Supplementary CI Plus Specification
for
Service / Network Operators
Version 1.4

31 Chertsey Street, Guildford, Surrey, GU1 4HD, UK

A company registered in England and Wales

Registered No: OC341596

Contents

1 References

1.1 Normative references

[1] CI Plus Specification, v.1.3.2
http://www.ci-plus.com

[2] ETSI EN301 192: Digital Video Broadcasting (DVB); DVB specification for data broadcasting.

[3] ISO/IEC 13818-6: Information technology - Generic coding of moving pictures and associated audio information, Extensions for DSM-CC.

[4] ETSI EN 300 468: Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems.

[5] ETSI TR 101 162, Digital Video Broadcasting (DVB); Allocation of Service Information (SI) and Data Broadcasting Codes for Digital Video Broadcasting (DVB) systems.

[6] IETF RFC 1950 (1996): ZLIB Compressed Data Format Specification version 3.3.

2 Definitions, symbols and abbreviations

2.1 Definitions

CICAM: Common Interface Conditional Access Module

reserved_future_use: Indicates that the value may be used in the future. All "reserved_future_use" bits are set to "1"

2.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BAT	Bouquet Association Table
BCD	Binary Coded Decimal
CA	Conditional Access
CICAM	Common Interface Conditional Access Module
CIP	Common Interface Plus
ECM	Entitlement Control Message
EIT	Event Information Table
EMM	Entitlement Management Message
LSB	Least Significant Bit
MJD	Modified Julian Date
NIT	Network Information Table
PID	Packet Identifier
PMT	Program Management Table
RSA	Rivest Shamir Adleman public key cryptographic algorithm
RSD	Revocation Signalling Data
SDT	Service Description Table
SI	Service Information
SOCRL	Service Operator Certificate Revocation List
SOCWL	Service Operator Certificate White-List
SOPKC	Service Operator Public Key Certificate
SOP	Service Operator Public Key
SOQ	Service Operator Private Key

3 Technical mechanisms

3.1 Requirements for Host revocation

This section details the revocation mechanism as described in section 5.5 of the CI Plus Specification [1]. The Host revocation mechanism is linked to a specific Service Operator. Host service revocation comprises black listing and white listing. The black list is called Service Operator Certificate Revocation List (SOCRL) and supports all revocation granularities listed in section 5.5.2 [1]. The white list is called the Service Operator Certificate White List (SOCWL) and contains identifiers for single Host devices for which revocation should be removed but are still listed in the latest SOCRL. The SOCWL shall overrule the SOCRL. The SOCWL shall always refer to the latest version of the SOCRL.

The scope of revocation is limited to the network of the Service Operator where revocation is deployed and is connected to the CA system.

3.1.1 RSD signalling

The CICAM shall receive information from the Service Operator that enables it to download new and updated SOPKC, SOCWL and SOCRL files. This information is conveyed as Revocation Signalling Data (RSD) and its definition is based on the following requirements.

Table 3-1: Signalling requirements

	Requirements
RS.1	The RSD detection shall be switched on or off by the CA system.
RS.2	When RSD detection is switched on, the CICAM shall download the RSD. To assure RSD detection, the RSD shall be present on the network at all times when RSD detection is switched on.
RS.3	The provision to the CICAM of the RSD version number, RSD transmission time out, RSD detection on/off state and the service operator identification shall be protected by the CA System against replay, tampering and blocking. The RSD transmission timeout and the service operator identification may be pre-configured in the CICAM.
RS.4	The CICAM shall verify the digital signature of the RSD with the public key in the Service Operator Certificate before it is used.
RS.5	The RSD shall cycle at least 4 times per transmission timeout. The timeout shall be persistent and shall not be reset due to a power-cycle or reset. The timeout shall be configured by the CA system
RS.6	The RSD shall identify the Service Operator.
RS.7	The RSD shall identify the services that require CI Plus protection.
RS.9	The RSD shall indicate where the latest SOPKC file is located in the CI Plus Data Carousel.
RS.10	The RSD shall indicate where the latest SOCWL file is located in the CI Plus Data Carousel.
RS.11	The RSD shall indicate where the latest SOCRL file is located in the CI Plus Data Carousel.
RS.12	The RSD shall indicate the transmission time-out for the SOCRL.
RS.13	The SOCRL and SOCWL shall be protected against replay, tampering and blocking.
Note 1:	Requirements RS.7 to RS.13 are defined in the context of the Service Operator as indicated by RS.6.

