UNIVERSAL POSTAL UNION

Certification process for UPU security standards S58 and S59

Berne 2020

Stl/Pro

I. Introduction

1 The objectives of the UPU security strategy are to educate, to raise awareness, and to increase security within all operations of the postal sector through compliance with UPU security standards S58 (General security measures) and S59 (Office of exchange and international airmail security).

2 This security strategy is designed to proactively create a process whereby restricted unions, or cooperative agreements between designated operators (DOs), can be a beneficial component of ensuring a secure universal service, for the benefit of their respective member countries, employees and the international mailing public. The protection of the international postal supply chain for the safe and secure exchange of mail among all member countries is critical for the continued viability of the postal sector. To enhance security among DOs, there is significant value in the concepts of peer support, sharing of international standards and best practices, and mutual cooperation among Posts that share similar security challenges.

3 The certification process is intended to provide a means to assist member countries in identifying opportunities to improve security, measure the degree of compliance to the UPU security standards, and formally recognize successful implementation of the standards.

II. Background

4 In 2010, the conveyance of explosive materials through courier air transport gave rise to international support for the development of postal security standards consistent with the established guidelines of other cargo transportation agencies for the protection of commerce in the international supply chain.

5 In response, the UPU Postal Security Group (PSG) developed general security standards in cooperation with Union member countries and other external stakeholders, such as the International Civil Aviation Organization (ICAO), International Air Transport Association (IATA), European Union (EU), Transportation Security Administration (TSA) and World Customs Organization (WCO). The security standards are in furtherance of article 08-001 of the Convention Regulations, which states that the aim of the postal security strategy is “to raise quality of service as a whole; increase employee awareness of the importance of security; create or reinforce security units; share operational, security and investigative information on a timely basis; propose to legislatures, wherever necessary, specific laws, regulations and measures to improve the quality and security of worldwide postal services; and provide guidelines, training methods and assistance to postal officials to enable them to deal with emergency situations that could endanger life or property or could hamper the mail transport chain, in order to maintain the continuity of operations”.

6 Convention article 8 was introduced following the 2016 Istanbul Congress, setting out the issue of postal security as follows:

> “Article 8
> Postal security
>
> 1 Member countries and their designated operators shall observe the security requirements defined in the UPU security standards and shall adopt and implement a proactive security strategy at all levels of postal operations to maintain and enhance the confidence of the general public in the postal services provided by designated operators, in the interests of all officials involved. This strategy shall include the objectives defined in the Regulations, as well as the principle of complying with requirements for providing electronic advance data on postal items identified in implementing provisions (including the type of, and criteria for, postal items) adopted by the Council of Administration and Postal Operations Council, in accordance with UPU technical messaging standards. The strategy shall also include the exchange of information on maintaining the safe and secure transport and transit of mails between member countries and their designated operators.
>
> 2 Any security measures applied in the international postal transport chain must be commensurate with the risks or threats that they seek to address, and must be implemented without hampering worldwide mail flows or trade by taking into consideration the specificities of the mail network. Security measures that have a potential global impact on postal operations must be implemented in an internationally coordinated and balanced manner, with the involvement of the relevant stakeholders.”

7 These provisions were initially approved (as article 9) at the 2012 Doha Congress, coming into effect on 1 January 2014. The UPU Postal Operations Council granted status 2 to S58 and S59 in February 2016.

8 To facilitate compliance with the approved postal security standards, the PSG, in collaboration with the United States Postal Inspection Service's global security programme and the CERT® programme at Carnegie Mellon University's Software Engineering Institute, developed a physical security risk assessment tool to measure the security of international mail processing centres (IMPCs) and similar transportation processing facilities, commonly referred to as international offices of exchange (OEs) and airmail units (AMUs).

III. Preparation and pilot implementation of a security certification process

9 In October 2015, document POC C 1 PSG 2015.2–Doc 6 was presented to the PSG. This document outlined a methodology for self-assessment, peer review and UPU validation of DOs' compliance with security standards S58 and S59.

