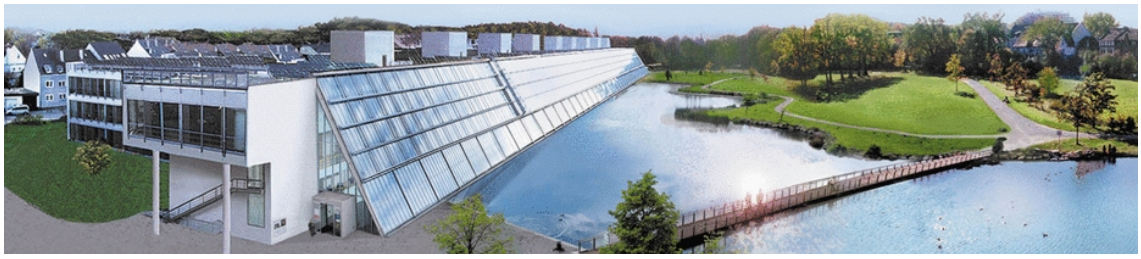

Deviations of the D-Trust TSE

when compared to the TR-03151

Version 1.4 • 2020-05-26

cv cryptovision GmbH • Munscheidstr. 14 • 45886 Gelsenkirchen • Germany
www.cryptovision.com • info@cryptovision.com • +49-209-167-2450

Content

Version Control

Version	Date	Author	Changes to Previous Version
1.0	2020-05-04	Ben Drisch	Initial version
1.1	2020-05-07	Hans Hudde	ERS assignment
1.2	2020-05-08	Mathias Neuhaus	Audit- and System-Logs
1.3	2020-05-11	Mathias Neuhaus	Added function specifications
1.4	2020-05-26	Mathias Neuhaus	Added Audit-Log details

1 Extensions to the TR-03151

The SE-API as specified in the TR-03151 (BSI, 2018) has been extended in several aspects.

Extreme care was taken to define each separate extension to be compatible with but never contradict the definitions in TR-03151.

1.1 Functional Extensions

The following functions have been added to the SE-API definitions from TR-03151.

These functions allow configuration of the TSE or provide detailed information on the TSE.

Note: The naming in this chapter only gives the method names used in the Java SE-API;
for the "C" SE-API the function names have to be prepended with **`se_`**;
for the "extended" C SE-API an **`Ex`** is appended to the "C" SE-API function names.

Detailed information on each of these functions is found in the cryptovision SE-API documentation (→ (cryptovision, 2020) and (cryptovision, 2020)).

1.1.1 mapERStoKey

The command `mapERStoKey()` is used to assign a specific signature key (keyID) to an ERS (ClientID) or to delete such an assignment.

This method is based on the PP-0105 (BSI, 2019) requirement that signatures must only be made for ERSs known beforehand. Because this assignment cannot be done at production time of the TSE, this additional method was introduced.

Access to this function is possible only after authentication as a user in the Admin role.

This function will produce an additional system log (→ 1.3.2.1).

As such an ERS assignment is necessary just once (per ERS), the system logs generated should not interfere during successive log-file evaluation.

1.1.2 deactivateTSE and activateTSE

The commands `deactivateTSE()` and `activateTSE()` are meant to temporarily disable an entirely personalized TSE during transport. By deactivating the TSE signing of transaction logs is not possible until it is activated again. PIN assignments and ERS mappings are kept throughout this process.

Access to these functions is possible only after authentication as a user in the Admin role.

These functions generate additional system logs (→ 1.3.2.2 and → 1.3.2.3 respectively).

During every-day use, such (de-) activations will not occur frequently; interference with log-file evaluation are not to be expected.

1.1.3 getOpenTransactions

The command `getOpenTransactions()` retrieves the list of dangling ("open") transactions from the SE.

1.1.4 getTimeSyncInterval

The command `getTimeSyncInterval()` retrieves the proposed update interval for the CSP time base.

