UNIVERSAL
POSTAL
UNION

ELECTRONIC CONSIGNMENT SECURITY DECLARATION GUIDELINES

October 2018

I. eCSD guidelines for designated operators

1 Objective

These guidelines are aimed at the designated operators (DOs) that are implementing the electronic consignment security declaration (eCSD) for mail consignments.

The purpose of the guidelines is to provide DOs with a simple description of how to implement the eCSD and where to find further information.

2 Context

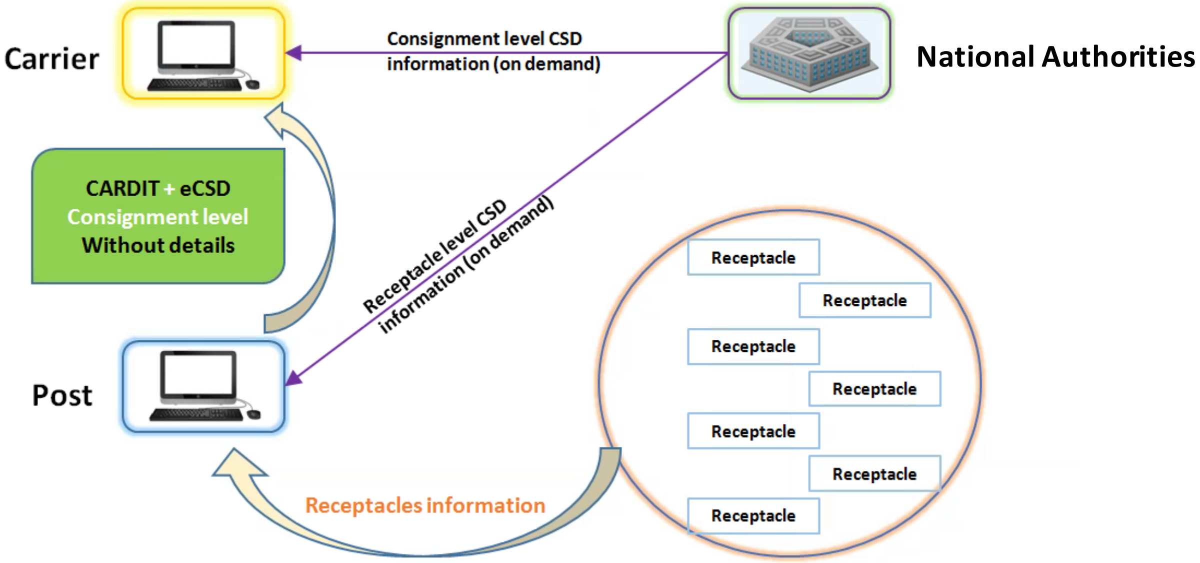
2.1 For the industry in general and for all parties involved in the supply chain, it is important that the transport of mail be carried out in an approved, secure and efficient way. This is done by preparing a CSD and forwarding the CSD data to the carrier, preferably electronically or, if that is not possible, as a paper CSD instead. In short, the eCSD provides information on by whom, how and when a consignment was secured.

2.2 In order to continue the pursuit of paper-free movement of mail, this document will focus mainly on the eCSD for mail. The eCSD is transmitted to the carrier as part of the CARDIT message.

2.3 The idea behind the eCSD is to ensure that the consignment is:

- secured upstream as early in the process as possible;
- protected from unlawful interference until it reaches the airport of destination.

2.4 The figure below shows the eCSD process.



3 Requirements

In order to be able to work with the eCSD, the following requirements must be met.

3.1 If the DO wants to assign a security status, the DO must be authorized to secure the mail (e.g. as a regulated agent), have a security programme that meets the requirements of the national authorities in the DO's home country, and observe the regulations of either the origin or destination authorities.

3.2 The DO must be able to send CARDIT messages with security information, i.e. CARDIT version 2.1 (UPU standard M48) or a newer version.

3.3 Good data quality and connectivity are important to ensure a smooth process without any delays.

3.4 The CARDIT must be generated and transmitted to the carrier before the mail is physically handed over to the carrier/ground handler.

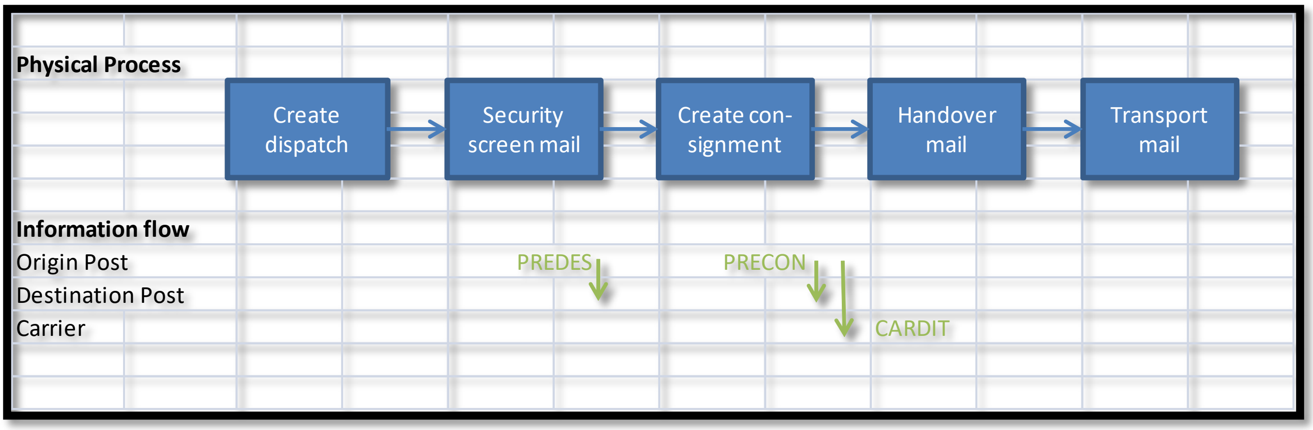
3.5 The DO must, upon request, be able to print the CSD (paper version of the eCSD).

