p. 2745)
- [KSV] Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr,(Kassensicherungsverordnung – KassenSichV), Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 66, ausgegeben zu Bonn am 6. Oktober 2017
- [PP-SMAERS] Common Criteria Protection, Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), Aktuell in Version 0.7.5
- [ST-TSE] swissbit TSE - Common Criteria Security Target, Version 1.8.4
- [Verpackungsprüfanweisung] swissbit TSE - Verpackungsprüfanweisung, Version 1.1.0