1.1.5 getPinStatus and initializePinValues

The command `getPinStatus()` retrieves the current "transport" status of the PINs and PUKs defined in the SE and `initializePinValues()` switches PINs and PUKs from "transport" status to "use" status and assigns the PIN / PUK values.

1.1.6 exportData

The `exportData()` method has been implemented in two additional variants, providing direct I/O to a file (specified by its fileName) or a Java OutputStream.

1.1.7 exportMoreData and deleteStoredDataUpTo

`exportMoreData()` can be used to export data beginning at the last seen log entry.
`deleteStoredDataUpTo()` can be used to delete data up to a specific log entry.

These two functions - counterparts of each other - speed up data export considerably. Additional variants of `exportMoreData()` exist like for `exportData()`.

1.1.8 getSignatureAlgorithm

The command `getSignatureAlgorithm()` returns the signature algorithm used.

1.1.9 getLifeCycleState

The command `getLifeCycleState()` returns the current life cycle state.

1.1.10 getTransactionCounter

The command `getTransactionCounter()` returns the last transaction number.

1.1.11 getTotalLogMemory

The command `getTotalLogMemory()` returns the size of the log memory.

1.1.12 getAvailableLogMemory

The command `getAvailableLogMemory()` returns the remaining free log memory.

1.1.13 getERSMappings

The command `getERSMappings()` returns an ASN.1 encoded sequence of mappings of ERSs (clientID) to key serial numbers (keyID).

1.1.14 getSignatureCounter

The command `getSignatureCounter()` returns the current signature counter for a given key.

1.1.15 getCertificateExpirationDate

The command `getCertificateExpirationDate()` returns the certificate expiration date.

1.1.16 exportPublicKey

The command `exportPublicKey()` returns the public signature key from the certificate.

1.1.17 getWearIndicator

The command `getWearIndicator()` returns an indicator for data retention.

1.1.18 getUniqueId

The command `getUniqueId()` returns the unique (hardware) ID of a TSE.

1.1.19 getFirmwareId

The command `getFirmwareId()` returns the version of the TSE firmware.

1.1.20 getCertificationId

The command `getCertificationId()` returns the (BSI) certification ID of the cryptovision TSE.

1.2 Data Handling Extensions

1.2.1 additionalData in StartTransaction and FinishTransaction Commands

The parameter `additionaData` of the StartTransaction (→ (BSI, 2018), ch. 4.4.1) and FinishTransaction (→ (BSI, 2018), ch. 4.4.3) commands are defined as "Reserved for future use". It is to be included in the TSE signature as `additionalExternalData` (→ (BSI, 2018), ch. 2.3.1).

The D-Trust / cryptovision TSE does support this parameter.

When specified / non-null, it will be included in the signature as specified in TR-03151 (BSI, 2018).
When not specified / null, `additionalExternalData` will be omitted from the signature input.

This fulfills the specification in TR-03151 exactly.

1.2.2 additionalInternalData in Initialize System Logs

The system log generated by the **Initialize** function (→ (BSI, 2018), ch. 4.3.1) will provide information on the secure element as `additionalInternalData`:

Table 1 additionalInternalData for Initialize

Data field	Tag	Data type	Mandatory?	Description
seHWversion	0x81	OCTET STRING	m	Contains the hardware serial number of the secure element.
smaersVersion	0x82	OCTET STRING	m	Contains the version number of the SMAERS application (**0105**).
cspVersion	0x83	OCTET STRING	m	Contains the version number of the CSP application (**000B**).

This is compatible to the specification in TR-03151 (BSI, 2018).

1.3 Log Extensions

1.3.1 Audit Logs

Audit entries are generated for the events listed in → Table 2 in and are exported as audit logs.

The table is complete; seemingly missing IDs are not used, in a CSP configured for the SMAERS application.