3.6 The DO must log all screening activities so that, upon request, it is able to provide documentation proving that the mail was screened and identifying the screening methods that were used and the individual who performed the security screening.

3.7 The DO must archive the security information and keep the data for the duration of the flight, and for a minimum of 24 hours.

4 *Description of work*

The figure below shows the high-level process and the related information flow.



In the above process diagram, it is assumed that the security information is transmitted electronically. If this is not the case, the CSD must be printed after the consignment is created and handed over together with the mail. If the CSD is printed, it is strongly recommended that the CN 70 be used.

4.1 Create dispatch: The dispatch is created according to UPU regulations.

4.2 Security screen mail

4.2.1 The mail is screened according to the agreement between the DO and the national authorities in the DO's home country. It should be noted that, if items are removed from receptacles (e.g. owing to security issues), the receptacle information and the content of the PREDES message could change. The PREDES message should therefore be sent after the security screening has been completed.

4.2.2 As part of the screening process, the DO must log the following information:

– The time at which the mail receptacle was screened.

– The individual who screened the mail receptacle (it is recommended that the title of the employee be used).

– The screening methods used to screen the mail receptacle.

4.2.3 The log must meet the requirements set by the national authorities in relation to how the data is logged and archived. The log must be kept for the duration of the flight, and for a minimum of 24 hours.

4.2.4 The DO does not have to inform the contracted carrier(s) as to who was responsible for security screening the mail or when the eCSD was issued, provided that the information is logged and made available upon request.

4.2.5 It is recommended that there be close dialogue between the DO and the contracted carriers regarding requirements at transit points.

4.3 Create consignment

4.3.1 After the mail receptacles have undergone security screening, the consignment is created. At this point, the PRECON message is sent to the destination DO and the CARDIT message is sent to the carrier.

4.3.2 It is important to note that the CARDIT message is sent to the contracted carrier(s). It is the responsibility of the contracted carrier to inform subcontractors, if any, and ground handlers.

4.3.3 Annex 2 contains the completion instructions for each data element along with a sample of the physical CSD form.

The table below shows to whom the CARDIT message with eCSD information is to be sent for the different transport types.

Transport	*Description*	*Who receives eCSD from origin DO*	*Comments*	*Message exchange*
Direct transport	A to B	Contracted carrier	The contracted carrier can use another carrier as a subcontractor. The contracted carrier is responsible for forwarding the eCSD to the carrier that is flying. Closed transit sent via the DO at point B is considered direct transport from A to B. The DO at B will re-consign the mail together with its own mail.	CARDIT including eCSD security data sent from DO to contracted carrier.
Transhipment	A via B to C One carrier, two or more flights	Contracted carrier		CARDIT including eCSD security data sent from DO to contracted carrier.
Transhipment	A via B to C Two carriers, one of whom has the contract for the whole route	Contracted carrier	The contracted carrier is responsible for forwarding the CARDIT and eCSD to the other carrier. The CARDIT including eCSD security data is sent from the DO to the contracted carrier. Case 1: Contracted carrier flies the first part and subcontractor flies the second part: – First part: Contracted carrier has all required information. – Second part: At point B, the contracted carrier hands over the mail to the subcontracting carrier. The eCSD might be the original eCSD from the CARDIT or an eCSD (officially) created by that carrier in the event that the mail was re-secured. Case 2: Subcontracted carrier flies the first part and contracted carrier flies the second part: – First part: Contracted carrier supplies eCSD information to subcontracted carrier upon receipt of CARDIT(s).	CARDIT including eCSD security data sent from DO to contracted carrier. Current message gap between the two carriers.

Transport	*Description*	*Who receives eCSD from origin DO*	*Comments*	*Message exchange*
Transhipment (cont.)			– Second part: At point B, the subcontracted carrier hands over the mail to the contracted carrier. The eCSD might be the original eCSD from the CARDIT or an eCSD (officially) created by that carrier in the event that the mail was re-secured. Case 3: Contracted carrier flies none of the parts and the subcontractor flies the whole route: – First part: Contracted carrier supplies eCSD information to subcontracted carrier upon receipt of CARDIT(s). – As the whole route is carried by the subcontractor, the eCSD is managed by the subcontractor.	
	A via B to C Two carriers, each with their own contract	Both contracted carriers will receive the CARDIT (with eCSD). At transfer, the first carrier will supply the eCSD with updated information to the second carrier in a separate message	The transport segment qualifier (TSQ) 10 carrier will supply the eCSD data to the TSQ 20.	CARDIT including eCSD security data sent from DO to both carriers. Assumption: DO will only change transport data in the CARDIT and the eCSD will remain unchanged. Current message gap between the two carriers.