3.1.2 Data carousel signalling

The RSD, SOPKC, SOCRL and SOCWL may all be regarded as files. The CICAM shall download the RSD file (V1 or V2), the SOPKC, a SOCRL (V1 or V2), and the SOCWL (if present) using the broadcast channel, where the files are repeatedly transmitted using a dedicated carousel: the CI Plus data carousel.

The CI Plus Data Carousel shall conform to the One-layer Data Carousel as specified in [2], Clause 10. The CI Plus Data Carousel shall contain at most six files: RSD V1, RSD V2, SOPKC, SOCRL V1, SOCRL V2 and SOCWL.

Each file in the CI Plus Data Carousel is identified by a combination of a ‘module_id’ and a ‘moduleVersion’ field. Both are part of the ‘moduleInfo’ list of the DownloadInfoIndication (DII) message ([2], Clause 10.1.3). The maximum ‘moduleSize’ is 500KiB. The CI Plus Data Carousel is broadcast on a single PID.

When the CICAM establishes that there is revocation data to download it shall use the module list in the RSD (V1 or V2) to determine which files are updated and available for download. The 'module_id' field is specified according to Table 3-2. The 'module_version' fields are equal to the version numbers contained in the SOCRL and SOCWL files, which are authentic because of the digital signature. The 'module_version' field shall always be equal to 0x01 for the SOPKC file.

Table 3-2: module_id values

module_id	File
1	SOPKC
2	SOCRL V1
3	SOCRL V2
4	SOCWL
5	RSD V1
6	RSD V2

The RSD shall first be checked for validity using the service_operator_identity. The RSD version_number shall be checked against the version number delivered using the CA System. If revocation is enabled (on) and the RSD file does not exactly match the RSD file information delivered by the CA system then the CICAM becomes limited operational.

The CICAM shall always download the SOPKC from the carousel, regardless of the 'module_version' in the RSD and it is permitted to obtain the SOPKC directly. After reception of the SOPKC the CICAM shall first verify the SOPKC using the root certificate and thereafter it shall use the SOPKC to validate the RSD.

Once the RSD and SOPKC are confirmed to be valid, the CICAM shall download the remaining files that are indicated by the module list in the RSD. After a successful download of the SOCRL or SOCWL files, the authenticity of the data shall be tested by verifying the digital signatures using the RSA public key from the SOPKC.

As a last step, the 'module_version' as found in the downloaded SOCRL and SOCWL, shall be verified against the version numbers contained in the RSD. The version numbers that are contained in the files are authentic because they are protected by the digital signature and provide protection against replay.

Digital signatures shall comply with RSASSA-PSS as specified in [1], Annex I.

3.1.2.1 Data broadcast descriptors

The data_broadcast_id_descriptor identifies the type of the data component and is placed in the component loop of the PSI PMT table. Its exact use and meaning is dependent upon the value of the data_broadcast_id field. The selector_bytes of the data_broadcast_id_descriptor and data_broadcast_descriptor shall be zero length for a CI Plus LLP data carousel.

There shall be at most one instance of the data_broadcast_id_descriptor with the CI Plus LLP registered value of data_broadcast_id [5] in the PMT. i.e. Only one elementary stream may carry the CI Plus Data Carousel.

data_broadcast_id = `0x0122 (CI Plus LLP)`

3.1.3 File Formats

The file formats for the RSD, SOCRL, SOCWL and SOPKC are based on a Tag-Length-Value (TLV) structure indicating the file_tag and the file_len. The ROT shall supply these files to the Service or Network Operator for delivery on the Data Carousel.