10 The compliance certification process was piloted by the Postal Union of the Americas, Spain and Portugal and the Caribbean Postal Union. During the pilot project, seven DOs were assessed, and five were deemed to be in compliance with security standards S58 and S59.

11 The certification process has been aligned, as far as possible, with the existing UPU quality management certification process. It has also been developed in accordance with existing security standards and compliance certification processes of relevant external stakeholders, including ICAO, IATA and the WCO.

IV. Certification process

12 The certification process tested and refined during the pilot project can be summarized as follows:

a *Creation of a security action group:* It is recommended that a security action group be created within a restricted union or region, or among a number of Posts wishing to cooperate, support and share best practices in a mutual endeavour to maintain the UPU security standards. The security action group should comprise security focal points from the DOs involved. It is further recommended that a security certification committee be designated within the group. Details on the creation of the group and its membership should be provided in a letter to the PSG or via e-mail (security@upu.int).

b *Participation in a security training workshop:* Successful participation in a workshop, with content approved by the UPU security specialist (on behalf of the PSG), is vital to ensure that security experts are knowledgeable of the criteria outlined in S58 and S59, as well as the appropriate application of the self-assessment and risk assessment tools. The workshop content will include topics relevant to S58 and S59, along with guidance on implementing the security standards in critical facilities and instruction on the use of the self-assessment and risk assessment tools. Workshop participation should be limited to personnel with direct security-related responsibilities. Ideally, the workshop will be hosted by a DO in order to include a visit to an OE and to reinforce support for three days of instruction, practical exercises and applications within an identified critical facility. Workshop participants should, preferably, follow the online postal security course available on the UPU's distance learning tool, Trainpost, prior to attending the classroom training. An initial self-assessment based on at least one of the critical facilities of the attendee DO should be provided to the workshop coordinator before the workshop.

c *Self-assessment:* Using the guidance and tools provided at the security workshop, the security representatives are responsible for leading a thorough internal examination of postal operations and security within their respective Posts to assess compliance with the security standards. When compliance is achieved and certification is desired by a DO, the self-assessment (attached as Annex 1) and all additional required documentation (attached as Annex 2) must be compiled for submission to the respective security certification committee and the UPU International Bureau (IB).

d *Compliance review:* A DO seeking to attain certification must request a compliance review. Prior to submission of a review request, the DO will appoint a national certification coordinator/focal point, responsible for responding to inquiries for additional information and for assisting in arranging the compliance review. In order to initiate the review:

- The DO should request a review directly from the IB by sending an e-mail to the UPU security mailbox: security@upu.int. This request should include a self-assessment report, associated documentation, and photographic evidence of critical security measures in place within the DO's operations. The request will be evaluated by a team compromising the security manager and relevant regional programme of the Development and Cooperation Directorate. This evaluation will also ascertain event scheduling, resourcing and other project considerations. In order to be considered for review and certification, the DO must demonstrate a minimum of basic compliance with the security standards.

  The requesting DO will be required to pay the IB an amount to cover the average mission expenses for two security experts (see section VIII). The DO coordinator will also assist in arranging suitable hotel accommodation for the experts, in agreement with the IB. During the mission, the coordinator will fulfil the following duties: meet the experts on arrival; provide local transport as needed to accomplish the mission; allow access to all postal operations necessary to assess compliance with the standards; and provide the experts with the necessary administrative support for the review (office, incidental secretariat, supplies, photocopies, Internet access, etc.).

- The DO may request a review within the respective regional security action group. To ensure tracking and consistency, a copy of the request, together with all supporting documentation, must be sent to the UPU's Regional Project Coordinator (Annex 3) and the UPU security mailbox: security@upu.int. The regional security certification committee or restricted union security action group will, in coordination with the UPU Security Programme Manager, review the self-assessment documentation and determine readiness for peer review. A full on-site review will then be conducted within the specified critical facility, using the assessment criteria provided by the IB. The review will be conducted by the security action group members, along with representative(s) from the IB where possible. The requesting DO and security experts will agree on the settling of the expenses associated with the review.

e *Certification levels:* Modelled in alignment with the UPU quality management certification system. The results of the compliance review will determine the certification level demonstrated by security measures successfully implemented within the DO.