4.4 Handover mail

4.4.1 The full consignment is handed over to the ground handler/carrier before the agreed latest handover time at origin.

4.4.2 It is important to note that the full consignment cannot be handed over before the final version of the CARDIT (CARDIT function code 47) has been generated and transmitted to the contracted carrier.

4.5 Transport mail: The mail is transported to the destination by the carrier(s).

4.5.1 In order to ensure a smooth process without any delays, it is important to have good data quality and connectivity. If there is an issue in either one of these areas, the process will not run smoothly and the result will be delayed mail and/or extra workload to secure the mail.

4.5.2 It is therefore highly recommended that contingency plans be agreed on for all relevant issues with the contracted carrier(s). The contingency plans should be included in the contract between the DO and contracted carrier(s).

5 *Deliverables/output*

Following the above, the DO issues a CSD/eCSD.

Annex 3 provides an example of a CARDIT with the security information, the eCSD, and the printed CSD filled out with the relevant information.

6 *Further information*

Further information can be found by consulting the following:

– UPU standards
  - M39 CARDIT/RESDIT – Data flow version 2: Introduction and examples
  - M48 CARDIT V2.1
  - M49 RESDIT V1.1

– IATA Resolution 651: Consignment Security Declaration

For any questions, please contact standards@upu.int.

Annex 1 – Definitions/acronyms

– *CARDIT:* Message sent from a designated operator originating a consignment to a carrier (such as an airline) that is going to transport that consignment (definition in M39).

– *Carrier:* Includes the air carrier issuing the air waybill and creating the shipment record and all other air carriers that carry or undertake to carry the cargo under the air waybill or shipment record or to perform any other services related to such air carriage.

– *Consignment:* A set of one or more receptacles of a particular mail category, using a common transport on a particular occasion, from a specific place of loading to a specific place of final destination (definition in the UPU standards glossary).

– *Consignment security declaration (CSD):* The consignment security declaration provides regulators with an audit trail of how, when and by whom cargo has been secured along the supply chain.

– *Dispatch:* Mail aggregate for which, under the terms of a single dispatch agreement, responsibility is (to be) handed over from one mail processing centre to another and which is accounted for as a unit between the operators involved (definition in the UPU standards glossary).

– *Mail:* A system for physically transporting documents and/or parcels according to rules and regulations set by the UPU.

– *Designated operator (DO):* The designated operator issuing the CN 38 and sending the mail and CARDIT.

– *PRECON*: Message between designated operators that contains information about a consignment of mail which has been prepared for handover to the carrier responsible for transporting the consignment between the two designated operators concerned (definition in M39).

– *PREDES:* Message between designated operators containing information about a dispatch of mail which has been prepared by an exchange office for delivery to an exchange office in another country (definition in M39).

– *Receptacle:* Physical device which can be used to contain or carry mail so as to assist in its handling or transportation as a unit (definition in the UPU standards glossary).

– *Regulator:* Official authority imposing rules and regulations.

Annex 2 – Completion instructions per data element

This annex contains instructions for filling out the data elements. The name of the heading in the form is shown in brackets along with a corresponding number indicating its position on the form (see sample form provided at the end of the annex). Reference is made to the UPU technical standards on CARDIT messages for specific examples.

Security-status-party-code (Regulated Entity Category (KC, RA or AO) and Identifier – position 1)

The code and the unique identifier of the party under whose responsibility the security statement is issued. DOs will normally use a regulated agent (RA) or none of the mentioned possibilities.

Document message number (Unique Consignment Identifier – position 2)

The consignment identifier generated by the systems.

Departure-location-code (Origin – position 4)

The identification of the origin of the consignment (IATA location code).

Arrival-location-code (Destination – position 5)

The identification of the final destination of the consignment (IATA location code).

Departure-location-code for leg 2 (Transfer/Transit points (if known) – position 6)

The identification of an en-route stopping point where mail may be transferred to another aircraft or remain on board the same aircraft should be entered if known to the issuer (e.g. IATA three-letter airport or city code). Otherwise, this field may be left blank.

Security-status-code (Security Status – position 7)

This field contains the security status code of the entire consignment. The coded identification of the security status must be entered to indicate whether the consignment is secure for:

– passenger, all-cargo and all-mail aircraft ("SPX")

– all-cargo and all-mail aircraft only ("SCO")

– passenger, all-cargo and all-mail aircraft, in accordance with high-risk requirements ("SHR")

If the receptacles have different security statuses, the lowest status is used. For example, if a consignment is made up of a total of three receptacles, with two receptacles screened for SPX and one for SCO, the security status for the consignment will be SCO. See the table below.