The value of 'file_tag' field is specified according Table 3-3.

Table 3-3: file_tag values

file_tag value	file
0xDx	Reserved – compressed file format
0xE1	SOPKC
0xE2	SOCRL V1
0xE3	SOCRL V2
0xE4	SOCWL
0xE5	RSD V1
0xE6	RSD V2

3.1.3.1 Compressed File Format

The use of the compressed file format is optional. When it is used, the compressed variants of the RSD, SOCRL, SOCWL and SOPKC are packaged in a generic wrapper that identifies the compression method as shown in Table 3-4.

Table 3-4: compressed_file Syntax

Syntax	No. of bits	Mnemonic
`compressed_file() {`		
`  compression_tag`	`16`	`uimsbf`
`  compressed_data_len`	`24`	`uimsbf`
`  uncompressed_data_len`	`24`	`uimsbf`
`  compressed_data`	`N`	`bslbf`
`}`		

compression_tag. The 8 most significant bits of the compression_tag identify the compression algorithm according to Table 3-5. The 8 least significant bits are copied from the file_tag associated with the compressed_data and identify the compressed file according Table 3-3.

Table 3-5: compression_tag most significant byte values

Value	Description
`0xD0`	zlib compression structure of RFC 1950 [6]
`0xD1–0xD7`	CI Plus LLP reserved for future use
`0xD8–0xDF`	User defined

compressed_data_len. The compressed_data_len field specifies the length of the compressed_data field in bytes.

uncompressed_data_len. The length in bytes of the compressed_data field once it has been decompressed using the compression method specified by the compression_tag. The uncompressed file contains TLV content according to Table 3-3.

compressed_data. This field contains a compressed RSD_file, SOCRL_file, SOCWL_file or SOPKC_file. The number of bits N are calculated as follows `N=(compressed_data_len * 8)`.

3.1.4 RSD file format

The RSD_V1 file is defined in Table 3-6. The RSD_V2 file is defined in Table 3-7.

This is provided for information only as the ROT creates this file.

Table 3-6: RSD_V1_file Syntax

Syntax		No. of bits	Mnemonic
RSD_V1_file() {			
file_tag		8	uimsbf
file_len		24	uimsbf
version_number	//RS.3	16	uimsbf
valid_until_timestamp	//RS.3	32	bslbf
service_operator_identity	//RS.6	64	bslbf
encryption_method_identity		8	bslbf
transaction_id		32	uimsbf
reserved_for_future_use		8	bslbf
number_of_file_entries		8	uimsbf
for (i = 0; i < N; i++) {			
module_id	//RS.9+10+11+12	16	uimsbf
module_version	//RS.9+10+11+12	8	uimsbf
transmission_timeout	//RS.13	24	uimsbf
reserved_for_future_use		8	bslbf
}			
number_of_service_entries		16	uimsbf
for (i = 0; i < N; i++) {			
service_id	//RS.7	16	uimsbf
}			
RSD_file_signature	//RS.3+4+6	2048	bslbf
}			

Table 3-7: RSD_V2_file Syntax

Syntax		No. of bits	Mnemonic
RSD_V2_file() {			
file_tag		8	uimsbf
file_len		24	uimsbf
version_number	//RS.3	16	uimsbf
valid_until_timestamp	//RS.3	32	bslbf
service_operator_identity	//RS.6	64	bslbf
encryption_method_identity		8	bslbf
reserved_for_future_use		40	bslbf
number_of_file_entries		8	uimsbf
for (i = 0; i < N; i++) {			
module_id	//RS.9+10+11+12	16	uimsbf
module_version	//RS.9+10+11+12	8	uimsbf
transmission_timeout	//RS.13	24	uimsbf
reserved_for_future_use		8	bslbf
}			
number_of_service_entries		16	uimsbf
for (i = 0; i < N; i++) {			
service_id	//RS.7	16	uimsbf
}			
RSD_file_signature	//RS.3+4+6	2048	bslbf
}			

file_tag. The file_tag field is specified as 0xE5 for RSD_V1 or 0xE6 for RSD_V2.

