European Union Aviation Safety Agency

Notice of Proposed Amendment 2024-08 (C)

in accordance with Article 6 of MB Decision 01-2022

Proposed amendments to Commission Regulation (EU) 2015/340 (air traffic controllers' licences and certificates)

Table of contents

Proposed regulatory material

The text of the amendment is arranged to show deleted, new or amended, and unchanged text as follows:

— deleted text is ~~struck through~~;

— new or amended text is highlighted in blue;

— an ellipsis '[…]' indicates that the rest of the text is unchanged.

Where necessary, the rationale is provided in *blue italics*.

Commission Regulation (EU) 2015/340 (Air traffic controllers' licences and certificates)

Article 4 — Definitions

For the purposes of this Regulation, the following definitions shall apply:

[…]

(14) 'licence' means a document issued in physical or electronic format and endorsed in accordance with this Regulation and entitling its lawful holder to exercise the privileges of the ratings and endorsements contained therein;

[…]

(33) 'licence issued in electronic format' means a licence issued on a self-contained mobile electronic visual display device. A licence issued in electronic format may be referred to as an 'electronic personnel licence';

(34) 'licence issued in physical format' means a licence issued on paper or other suitable material, including plastic cards;

(35) 'electronic personnel licence system' means an integrated system comprised of the computer hardware, network and communication facilities, computer software, validated data, users and associated regulatory framework to enable the issuance of licences in electronic format and the conduct of verification activities;

(36) 'self-contained mobile electronic visual display device' means a device such as a mobile phone, tablet or other mobile device that enables the generation and verification of the authenticity and validity of a licence issued in electronic format;

(37) 'medical certificate' means a document issued in either physical or electronic format containing the items specified in point ATCO.AR.F.005 of Annex II (Part ATCO.AR), confirming compliance with the medical requirements in Annex IV (Part ATCO.MED).

Article 12 – Transitional measures regarding the inclusion of the information regarding the medical certificate in licences issued in electronic format

1. By way of derogation from point ATCO.AR.D.002(g) of Annex II (Part ATCO.AR), Member States may decide to not include in a licence issued in electronic format the mandatory information regarding the medical certificate of the licence holder as required in Appendix 2 to Annex II (Part ATCO.AR) until [date of entry into force/applicability date + 10 years]. In that case, the holder of a licence issued in electronic format shall hold a medical certificate issued in physical format in accordance with Annex IV (Part ATCO.MED).

ANNEX I (Part ATCO)

ATCO.A.005 Application for the issue of licences, ratings and endorsements

[…]

(c) The licence shall remain the property of the person to whom it is issued, unless it is revoked by the competent authority. ~~The licence holder shall sign the licence.~~

[…]

ATCO.A.017 Obligation to present documents

(a) A (student) air traffic controller shall without undue delay present his or her licence, medical certificate, and a personal identification document (containing his or her photo) for inspection upon request by an authorised representative of a competent authority.

(b) The holder of the (student) air traffic controller licence issued in electronic format shall report to the competent authority that issued his or her licence the loss or theft of the self-contained mobile electronic visual display device on which the licence was generated.

ATCO.A.020 Revocation and suspension of licences, ratings and endorsements

(a) Licences, ratings and endorsements may be suspended or revoked by the competent authority according to ATCO.AR.D.005 when the licence holder does not comply with the requirements of this Part.

(b) When ~~the~~ licence holders ~~have~~s ~~his/her~~ their licence suspended or revoked, they ~~he/she~~ shall immediately return the licence issued in physical format to the competent authority according to the administrative procedures established by that authority.

(c) With the issue of the air traffic controller licence, the student air traffic controller licence is revoked and shall, in case it is a licence issued in physical format, be returned to the competent authority ~~which is issuing the air traffic controller licence~~.

ANNEX II (Part ATCO.AR)

ATCO.AR.D.001 Procedure for the issue, revalidation and renewal of licences, ratings, endorsements and authorisations

(a) The competent authority shall establish procedures for the application, issue and exchange of licences, issue of ratings and endorsements, as well as the revalidation and renewal of endorsements. These procedures may include:

(1) the issue of temporary OJTI authorisation and temporary assessor authorisation; and

(2) if applicable, the authorisation for assessors to revalidate and renew unit endorsements in which case assessors shall submit all records, reports and any other information to the competent authority as defined in such procedures.

(b) Upon receiving an application and, if relevant, any supporting documentation, the competent authority shall verify the application completeness and whether the applicant meets the requirements set out in Annex I.