Receptacle				*Consignment*
NSC	SPX	SCO	SHR	
1	0	0	0	NSC
0	0	0	1	SHR
0	0	1	0	SCO
0	0	1	1	SCO
0	1	0	0	SPX
0	1	0	1	SPX
0	1	1	0	SCO
0	1	1	1	SCO

0 = No receptacles with the security status

1 = One or more receptacle with the security status

Consignor-status-code and Consignor-ID (Received from – position 8)

If secured mail has been received from an account consignor, regulated agent or known consignor, the status code identifying the reason for screening is included here.

If the DO screens all mail, no matter where it comes from, before handing it over to the next party in the supply chain, this field will be empty.

Screenings-method-code (Screening Method – position 9)

This box must be left blank as the CSD will give only information at consignment level. However, the DO must retain records on the screening methods.

Screening-exemption-code, se-applicable-authority, se-applicable-regulation (Grounds for Exemption – position 10)

This box must be left blank as the CSD will give only information at consignment level. However, the DO must retain records on the screening methods.

Security-status-issuer (Security Status Issued by – position 12)

The name or employee ID number of the security manager of the party under whose responsibility the security statement is issued.

It should be noted that the DO is not obliged to give this information according to the regulations. However, the DO must log the information and is obliged to provide it on request.

Security-status-date-time (Security Status Issued on – position 13)

The date and time of issuance of the security status. This is when the consignment is closed and the CARDIT including the security information is generated.

It should be noted that the DO is not obliged to give this information according to the regulations. However, the DO must log the information and is obliged to provide it on request.

Cons-security-status-line (Additional Security Information – position 15)

Allows the option of including additional free text (e.g. if a carrier has specific requirements).

In addition to the above data elements, some other fields in the form must be filled out.

Contents of Consignment – position 3

This is always "Mail". Mail is considered to be consolidated, so the box "Consolidation" is always to be checked.

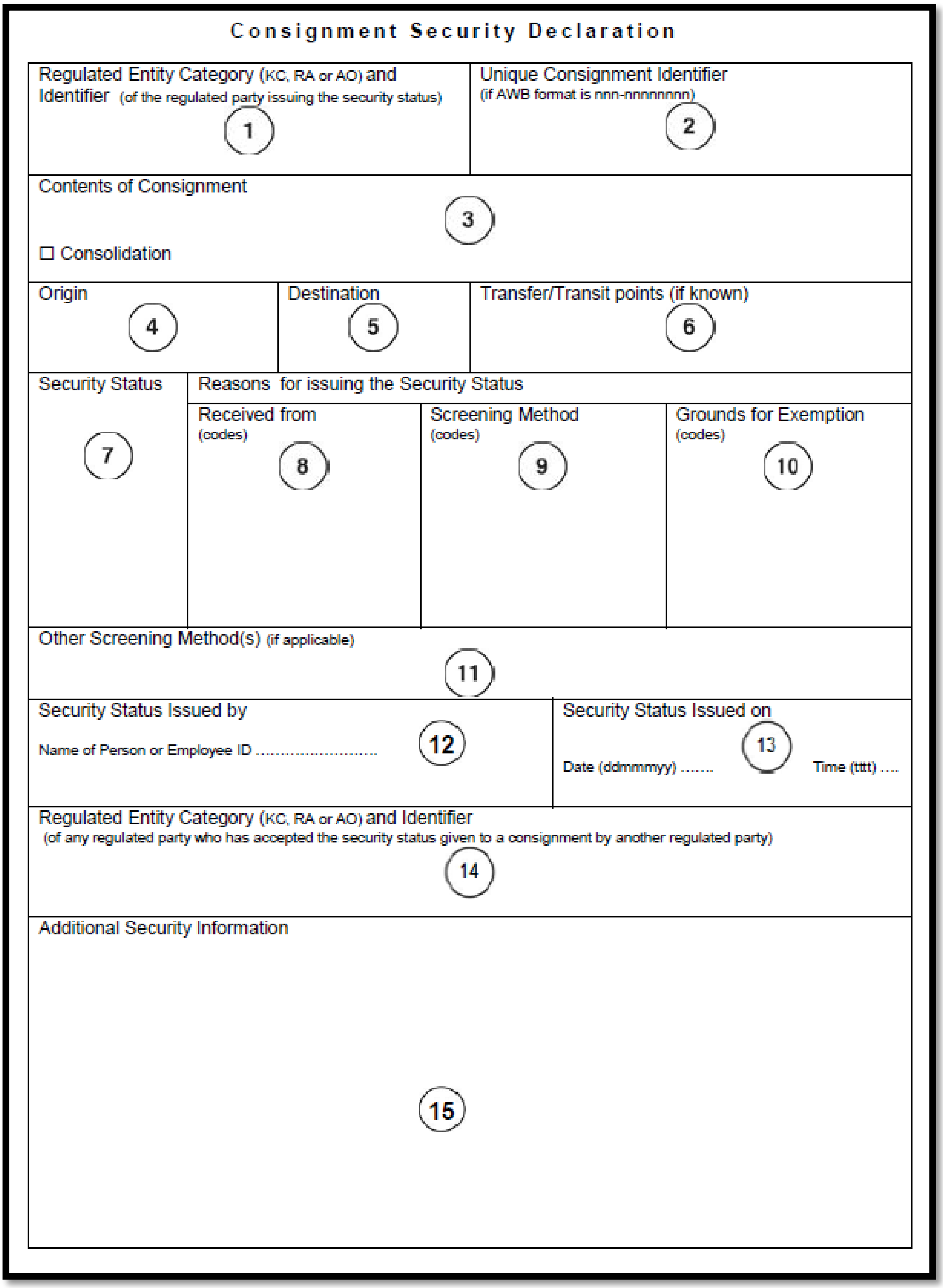
N.B. – In a CARDIT message, the presence of eCSD information implies that the mail is consolidated. Therefore, there is no indicator corresponding to the check box on the paper CSD.