Table 2 Audit types

ID	Name	Description
01	Audit Start-up	Once during initial power-up of the TSE
03	Authentication re-tries exhausted	When exceeding the retry-counter for a PIN
06	Set Time	At each update of the time
07	UCP	During installation of an “Update Code Package” (UCP)

Audit logs are formatted according to TR-03151 (→ (BSI, 2018), ch.2.1;
seAuditData is defined in → Table 3.

Table 3 Contents of seAuditData

Data field	Tag	Data type	Mandatory?	Description
Audit type	0x8A	BYTE	m	ID from → Table 2
Result	0x6B	BYTE	m	success (0x00), error (0x01), aborted (0xFF)
Time stamp	0x8C	INTEGER	m	Unix Time encoded in an 8 byte INTEGER
User name	0x8D	PrintableString	o	Omitted for the „unidentified user“, otherwise the name of the authorizing user
Additional data	0x8E	→ Table 4 → Table 5	o	Additional data depending on the audit type (→ Table 4 and Table 5)

1.3.1.1 Additional Data in Set Time Audit Logs

The “Additional data” field in Set Time Audit Logs (→ Table 3) will be present in case of a successful time update only.

Table 4 Additional data of the “Set Time” audit log

Data field	Tag	Data type	Mandatory?	Description
Additional data	0x8E	INTEGER	m	Unix Time encoded in an 8 byte INTEGER

1.3.1.2 Additional Data in Update Code Package (UCP) Audit Logs

Table 5 Additional data of the “UCP” audit log

Data field	Tag	Data type	Mandatory?	Description
Additional data	0x8E	OCTED STRING	m	current CSP version (2 byte) || version of update package (2 byte)

1.3.2 System Logs

System logs are generated for the operations specified in TR-03151 (BSI, 2018) and PP-SMAERS (BSI, 2019).

This section specifies the additional system logs.

1.3.2.1 ErsAssignment

Any ERS assignment to a signature key (→ 1.1.1) will generate a system log.

"ErsAssignment" will be used for the `operationType` field, while the `systemOperationData` is specified in → Table 6.

Table 6 systemOperationData for mapERStoKey

Data field	Tag	Data type	Mandatory?	Description
clientId	0x81	PrintableString	m	Contains the name of the ERS (clientID)
serialNo	0x82	OCTET STRING	m	Contains the serial number of the signature key (keyID) in case of an ERS assignment; empty in case of an ERS DE-assignment

1.3.2.2 DeActivateSE

Temporary deactivation of a TSE (→ 1.1.2) will produce a system log.

"DeActivateSE" will be used for the `operationType` field, while the `systemOperationData` is specified in → Table 7.

Table 7 systemOperationData for deactivateTSE

Data field	Tag	Data type	Mandatory?	Description
timeOfDeactivation	0x81	INTEGER	m	Contains the time of the Secure Element when its deactivation is started.

1.3.2.3 ActivateSE

Re-activation of a temporarily deactivated TSE (→ 1.1.2) will produce a system log.

"ActivateSE" will be used for the `operationType` field, while the `systemOperationData` is specified in → Table 8.

Table 8 systemOperationData for activateTSE

Data field	Tag	Data type	Mandatory?	Description
description	0x81	PrintableString	m	Contains the empty string.

Literaturverzeichnis

BSI. (2018, December 20). *Technical Guideline BSI TR-03151 Secure Element API (SE API) - Version 1.0.1.* Retrieved from https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03151/index_htm.html

BSI. (2019, April 01). *BSI-CC-PP-0105-2019 - Common Criteria Protection Profile - Security Module Application for Electronic Record- keeping Systems - Version 0.7.5.* Retrieved from https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0105.html

cryptovision. (2020, April). *cryptovision SE-API ("C").* Retrieved from https://tse-support.cryptovision.com/jira/servicedesk/customer/kb/view/14025018

cryptovision. (2020, April). *cryptovision SE-API (Java).* Retrieved from https://tse-support.cryptovision.com/jira/servicedesk/customer/kb/view/14025018