- Entry level or basic certification
- Level C (Bronze)
- Level B (Silver)
- Level A (Gold)
- Plus certification (+)

f *IB validation:* Following the peer or IB expert review, the final report, digital audit workbook and any associated documentation must be provided, with recommendation for the appropriate certification level. The audit team leader must e-mail the documents in Word format to the IB (Postal Security Programme Manager, security@upu.int) within 10 working days of the review, to validate the process and record the status. When all criteria have been fulfilled, the DO will be issued with a certificate signed by the UPU Director General. The certificate will be valid for three years; to maintain certification, the process must be repeated at the end of the three-year cycle. The IB invites recipient DOs to an official certification award ceremony attended by senior staff from the DO and the UPU. This ceremony will be held during the annual session of the POC or CA or on any other suitable occasion. The certificate will be presented by the Director General in his role as POC Secretary General. All other DOs will be informed of the certification results on the UPU website.

V. Certification languages

13 To ensure a standard level of assessment by consultants, only French or English (as working languages of the IB) should be used for the certification documentation and by the consultants during the on-site audit. The choice between these two languages lies with the operator. For questionnaires and correspondence on this topic between DOs and the IB, all UPU languages (French, English, Arabic, Portuguese, Russian and Spanish) may be used as usual.

VI. Certification level criteria

14 To reach one of the five security standards certification levels, specific criteria must be met. The assessments for both S58 and S59 are conducted, and scored, concurrently. This assessment utilizes a trained contingent of subject matter experts to review, evaluate, and reach a consensus-based decision for each section and subsection of security standards S58 and S59. The subject matter experts conduct evidence-based pre-assessment and on-site assessment through three main components: direct artefacts, indirect artefacts and affirmations.

15 The colour-coded chart below delineates the scale utilized to determine compliance with the security standards. The practice level characterizations used for each standard subsection include fully implemented (FI), largely implemented (LI), partially implemented (PI) and not implemented (NI). The goal level characterizations – satisfied (S) and not satisfied (NS) – are used for each standard section.

UPU Assessment Characterization scheme

Practice-level characterizations

Heat map	Name	Rule set	Point thresholds (0 to 10 scale)
FI	Fully Implemented (FI)	• One or more direct artifacts are present and judged to be adequate, • at least one indirect artifact and/or affirmation exists to confirm the implementation, and • no weaknesses are noted.	9 to 10
LI	Largely Implemented (LI)	• One or more direct artifacts are present and judged to be adequate, • at least one indirect artifact and/or affirmation exists to confirm the implementation, and • one or more weaknesses are noted.	7 to 8
PI	Partially Implemented (PI)	• Direct artifacts absent or judged to be inadequate • one or more indirect artifacts or affirmations suggest that some aspects of the practice are implemented, and • one or more weaknesses noted. OR • One or more direct artifacts are present and judged to be adequate, • no other evidence supports (indirect artifacts, affirmations) supports the direct artifact(s), and • one or more weaknesses are noted.	4 to 6
NI	Not Implemented (NI)	• Direct artifacts are absent or judged to be inadequate, • no other evidence (indirect artifacts, affirmations) supports the practice implementation, and • one or more weaknesses are noted.	0 to 3
N/A	Not Applicable (NA)	• The standard section does not apply (e.g. A6.2 only applies to organizations that use contractors for mail handling/transport operations or other sensitive functions)	?