Other Screening Method(s) (if applicable) – position 11

If the code entered in box 9 indicates that other means were applied, then text specifying the other means used must be entered.

Regulated Entity Category (KC, RA or AO) and Identifier – position 14

In this field, all the parties that have had the mail in their possession are listed with their code and identifier. As the DO is the issuing party, this field is not filled out.



Consignment Security Declaration

Regulated Entity Category (KC, RA or AO) and Identifier (of the regulated party issuing the security status) ①

Unique Consignment Identifier (if AWB format is nnn-nnnnnnnn) ②

Contents of Consignment ③

□ Consolidation

Origin ④

Destination ⑤

Transfer/Transit points (if known) ⑥

Security Status ⑦

Reasons for issuing the Security Status

Received from (codes) ⑧

Screening Method (codes) ⑨

Grounds for Exemption (codes) ⑩

Other Screening Method(s) (if applicable) ⑪

Security Status Issued by

Name of Person or Employee ID .... ⑫

Security Status Issued on

Date (ddmmmyy) .... ⑬ Time (tttt) ....

Regulated Entity Category (KC, RA or AO) and Identifier
(of any regulated party who has accepted the security status given to a consignment by another regulated party) ⑭

Additional Security Information

⑮

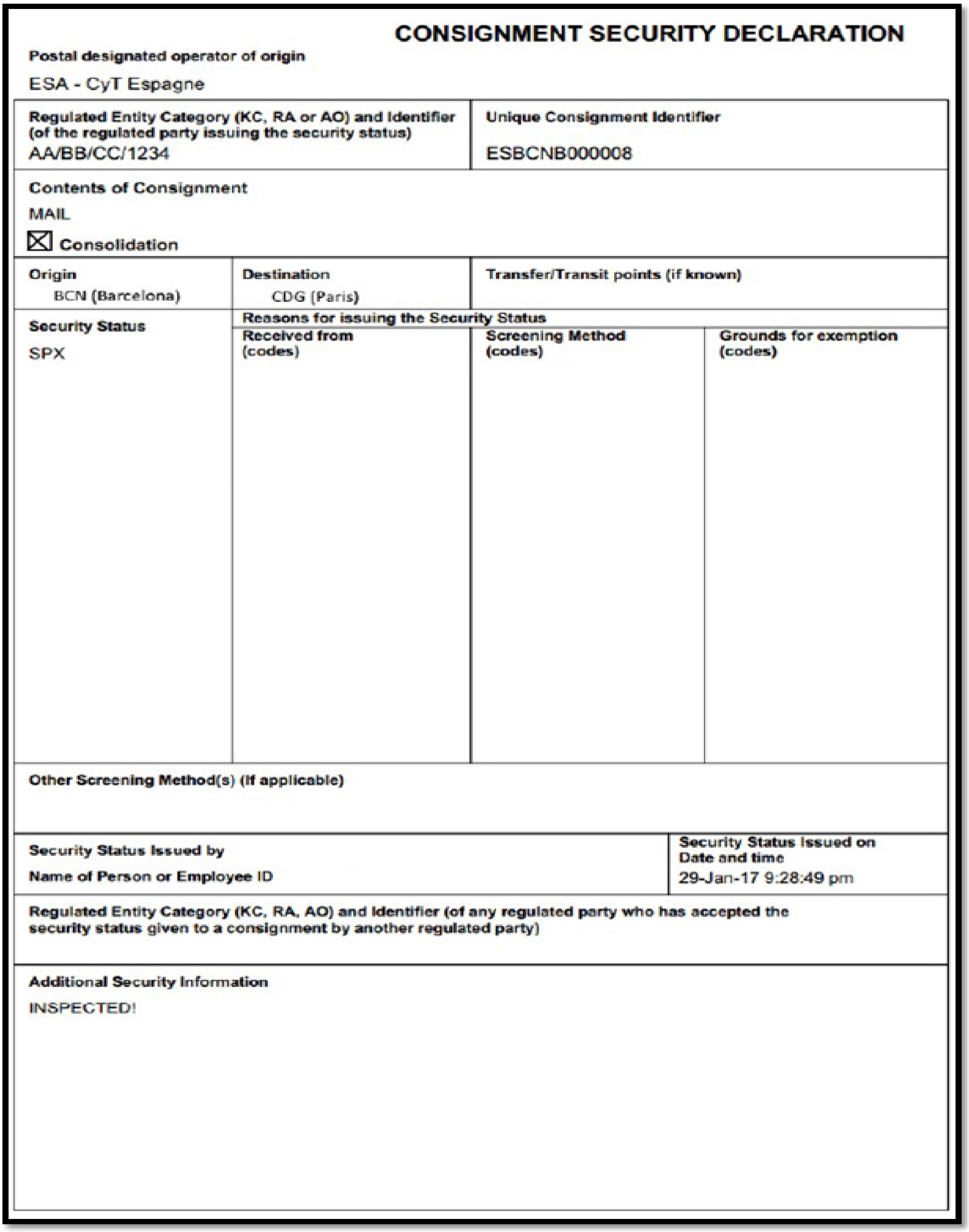
Annex 3 – Example of an eCSD (part of the CARDIT version 2.1 – M48)