(c) If the applicant meets the applicable requirements, the competent authority shall issue, revalidate or renew, when appropriate, the relevant licence, rating(s) and endorsement(s) using only one of the two formats for licences established in Appendix 1 ~~of~~ to Annex II. The temporary OJTI authorisation referred to in point ATCO.C.025 and the temporary assessor authorisation referred to in point ATCO.C.065 shall be issued as a separate document wherein the privileges of the holder as well as the validity of the authorisation shall be specified.

(d) For the purpose of reducing unnecessary administrative burden, the competent authority may establish procedures for establishing a unique date of validity for several endorsements. In any case, the validity periods of the endorsements concerned shall not be extended.

(e) The competent authority shall replace the air traffic controller licence if necessary for administrative reasons and when point (XIIa) of the licence issued in physical format is completed and no further space remains. The date of the first issue of the ratings and rating endorsements shall be transferred to the new licence.

AMC1 ATCO.AR.D.001(a)(2) Procedure for the issue, revalidation and renewal of licences, ratings, endorsements and authorisations

EXERCISE OF LICENCE PRIVILEGES BEFORE THE INFORMATION IN THE ELECTRONIC PERSONNEL LICENCE SYSTEM HAS BEEN UPDATED

When licences issued in electronic format are used, the competent authority may develop procedures to allow privileges to be exercised by the licence holder before the information in the electronic personnel licence system has been updated following the issue, revalidation or renewal of a unit endorsement. The period for application of this procedure should be a maximum of 8 weeks after successful completion of the applicable examination(s) and assessment(s).

GM1 ATCO.AR.D.001(e) Procedure for the issue, revalidation and renewal of licences, ratings, endorsements and authorisations

ADMINISTRATIVE REASONS

For the purpose of issuing a new licence, administrative reasons may be the following but are not limited to:

(a) loss of the licence issued in physical format or of the self-contained mobile electronic visual display device;

(b) theft of the licence issued in physical format or of the self-contained mobile electronic visual display device;

(c) significant damage leading to illegibility~~.~~ ;

(d) replacement of the self-contained mobile electronic visual display device.

ATCO.AR.D.002 Licences issued in electronic format and establishment of an electronic personnel licence system

(a) The competent authority may decide to issue licences in electronic format to all licensed groups of personnel, certain groups of personnel or certain individuals. For the same type of licence, the same individual licence holder cannot hold both a licence issued in physical format and a licence issued in electronic format.

(b) By way of derogation from point (a), the (student) air traffic controller is entitled to have a licence issued in electronic format together with a document in physical format, issued in accordance with point ATCO.AR.D.001, allowing the licence holder to exercise the privileges of the licence for a maximum period of 8 weeks after successful completion of the applicable examination(s), pending the endorsement of the licence issued in electronic format.

(c) The competent authority having issued a licence in electronic format shall ensure that authorised personnel can verify the authenticity and validity of the licence and are able to determine its privileges.

(d) The authenticity and validity of a licence issued in electronic format shall be electronically verifiable:

(1) online when an internet connection is available; or

(2) offline when no internet connection is available through a means that imposes no undue burden on the authorised personnel verifying the authenticity and validity of the licence.

(e) When the competent authority issues licences in electronic format, it shall establish and implement procedures for the establishment and operation of an electronic personnel licence system.

(f) The electronic personnel licence system shall ensure interoperability, security, confidentiality, data protection, authentication, and accessibility of the licences issued in electronic format.

(g) A licence issued in electronic format shall include the current information on the medical certificate with class, expiry date and any medical information deemed relevant by the competent authority in accordance with Part ATCO.MED.

(h) The competent authority shall develop and apply an administrative procedure for the update of the licence issued in electronic format, including its limitation, suspension or revocation.

(i) When holders of a licence issued in electronic format have reported the loss or theft of the self-contained mobile electronic visual display device on which their licence was issued, the competent authority shall invalidate this licence and generate a new licence licence on another device declared by the holder and to which they have access.

AMC1 ATCO.AR.D.002 Licence issued in electronic format and establishment of an electronic personnel licence system

ELECTRONIC PERSONNEL LICENCE SYSTEM

1. DEFINITIONS

The following definitions apply to this Acceptable Means of Compliance.

'Issuing authority' means a competent authority with competence to issue licences, including licensing authorities from third countries.

'Mdoc' means a document or application that resides on a self-contained mobile electronic visual display device or requires such a device as part of the process to gain access to the document or application.

'Verifying authority' means a competent authority with competence to verify the validity and authenticity of licences, including authorities from third countries with competence to verify the validity and authenticity of licences.