Goal-level characterizations

Heat map	Name	Rule set
S	Satisfied (S)	• All associated practices are characterized as either Fully Implemented (FI) or Largely Implemented (LI) or Not Applicable (NA), with at least one practice characterized as FI or LI AND • The aggregation of weaknesses does not have a significant negative impact on goal achievement
NS	Not Satisfied (NS)	• All other cases
N/A	Not Applicable (NA)	• All practices are characterized as Not Applicable (NA)

16 Certification levels: Modelled in alignment with the UPU quality management certification system.

– *Entry level or basic certification* – Conferred once the review team has evaluated the completed pre-questionnaire and confirmed that all documents and photographs support the answers provided. An on-site visit is then scheduled with the DO to obtain the next certification. A copy of all required documentation is attached as reference. Basic certification must be achieved before any additional certification is granted.

– *Level C (Bronze)* – Category specifically reserved for the least developed countries, as recognized by the UPU. Upon completion of the on-site review, partially implemented (PI) subsections will be allowed in the following four subsections of S58 only: 5.1.3.1, Physical barriers, specifically fencing and perimeter walls; 5.2.3.5, Employee parking; 5.2.3.5, Visitor parking; 7.1.3, Mail transport vehicle resilience, specifically covered vehicles. All other subsections must meet or exceed the largely implemented (LI) requirements.

- *Level B (Silver)* – Upon completion of the on-site review, all subsections must be confirmed as fully implemented (FI) or LI and all sections as satisfied (S) by the review team.
- *Level A (Gold)* – Upon completion of the on-site review, all subsections must be confirmed as FI and all sections as S by the review team.
- *Equivalently certified DOs:* In some cases, the DO is obliged to comply with the security requirements of its national legislative or regulatory civil aviation authorities, or of external organizations such as ICAO, IATA and the WCO. The UPU recognizes that these third-party standards (e.g. ICAO's Regulated Agent and the WCO's Authorized Economic Operator) may be more rigorous than those set forth in S58 and S59, which are considered to be basic standards attainable by all DOs.

  If a DO complies with these higher-level security standards and can show that they are equivalent to or exceed S58 and S59 standards, it may be possible for the DO to be accredited with an equivalency recognition of S58 and S59 certification, provided all security measures have been fully implemented. This would facilitate cooperation and harmonize efforts among stakeholders to develop and maintain a secure supply chain system.

  In order for the IB to recognize a DO as meeting these standards, the DO must submit the attached equivalency assessment workbook (Annex 4), related documentation as detailed in Annex 2, and a written justification to the PSG either via letter or e-mail (security@upu.int). DOs must clearly demonstrate their comparative equivalency to the UPU security standards S58 and S59. Once the assigned security audit team has reviewed the documentation and confirmed equivalency, the DO will be considered compliant with the minimum S58 and S59 standards and will receive a letter to that effect from the Director of the Postal Operations Directorate (DOP).
- Level + (Plus): In cases where certification – Level A (Gold), Level B (Silver) or Level C (Bronze) – has been awarded to the OE of a DO that is exchanging electronic advance data (EAD) with all DOs requiring EAD, the certified DO may request evaluation for Level + (Plus). The following benchmarks must be met to achieve + status:

  a Qualification: The DO is deemed eligible to request + status if, as origin DO, it is transmitting ITMATT (v1) and PREDES to all destination DOs requiring EAD transmissions (as per article 08-002.1 of the Convention Regulations).

  b Criteria: The applicant DO must have been providing ITMATT and PREDES to those countries requesting EAD for at least three months before the certification request is made. The chart below indicates the mail classes concerned and their corresponding targets to achieve + status. Reviewers will examine at least six consecutive months of data to determine whether the DO can attain the target percentages for three of the months. This allows for any unforeseen circumstances (i.e. force majeure or industrial action).

  c For destination countries requiring pre-loading advance cargo information (PLACI), CARDIT messages with risk assessment status in AR flag (based on EAD checks) must be provided at the specified minimum percentages.