file_len. The file_len field specifies the length of the RSD_file starting from the version_number, excluding the file_tag and file_len fields. The size of the RSD is expressed in bytes and shall not exceed the maximum file length of 2 KiB.

version_number. The version_number field specifies the version number of the RSD. The RSD version_number shall strictly increase. The RSD version_number shall be different from zero. The RSD version_number is also used to

prevent replay of previous RSDs by comparing it with the latest RSD version number that was detected by the CICAM (see section 5.5 of [1]).

valid_until_timestamp. The valid_until_timestamp field represents a point in time after which the RSD_file is considered as no longer applicable. If this timestamp is expired and the RSD version_number is the latest one required by the CAS, then the revocation shall be considered as disabled. The valid_until_timestamp field consists of 16-bits giving the 16 LSB of the Modified Julian Date (MJD) and 4 digits in 4-bit Binary Coded Decimal (BCD).

Example: 1993/10/13 12:45 is coded as "0xC0791245".

The valid_until_timestamp shall be set such that expiration occurs before the version_number wraps, there are 2^{15} different versions. A reasonable validity period might be 2 years.

service_operator_identity. The service_operator_identity field identifies the Service Operator Certificate of the Service Operator that has signed the RSD. The service_operator_identity is issued by the Root-of-Trust on request of a Service Operator. The CI Plus LLP service_operator_identity is equal to 0x0000000000000001. The service_operator_identity appears in the CN of the Service Operator certificates' subject field (see section 9.3.6 of [1]). When the CICAM verifies the integrity of the RSD file, it shall ensure that the service_operator_identity in the RSD file matches the CN in the Service Operator Certificate.

encryption_method_identity. The encryption_method_identity field is used to identify the encryption method used for the fields module_id, module_version and service_id. The encryption_method_identity '0x00' is mandatory for implementation.

Table 3-8: Encryption Method Identity

encryption_method_identity	Method
0x00	No encryption
0x01 – 0xFF	Reserved for future use
Note: when an encryption cipher is used the length of the encrypted fields shall be padded if required by a 1 (i.e. one) and then 0s (i.e. zeros).	

transaction_id. The transaction_id field is fixed to 0xFFFFFFFF for the CI Plus LLP service_operator_identity. Otherwise it is service operator specific.

reserved_for_future_use. This field is reserved for future use and shall be 0xFF but ignored by the CICAM.

number_of_file_entries. This 8-bit field specifies the number of file entries that appear in the loop following this field. Each entry corresponds to a single file that appears in the data carousel, represented by a module_id. The loop shall minimally include a SOPKC and a SOCRL (V1 or V2 depending on the RSD file_tag) file. The loop may optionally include a SOCWL file.

module_id. The module_id field is used to identify the correct file for download. Refer to section 3.1.2 for details.

module_version. The module_version field is used to identify the correct version of a file for download. Refer to section 3.1.2 for details.

transmission_timeout. The transmission_timeout field is used to specify the transmission timeout for the file. The time is expressed in milliseconds. The transmission_timeout is not applicable for the SOCWL file, it shall be set to 0xFFFFFF and ignored. For all other files, when the transmission_timeout is equal to 0xFFFFFF, it means that the transmission timeout definition is under the responsibility of the CA System.

number_of_service_entries. The number_of_service_entries field specifies the number of services that are protected by CI Plus. Each entry corresponds to a single service represented by the program number. The number of services shall be different from zero.

service_id. The service_id field identifies a service that is to be protected with CI Plus. This is a 16-bit field which serves as a label to identify this service from any other service. The service_id is the same as the program_number in the corresponding PMT (or SDT or EIT), as specified in [4]. A service_id value of 0x0000 may be used to indicate that all CA services of a network are CI Plus protected. A service_id value of 0xFFFF may be used to indicate that the CI Plus protection is determined using a CA system specific method.