The interchange below contains two CARDIT V2.1 messages. The second one is then illustrated with the corresponding paper CSD form.

Message *(segments related to eCSD in bold)*	*Explanation*
UNB+UNOA:2+ES101:UP+IBE11:DL+170129:2130+3'	Interchange from ES101 (Correos Spain) to IBE11 (airline Iberia)
UNH+3+IFCSUM:D:96ª:UN:CNS200'	First CARDIT V2.1 message in the interchange
BGM++ESBCNB000007+47'	Consignment ID: ESBCNB000007 Message function: 47 – Definitive (default value)
DTM+137:1701261556:201'	Consignment completion date–time: 26-Jan-2017, 15:56
FTX+ABK++A'	Consignment category: A (airmail)
RFF+AIA:AA/BB/CC/1234:SPX'	Consignment security information: Security status code: SPX (secured for passenger flight) Security status party code: AA/BB/CC/1234
DTM+539:1701261556:201'	Security status date–time: 26-Jan-2017, 15:56
RFF+AGE:ABCDEFGH'	Security status issuer: ABCDEFGH
RFF+AWN:FRCDGA'	Consignment destination: FRCDGA
GOR+1'	Applicable regulation, transport direction 1 (export)
TCC+U'	Mail class: U (letters)
EQN+1:NMB'	Number of receptacles: 1
QTY+101:15:KGM'	Weight of receptacles: 15 kg
TDT+20+IB0001+4'	Transport information, main carriage Flight: IB 0001
LOC+5+BCN:163:3'	Departure airport: BCN
LOC+7+CDG:163:3'	Arrival airport: CDG
DTM+189:1701270600:201'	Departure date–time: 27-Jan-2017, 06:00
DTM+232:1701270700:201'	Arrival date–time: 27-Jan-2017, 07:00
CNI++ESBCNBFRCDGAAUN70005001100150'	Receptacle ID: ESBCN…
GID++:BG'	Receptacle type: BG
MEA+WT+AAB+KGM:15'	Receptacle weight: 15 kg
UNT+25+3'	End of message
UNH+4+IFCSUM:D:96A:UN:CNS200'	Second CARDIT V2.1 message in the interchange
BGM++ESBCNB000008+47'	Consignment ID: ESBCNB000008 Message function: 47 – Definitive (default value)
DTM+137:1701292128:201'	Consignment completion date–time: 29-Jan-2017, 21:28

Message *(segments related to eCSD in bold)*	*Explanation*
FTX+ABK++A'	Consignment category: A (airmail)
RFF+AIA:AA/BB/CC/1234:SPX'	Consignment security information: Security status code: SPX (secured for passenger flight) Security status party code: AA/BB/CC/1234
DTM+539:1701292128:201'	Security status date–time: 29-Jan-2017, 21:28
RFF+AWN:FRCDGA'	Consignment destination: FRCDGA
GOR+1'	Applicable regulation, transport direction 1 (export)
TCC+U'	Mail class: U (letters)
EQN+1:NMB'	Number of receptacles: 1
QTY+101:18.5:KGM'	Weight of receptacles: 18.5 kg
TDT+20+IB0001+4'	Transport information, main carriage Flight: IB 0001
LOC+5+BCN:163:3'	Departure airport: BCN
LOC+7+CDG:163:3'	Arrival airport: CDG
DTM+189:1701300600:201'	Departure date–time: 30-Jan-2017, 06:00
DTM+232:1701300700:201'	Arrival date–time: 30-Jan-2017, 07:00
CNI++ESBCNBFRCDGAAUN70006001100185'	Receptacle ID: ESBCNB…
GID++:BG'	Receptacle type: bag
MEA+WT+AAB+KGM:18.5'	Receptacle weight: 18.5 kg
UNT+25+4'	End of message
UNZ+2+3'	End of interchange

CSD



CONSIGNMENT SECURITY DECLARATION

Postal designated operator of origin
ESA - CyT Espagne

Regulated Entity Category (KC, RA or AO) and Identifier (of the regulated party issuing the security status) AA/BB/CC/1234	**Unique Consignment Identifier** ESBCNB000008

Contents of Consignment
MAIL
☒ Consolidation

Origin BCN (Barcelona)	**Destination** CDG (Paris)	**Transfer/Transit points (if known)**	
	Reasons for issuing the Security Status		
Security Status SPX	**Received from (codes)**	**Screening Method (codes)**	**Grounds for exemption (codes)**

Other Screening Method(s) (If applicable)

Security Status Issued by **Name of Person or Employee ID**	**Security Status Issued on Date and time** 29-Jan-17 9:28:49 pm

Regulated Entity Category (KC, RA, AO) and Identifier (of any regulated party who has accepted the security status given to a consignment by another regulated party)

Additional Security Information
INSPECTED!