Category	*Target for ITMATT*	*Target for PREDES*	*Target for CARDIT*
EMS	98%	98%	80%
Parcels	90%	90%	75%
Tracked small packets	90%	90%	75%
Untracked packets	90%	90%	70%

At the time of the certification request, the applicant must have been transmitting EAD on at least 98% of all Express Mail Service (EMS) items being sent to those operators requesting EAD (refer to any parcel groups for appeals).

d Technical tools: Use of the CDS EAD confirmation tool (or equivalent) to ensure that the DO is not nesting items missing EAD into receptacles of postal dispatches, and that it has the ability to detect incoming referral messages from destination border security authorities and a standardized response protocol to these messages

The DO must provide evidence of these exchanges when the request for certification is made. This information will be evaluated remotely through UPU databases and through the data provided by the DO.

The DO should also provide a letter of request highlighting supporting information associated with the request. This information should be provided to the PSG via either mail or e-mail to the DOP Security mailbox (security@upu.int). Once all criteria are met, a (+) may be attached to the primary certification to indicate compliance with EAD exchange.

– *Recertification:* As stated above, certification that has been awarded to a specific OE of a DO will be valid for three years. In order to maintain certification the DO must be re-evaluated at the end of the three-year cycle. If the DO would like to maintain the same level of certification previously awarded to the OE – provided that the critical facility remains in the location where the original evaluation occurred – the DO must supply an updated self-assessment document along with time-stamped photographs depicting present-day conditions. Alternatively, evidence may be provided of continued compliance with national or international complementary regulations (e.g. ICAO's Regulated Agent and the WCO's Authorized Economic Operator). This information should be provided to the PSG, either via mail or e-mail to the DOP Security mailbox (security@upu.int). A copy should also be sent to respective restricted unions via the DO's traditional channels of communication. The UPU will assign a review team for this process. Once the reviewers are satisfied with the documentation, a WebEx interview will be scheduled and recertification may be completed remotely. The PSG may choose to conduct an on-site audit of any OE that is requesting recertification in an effort to confirm the information provided.

If a DO is seeking recertification above the previous level received, e.g. the DO is currently Silver and is pursuing Gold, an on-site review shall be required.

17 The following is a breakdown of the subsections and possible maximum scores:

– S58 5.1: 15 subsections, 150 maximum points

– S58 5.2: 12 subsections, 120 maximum points; manual: 3 subsections, 30 maximum points; automatic: 2 subsections, 20 maximum points

– S58 6.1: 7 subsections, 70 maximum points

– S58 7.1: 6 subsections, 60 maximum points

– S58 8.1: 5 subsections, 50 maximum points

– S58 9.1: 5 subsections, 50 maximum points

– S59 5.1: 10 subsections, 100 maximum points

– S59 6.1: 2 subsections, 20 maximum points

Maximum points for manual access control facility: 650

Maximum points for automatic access control facility: 640

VII. Financing of certification/recertification

a UPU

18 Work hours and related expenses incurred by the UPU Programme Security Manager in assessing requests and planning missions for compliance reviews will be funded by the UPU budget. The Union will also finance the organization and implementation of expert missions, the average costs of which are borne by the DOs.

b DOs

19 The DOs will bear the expenses of preparing and submitting self-assessment reports and requests for compliance reviews, including the preparation of the necessary documentation and translation, if applicable. DOs will also contribute to expert mission costs. If attendance at an award ceremony is desired by the DO, the operators concerned will finance the expenses of their representatives at the official certification award ceremony.

c Operators' contribution to consultants' missions

20 For DOs requesting review by IB-authorized experts, as an alternative to peer review, the contribution is set at 10,000 CHF per mission. To encourage participation from the DOs of the least developed countries, their mission contribution rate is set at 5,000 CHF.

Contributions should be paid to the following account:

CREDIT SUISSE

Account number:	0207–143 996 61–10
SWIFT code:	CRES CH ZZ 30R
Clearing:	507
IBAN:	CH53 0050 7014 3996 61010