When a service_id value of 0x0000 or 0xFFFF is used then this shall be the only service entry present in the loop and the number_of_service_entries field shall be specified as 1.

The service entries contained within the RSD_file may be locally scoped (on a per transport stream basis) or globally scoped (on a per network basis) as defined by the Service Operator. The service_id implicitly inherits the original network identity and transport stream identity of the transport stream in which the carousel is contained.

In a global network configuration, the service loop may contain service_ids that are not included in the current transport stream. In such configuration, it is the service operator's responsibility to ensure that service_ids are unique across the network such that any DVB CI service is not incorrectly enforced as CI Plus.

RSD_file_signature. The RSD_file_signature field is calculated over all preceding fields. It protects the file's integrity and provides single source authenticity with respect to its creator, the Service Operator. The signature is created according to RSA-SSA-PSS, 2048 (as specified in Annex I of [1]) and uses the Service Operator Private Key (SOQ) to calculate the signature and Service Operator Public Key (SOP) to verify the signature.

3.1.5 Additional requirements

CAS linked RSD detection is by default disabled in the CICAM and switching the RSD detection on or off is performed via a protected CA message. There are many existing mechanisms to deliver such a message securely to the CICAM; examples are per EMM, decoder data EMM, private data, ECM, or something else. A representative Simulcrypt system is shown in Annex A.

The exact message format is out of scope. Such a message shall be confidential and authentic and shall be preserved against replay. The CICAM shall preserve the RSD detection state over resets and reboots.

If revocation is activated, it is recommended that the revocation data is available on all transport streams of the network which carry CI Plus protected content.

3.1.6 Network (SI) signalling

The DVB linkage descriptor with a private linkage_type (See Table 3.9) provides a mechanism to signal the location of the CI Plus Data Carousel on a network. When used, the descriptor shall be within the scope of a private_data_specifier_descriptor with private_data_specifier value of `0x000040`, as defined in section Usage of CI Plus descriptors.

The linkage descriptor may be present in either the first loop of the NIT or in the first loop of a specifically identified BAT. The exact position of such linkage descriptor is Service Operator specific.

An example of network signalling using the linkage descriptor is shown in Annex B.

Table 3-9: CI Plus linkage_descriptor Syntax

Syntax	No. of bits	Mnemonic
`linkage_descriptor() {`		
`  descriptor_tag`	8	uimsbf
`  descriptor_length`	8	uimsbf
`  transport_stream_id`	16	uimsbf
`  original_network_id`	16	uimsbf
`  service_id`	16	uimsbf
`  linkage_type`	8	uimsbf
`  if (linkage_type == 0xCE){`		
`    data_broadcast_id`	16	uimsbf
`    service_operator_identity`	64	uimsbf
`    for (i=0; i<N; i++) {`		
`      private_data_byte`	8	bslbf
`    }`		
`  }`		
`}`		

The linkage descriptor is described in ETSI EN 300 468 [4], with the following semantics for the descriptor:

service_id: This 16-bit field identifies the service carrying the CI plus revocation data. This field may be specified as `0x0000` if the service is not specified and the linkage descriptor identifies the multiplex only.

linkage_type: This is an 8-bit field and shall be set to the user defined value of `0xCE` indicating a CI Plus linkage type.

data_broadcast_id: This 16-bit field identifies the data as belonging to CI Plus and shall always be set to the CI Plus data_broadcast_id value of `0x0122`, see section 3.1.2.1. This field shall be validated in conjunction with the linkage_type field to confirm that the linkage_descriptor identifies CI Plus revocation data.

service_operator_identity: This 64-bit field identifies the service operator for which the revocation information is intended. The value `0x0000000000000001` means the revocation information is intended for all operators. CI Plus LLP will allocate other values as required.

private_data_byte: This is an 8-bit field, the value of which is privately defined.