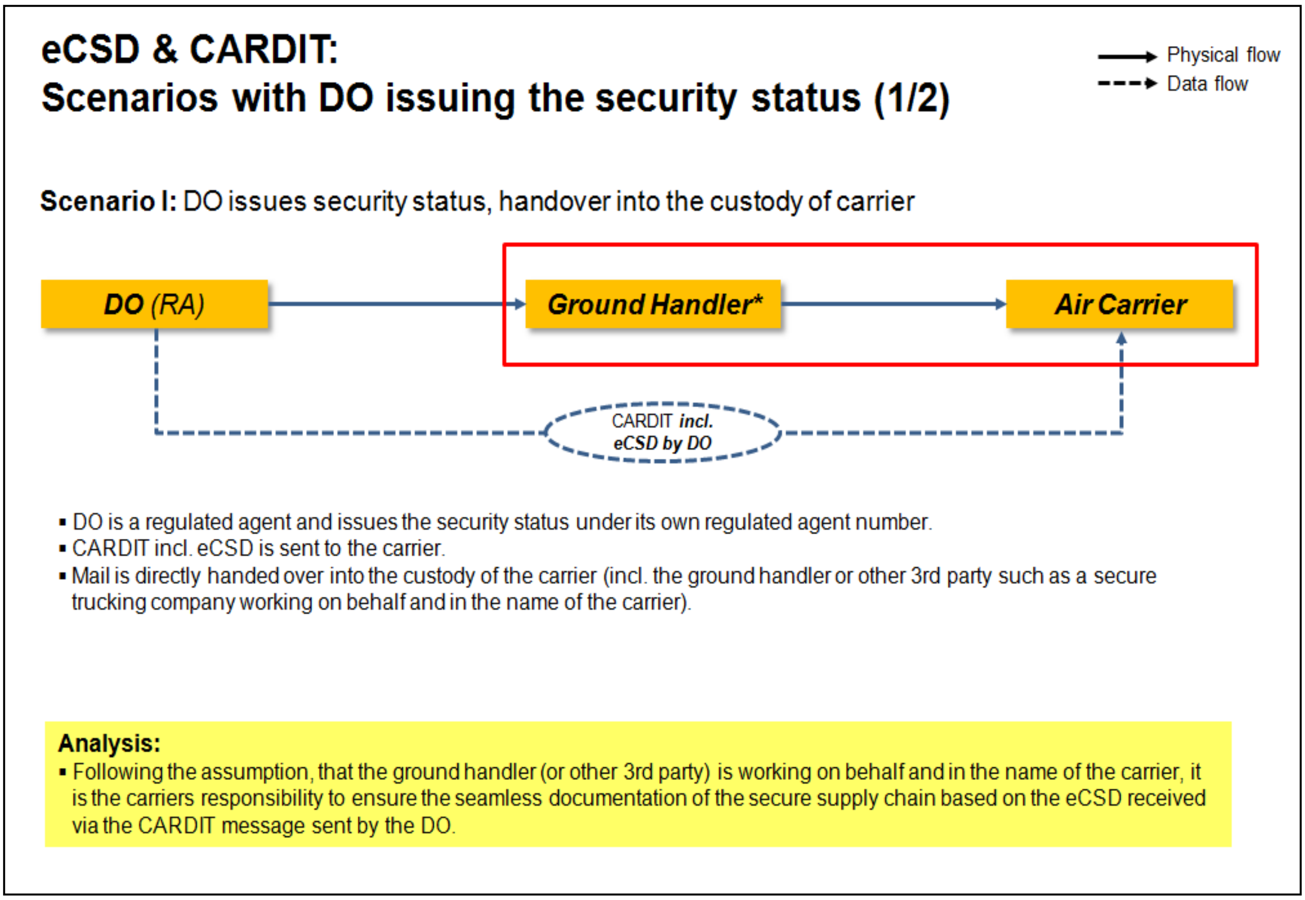
Annex 4 – eCSD and CARDIT scenarios

Below are scenarios in which the eCSD can be used. In other cases, the CARDIT must show that the mail is "not secured yet".

Assumptions:

- A DO can only include an eCSD with security approval in the CARDIT if the DO is a regulated agent.
- The CARDIT can only include an eCSD with security approval issued by a DO in the capacity of a regulated agent.
- The CARDIT cannot include an eCSD issued by a regulated agent other than the DO.
- Therefore, if the security status is not issued by the DO issuing the CARDIT, the CARDIT cannot include an eCSD with security approval, but must state "not secured yet" (NSC).

It is assumed that ground handlers work on behalf of carriers.