2. ABBREVIATIONS

API	application programming interface
CSR	certificate-signing request
EPL	electronic personnel licence
EPLAPP	application for a licence issued in electronic format
EPLDM	electronic personnel licence data model
EPLDS	data set for the licence issued in electronic format
EPLHD	electronic personnel licence holder device
EPLRAP	reading application for licences issued in electronic format
EPLRD	electronic personnel licence reading device
EPLSYS	electronic personnel licence system

HDPKIC	holder device public key infrastructure certificate
IAPKIC	issuing authority public key infrastructure certificate
IAS	issuing authority server
JWT	Java web token
LICSYS	licensing system
MSO	mobile security object
PKI	public key infrastructure
RDPKIC	reading device public key infrastructure certificate
TLS	transport layer security
URL	uniform resource locator

3. PRIOR TO IMPLEMENTATION

Once an issuing competent authority has decided that one or several types of licence will be issued in electronic format, it should decide on one of the following options:

(a) All the licences of that type will always be issued in electronic format.

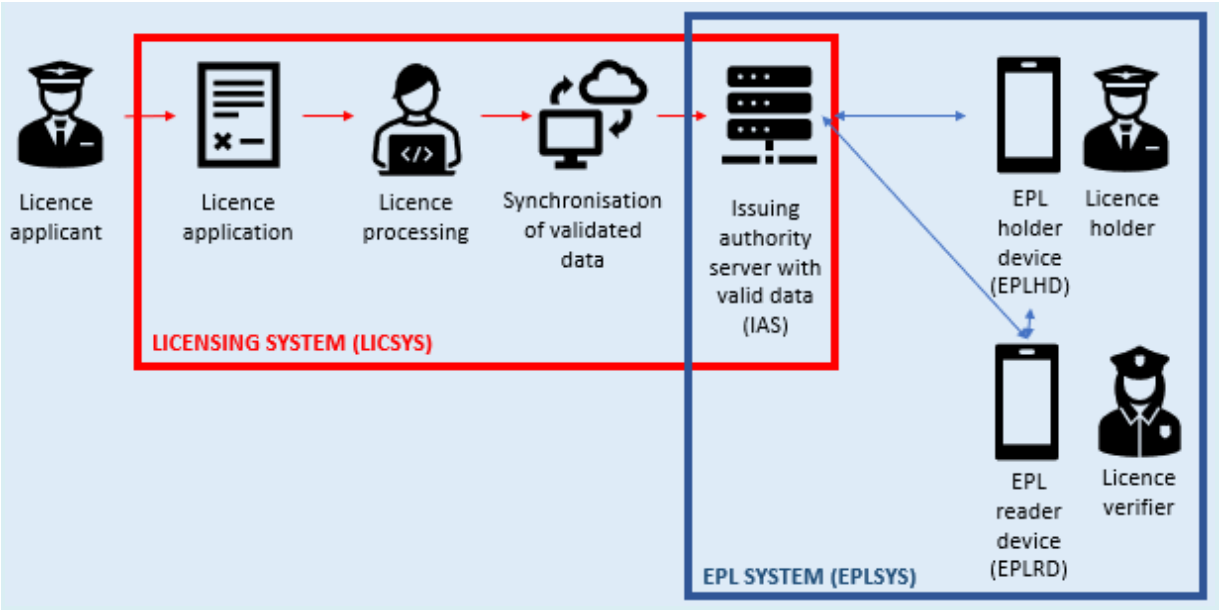
(b) The two formats of the licence will be maintained (both physical format and electronic format).

(c) If option (b) is selected, it also needs to be decided whether the licence issued in electronic format will be issued just for certain groups of personnel or specific individuals.

3.1 Licensing system and electronic personnel licence system

The licensing system (LICSYS) used by an issuing authority is not the electronic personnel licence system (EPLSYS). The LICSYS and the EPLSYS are independent systems that share the source where the information is stored: the issuing authority server (IAS) — see Figure 1.

Figure 1 — LICSYS and EPLSYS schema



(a) The LICSYS provides the tools that allow an issuing authority to manage the licence information in accordance with its procedures for issuing, updating and invalidating the licence data. Only data that has been validated in the national LICSYS and stored as valid licence information can be used by the EPLSYS.

(b) The LICSYSs used by different issuing authorities might be different one from another: maybe some issuing authorities use an existing market solution, and others have developed their own LICSYS in accordance with their needs. Each LICSYS should work in accordance with the requirements of the regulatory framework that applies to the issuing authority (such as EU regulations, national regulations and national procedures established for the issuance, renewal, revalidation, suspension and revocation of a licence).