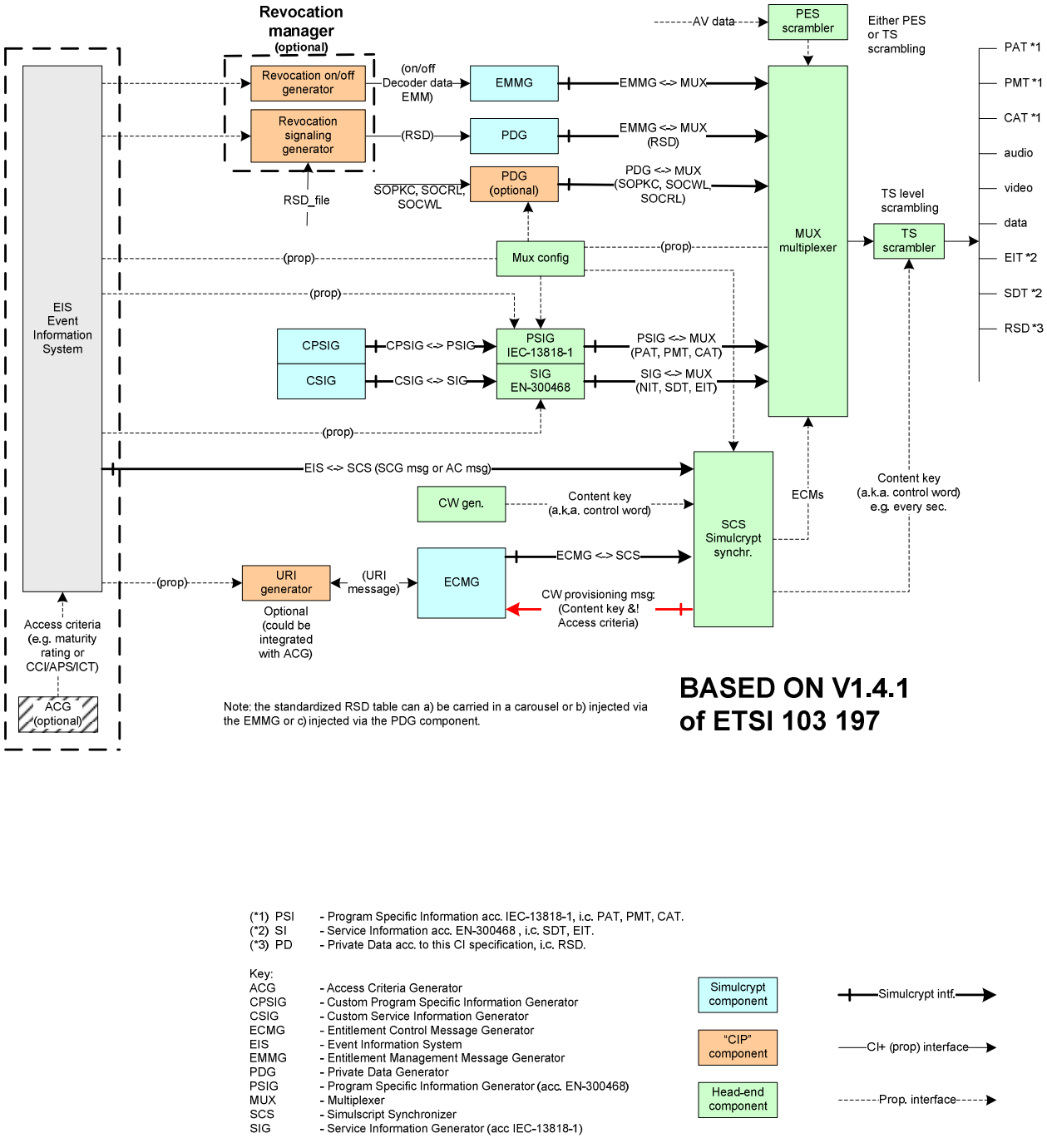
3.2 Usage of CI Plus descriptors

The CI Plus specification [1] defines the CI Plus LLP private descriptor ‘ci_protection_descriptor’ which is specified within the scope of the ‘private_data_specifier_descriptor’ [4], in section 10.1.1 for the host shunning function but does not define a ‘private_data_specifier’ value. A registered private data specifier value [5] is used and the value is defined as follows:

private_data_specifier `= 0x00000040 (CI Plus LLP)`

The CI Plus LLP ‘private_data_specifier’ shall prefix the CI Plus linkage linkage descriptor as defined in 3.1.6.