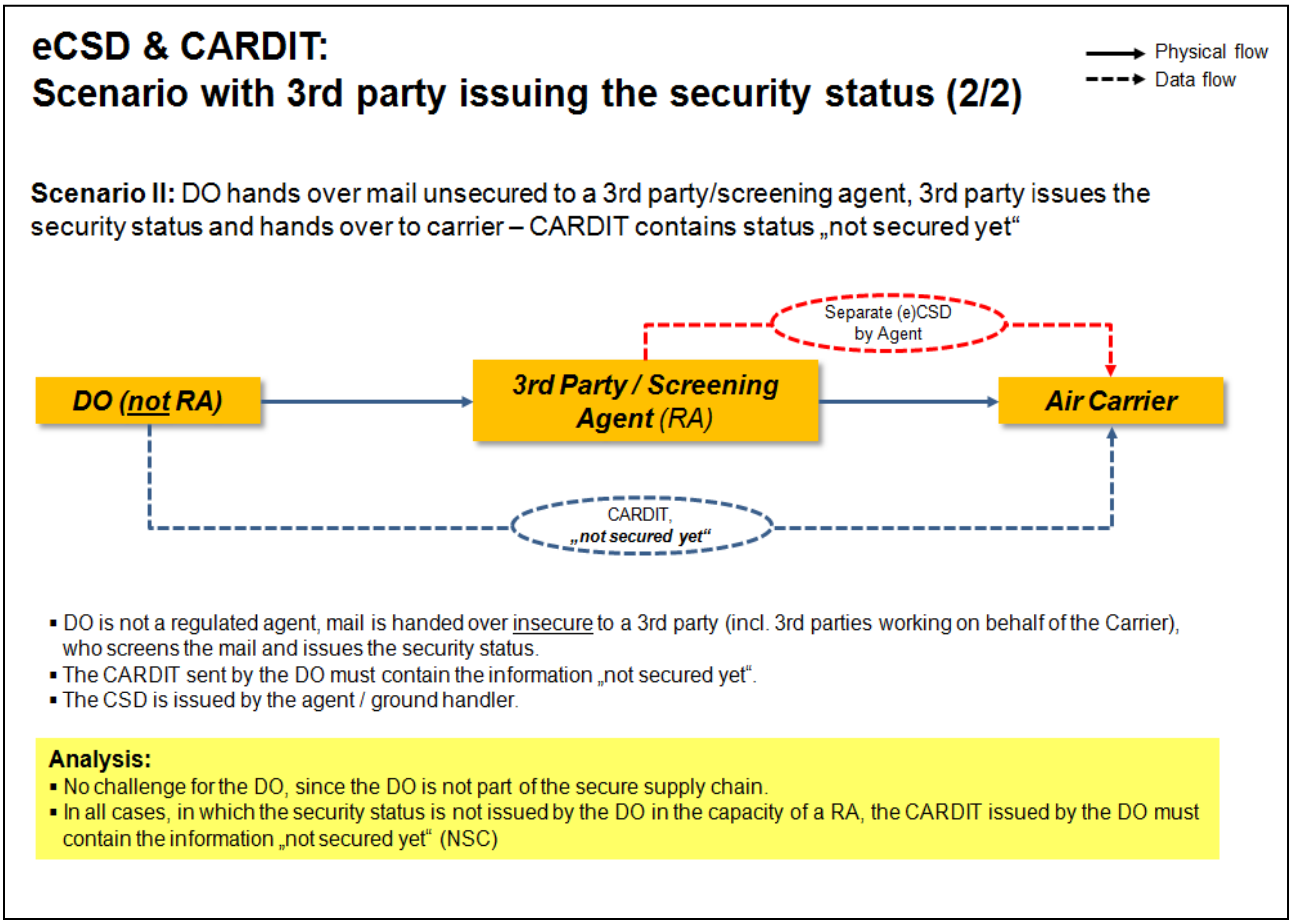
eCSD & CARDIT:
Scenarios with DO issuing the security status (1/2)

Scenario I: DO issues security status, handover into the custody of carrier

- DO is a regulated agent and issues the security status under its own regulated agent number.
- CARDIT incl. eCSD is sent to the carrier.
- Mail is directly handed over into the custody of the carrier (incl. the ground handler or other 3rd party such as a secure trucking company working on behalf and in the name of the carrier).

Analysis:

- Following the assumption, that the ground handler (or other 3rd party) is working on behalf and in the name of the carrier, it is the carriers responsibility to ensure the seamless documentation of the secure supply chain based on the eCSD received via the CARDIT message sent by the DO.



eCSD & CARDIT: Scenario with 3rd party issuing the security status (2/2)

Scenario II: DO hands over mail unsecured to a 3rd party/screening agent, 3rd party issues the security status and hands over to carrier – CARDIT contains status „not secured yet“

- DO is not a regulated agent, mail is handed over insecure to a 3rd party (incl. 3rd parties working on behalf of the Carrier), who screens the mail and issues the security status.
- The CARDIT sent by the DO must contain the information „not secured yet“.
- The CSD is issued by the agent / ground handler.

Analysis:

- No challenge for the DO, since the DO is not part of the secure supply chain.
- In all cases, in which the security status is not issued by the DO in the capacity of a RA, the CARDIT issued by the DO must contain the information „not secured yet“ (NSC)