(c) The EPLSYS provides the means by which the licence data and the medical data stored in a server of an issuing authority are converted to an mdoc and are transferred to the holder device (EPLHD).

(d) The EPLSYS also provides the method by which external parties (inspectors or other parties, who will be generally called 'verifiers') can get the licence information on an electronic personnel licence reading device (EPLRD) and proceed with the verification the authenticity and validity of the of the licence issued in electronic format. Both the EPLHD and the EPLRD will need the installation of software that can process the licence information..

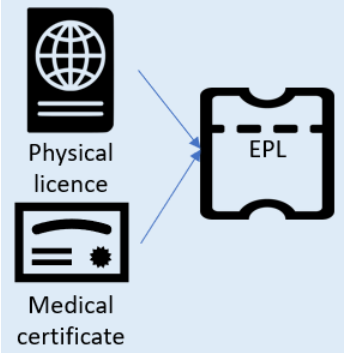
3.2 The data set for the licence issued in electronic format (EPLDS)

(a) Each type of licence issued in electronic format has a specific set of data defined in the Appendices to each applicable Regulation, such as Commission Regulation (EU) 2015/340 (air traffic controllers' licences and certificates).

(b) In contrast to licences issued in physical format, licences issued in electronic format share a common structure, a common data set of information that is the same for all types of licences. This common structure has been included in the affected regulations, and in this AMC it will be referred to as the data set for the licence issued in electronic format (EPLDS).

(c) The EPLDS includes both the licence information of the licence issued in physical format and the medical certificate information of the licence holder, if applicable, as certain types of licence might not require a medical certificate) — see Figure 2.

Figure 2 — Data sources for the licence issued in electronic format



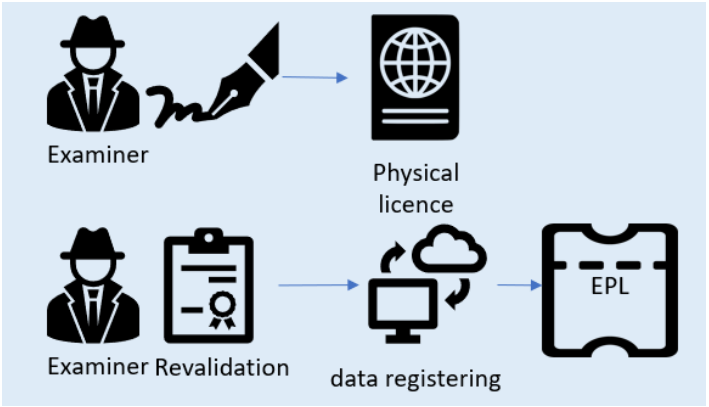
(d) Generally, the EPLDS is composed of two subsets of data: a subset related to the licence data issued in physical format and a subset related to the medical certificate — see Table 1. This creates unavoidable differences between the licence issued in physical format and the licence issued in electronic format.

Table 1 — Information data set for each type of document

Document	Licence data set	Medical data set
Physical licence	Yes	No
Medical certificate	No	Yes
EPL	Yes	When applicable

(e) Some licences issued in physical format allow the endorsement of rating revalidations by writing them down on the licence issued in physical format. The revalidation information is handwritten and signed by an examiner. Therefore, revalidations, even though they are part of the licence issued in physical format, are validated by a person in a different role: the examiner instead of the officer who signs the issuance of the licence. This creates a third source of licence information of licences issued in electronic format — see Figure 3.

Figure 3 — Revalidations as a third data source



3.3 The term ‘licence’ and life cycles

(a) A licence issued in electronic format should be seen as a representation of the licence information of the licence issued in physical format and the medical certificate at a particular moment in time. It will remain valid as long as the licence issued in physical format and the medical certificate remain the same, but the moment one of these subsets of data varies, this

representation is no longer valid, and another licence issued in electronic format supersedes the existing licence issued in electronic format. Therefore, licences issued in electronic format should be considered something that works in a similar way to how medical certificates do. The invalidation of a licence issued in electronic format does not equal the invalidation of a licence issued in physical format or the invalidation of a medical certificate; it only means that the information in that representation is no longer accurate.

(b) Both the licence issued in physical format and the licence issued in electronic format grant the licence holder the right to make use of the privileges given by them, and it makes no difference having one format or the other, but technically they are not the same because of the particularities of the licence issued in electronic format.