Annex A– RSD signalling in Simulcrypt (informative)



(*1) PSI - Program Specific Information acc. IEC-13818-1, i.c. PAT, PMT, CAT.
(*2) SI - Service Information acc. EN-300468 , i.c. SDT, EIT.
(*3) PD - Private Data acc. to this CI specification, i.c. RSD.

Key:

ACG	- Access Criteria Generator
CPSIG	- Custom Program Specific Information Generator
CSIG	- Custom Service Information Generator
ECMG	- Entitlement Control Message Generator
EIS	- Event Information System
EMMG	- Entitlement Management Message Generator
PDG	- Private Data Generator
PSIG	- Program Specific Information Generator (acc. EN-300468)
MUX	- Multiplexer
SCS	- Simulscript Synchronizer
SIG	- Service Information Generator (acc IEC-13818-1)

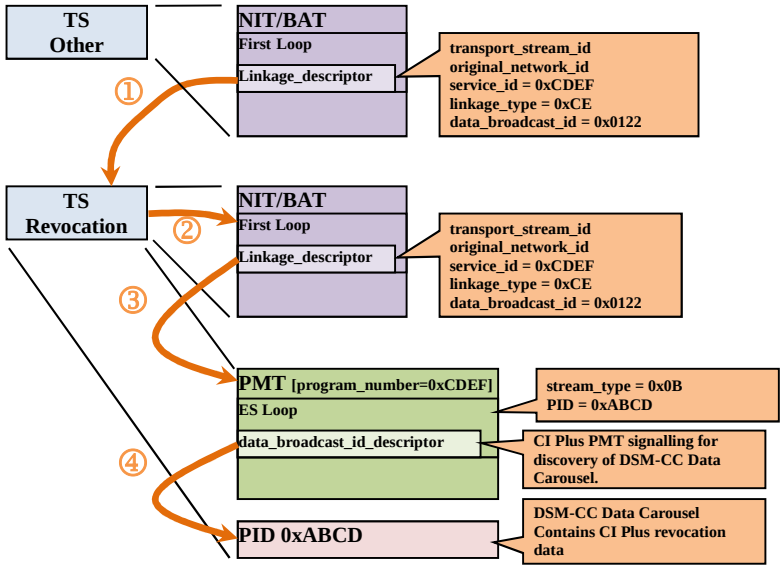
Simulcrypt component
"CIP" component
Head-end component
Simulcrypt intf.
CI+ (prop) interface
Prop. interface

Figure A-1: Example RSD integration in an Simulcrypt environment

Annex B– Network Discovery steps (informative)

The SI/PSI signalling network discovery mechanism for CI Plus revocation data is shown in Figure B-1:

Figure B-1: CI Plus revocation data discovery (Informative)



The CICAM behaviour is defined as follows where SI network signalling is present in the stream:

a) The CAM determines the revocation service according to the SI by interrogating the NIT/BAT (1,2), see section 3.1.6.

b) Whenever the Host tunes to the multiplex (3) that contains the revocation service then:

   i) CICAM loads the PMT of the service (3).
   ii) CICAM searches for a CI Plus data_broadcast_id_descriptor (section 3.1.2.1) and determines the carousel PID (4)
   iii) CICAM loads the carousel identifying the DownloadInfoIndication (DII) message ([2], Clause 10.1.3) and the modules transported
   iv) CICAM starts downloading the files starting by the RSD if the CA System only sends the information required in 3.1.1 and followed by the files reported in the RSD (see sections 3.1.2 and 3.1.4)
   v) CICAM authenticates the revocation data.
   vi) CICAM checks the revocation status of the Host and goes to limited operational if needed.