3.3.1 Issuance of a licence

Referring to licences (either licences issued in electronic format or licences issued in physical format), the issuance could be considered as the process by which the data of the document is validated by the issuing authority and the outcome is a valid licence being delivered to the licence holder. This process contains two important actions:

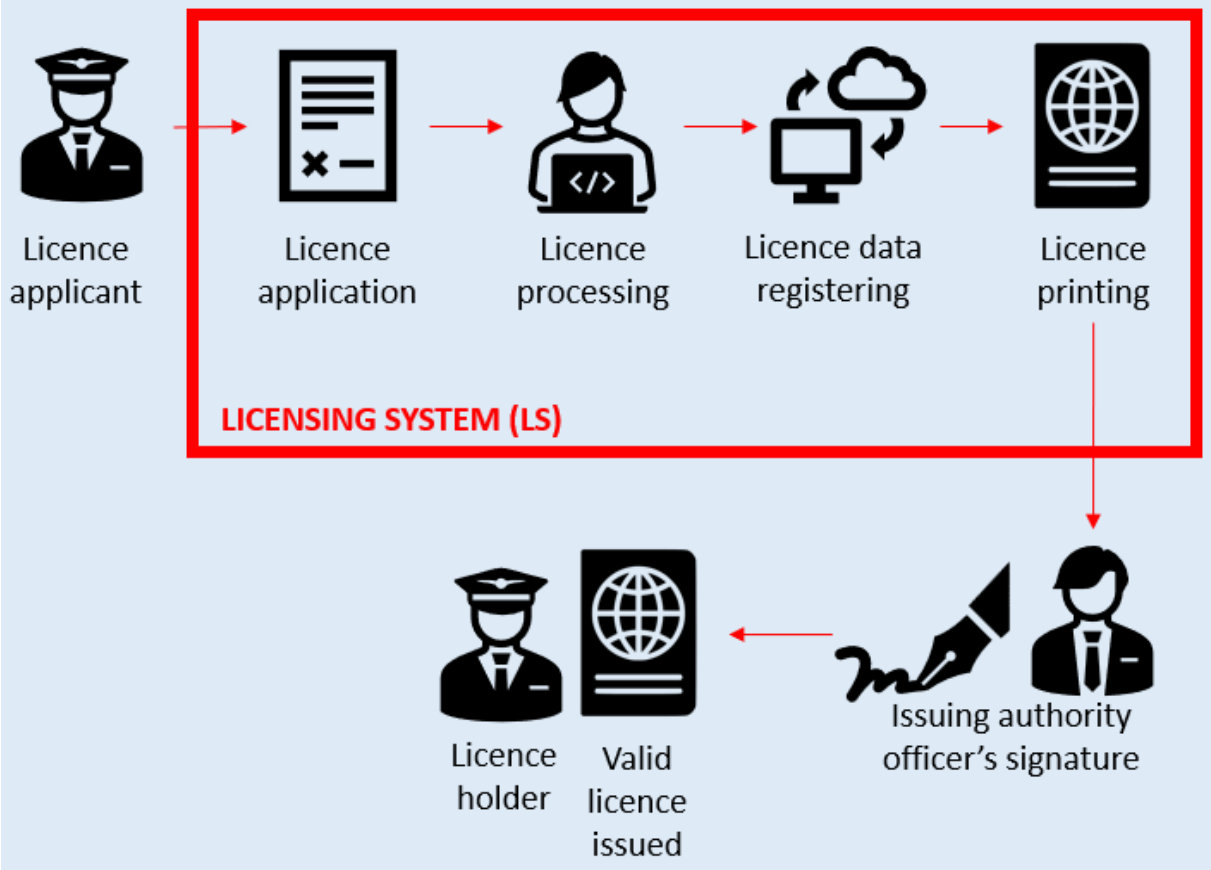
(a) generation of the licence: action by which the licence data is inserted into a document (independently of the format of the document, electronic or not);

(b) validation of data: action by which the licence data at a specific moment in time is rendered valid by a signature that comes from the competent authority.

3.3.1.1. Physical licence issuance process

When using licences issued in physical format, a simplification of the issuance process should be as shown in Figure 4:

Figure 4 — Physical licence issuance process



(a) A licence applicant (or holder, if a previous licence has already been issued), fills out a licence application and submits it to the issuing authority.

(b) The issuing authority officers process the application following the established procedures.

(c) The licence information is registered in the LICSYS and the licence is printed.

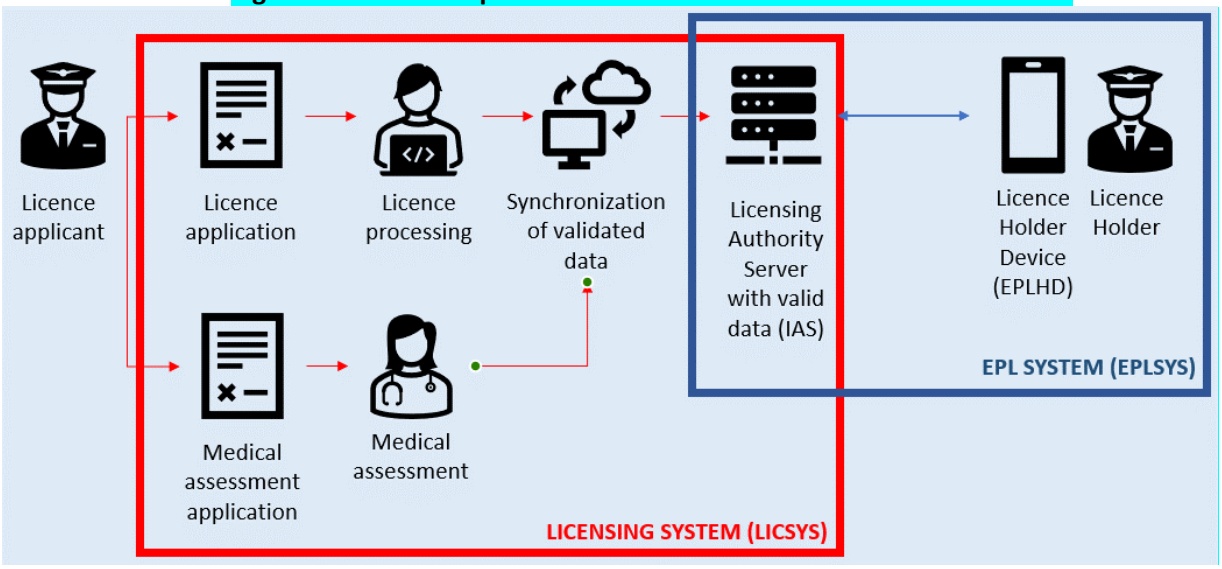
(d) The licence information is validated by an issuing authority officer's signature.

(e) The licence is given to the applicant, who becomes a licence holder.

3.3.1.2. Issuance process of the licence issued in electronic format

With an EPLSYS, the issuance process of a licence issued in electronic format would be as shown in Figure 5:

Figure 5 — Issuance process of the licence issued in electronic format



(a) A licence applicant (or holder, if a previous licence has already been issued) completes a licence application and submits it to the issuing authority.

(b) The issuing authority officers process the application following the established procedures.

(c) The licence data set information is registered in the EPLSYS. In order to be validated, it has to be signed digitally by an officer of the issuing authority.

(d) Since the medical information is included in the licence issued in electronic format, it needs to be available in the IAS. If it is not, it will be registered and validated by the medical assessor.

(e) Once validated, the licence data and the medical data set are stored in the IAS.

(f) The licence holder needs to install the application for the licence issued in electronic format (EPLAPP) on the EPLHD and send a request for the generation of a licence issued in electronic format to this specific device.

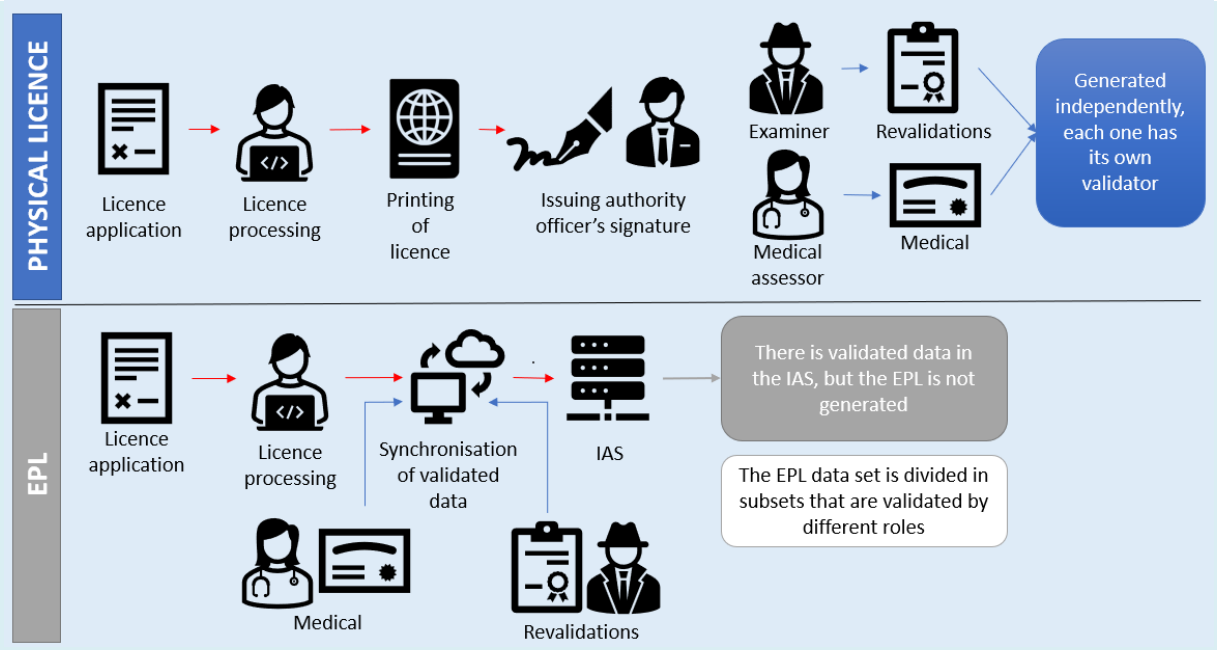
(g) The licence issued in electronic format is generated by the IAS and sent to the EPLHD.

(h) Once the licence issued in electronic format is received in the EPLHD, it is stored in the EPLAPP.

3.3.1.3. Comparison of issuance processes

If the processes of issuance of the licence issued in physical format and of issuance of the licence issued in electronic format are compared (see Figure 6), depending on the format of the licence, there are significant differences that affect the concept of issuance:

Figure 6 — Comparison of issuance processes



(a) Difference in the number of documents: The primary and most obvious difference is that, outside the electronic world, two separate documents exist for some licences: for example, with a flight crew licence, there are the licence issued in electronic format and the medical certificate. Revalidations are considered part of the licence data set, although they might have a different validator. With licences issued in electronic format, only one document exists, and parts of its information are validated by people in different roles.

(b) Updating licence information: The licence information of the licence issued in electronic format can be updated in response to changes in the licence issued in physical format data set or in the medical certificate data set. Every time that there is a change, a new licence issued in electronic format must be generated, so that the information it contains is valid and up to date. This entails that in a licence issued in electronic format will be generated and delivered more frequently than in a licence issued in physical format.

(c) Change of order in the actions of validation and generation: The licence issued in physical format is generated (printed) and then validated by the officer's signature (handwritten) whereas in an EPLSYS the licence data of the licence issued in electronic format must first be validated by an officer in the LICSYS (by an electronic signature) and then the mdoc is generated and finally electronically signed by the issuing authority. Note that the signature of the mdoc is intended to protect the mdoc information, not to validate the data it contains.

(d) Method of licence generation: A licence issued in physical format is generated when the issuing authority decides to do so, by printing it, whereas with an EPLSYS the data verified by the issuing authority is made available for generation of the licence in electronic format once the licence holder sends a request from the EPLHD.

(e) The licence holder is in charge of generating the information on the licence issued in electronic format: The licence issued in electronic format is linked to a specific self-contained mobile electronic visual display device. When the licence in electronic format is generated, it contains information about the device where it will be contained; therefore, the licence holder must have

provided the information about the device prior to the generation of the licence in electronic format, meaning that it is the licence holder who initiates the generation of the licence in electronic format.

3.3.2. Suspension and revocation of a licence

(a) When a licence is generated in electronic format, the issuing authority should also generate a public key infrastructure (PKI) certificate that represents the issuing authority, the issuing authority PKI certificate (IAPKIC), and the licence issued in electronic format is signed with this certificate. Further details of this process are provided in Section 0, but for now it should suffice to be aware that the EPLDS of each licence issued in electronic format will be signed with a unique IAPKIC that is specific for each licence issued in electronic format.

(b) A licence issued in electronic format should be considered a representation that reflects the licence data set information and the medical data set information at a specific moment in time. If any of this information changes, then the licence issued in electronic format must be invalidated and a new licence in electronic format generated. The invalidation of a licence issued in electronic format takes place by revoking the IAPKIC used to sign the EPLDS, but this revocation of the IAPKIC must not be confused with the administrative act of revocation of a licence or the revocation of a medical certificate, which would take away the privileges of the licence holder. Therefore, in order to avoid confusion, the revocation of an IAPKIC will be referred to in this AMC as 'invalidation', and the outcome is that the licence in electronic format signed with this IAPKIC is invalidated.

(c) An actual revocation of the licence entails the invalidation of the licence issued in electronic format, and no further generations of the licence are possible. This presents a completely different situation.

(d) The electronic personnel licence data model (EPLDM) does not include the status of the licence, so there is no way to indicate whether a licence issued in electronic format is valid, suspended or revoked. A licence issued in electronic format provides only valid and up-to-date information.

(e) If a licence is suspended by an administrative act, the existing IAPKIC used to sign the licence issued in electronic format shall be revoked and a new licence in electronic format generated without information, or with only the medical information if it was valid. In an EPLSYS as defined by ICAO, the difference between the revocation and the suspension would be noted because:

(1) In the case of revocation, no licence issued in electronic format exists and no new licence issued in electronic format can be generated.

(2) In the case of suspension, the licence in electronic format can be generated, but it is empty (no valid data is available), and new licences in electronic format can be generated. When the suspension ends, a further generation of the licence in electronic format would recover all the valid licence data.

(f) The revocation of a medical certificate will not revoke the licence data set; therefore, the existing IAPKIC used to sign the licence issued in electronic format is revoked and a new licence in electronic format without medical information is generated. In this case, there would be no difference between the revocation or suspension of a medical certificate; the medical information would not be displayed in the licence issued in electronic format just the same.

3.4. Verification of the authenticity and validity of a licence issued in electronic format

(a) The verification of the authenticity and validity of a licence issued in electronic format consists in verifying that the IAPKIC is still valid. When a licence issued in electronic format is invalidated, so is the IAPKIC, and the IAPKIC is added to a certificate revocation list in the IAS. This means that each licence issued in electronic format has a unique IAPKIC that is specific for each licence issued in electronic format, and its validity is checked, verifying whether the IAPKIC is still valid.

(b) It is important to be aware that the verification of the authenticity and validity of a licence issued in electronic format ensures that the information in the EPLDS has not been tampered with and it remains as provided by the issuing authority. The verification process of the EPLSYS does not check whether the ratings are still valid (it is possible that some ratings have an expiry date in the past and the licence issued in electronic format is still valid). Therefore, verifiers will need to look at the information provided and analyse whether the holder has the appropriate privileges to perform whatever task the holder is performing, just as done with a licence issued in physical format.

(c) The verification of the authenticity and validity of a licence issued in electronic format only verifies that:

(1) the licence issued in electronic format is still valid (the IAPKIC with which it was signed is not revoked); and

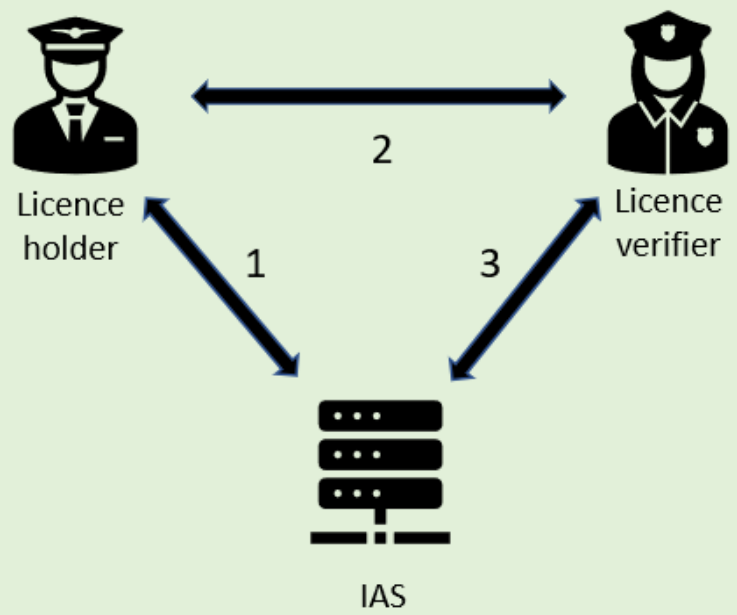
(2) the licence information of the licence issued in electronic format is as provided by the issuing authority.

4. EPLSYS

4.1. EPLSYS introduction

(a) An EPLSYS is an integrated system comprised of computer hardware, network and communication facilities, computer software, validated data, users, and rules and regulations to enable the issuance of licences in electronic format and the conduct of oversight activities.

Figure 7 — EPLSYS interfaces



Error! Reference source not found. represents the three interfaces of the EPLSYS, accordance to ISO 18013-5, which are:

1. interface between the issuing authority and the licence holder;
2. interface between the licence holder and the licence verifier;
3. interface between the licence verifier and the competent authority.

ISO 18013-5 applies to interfaces 2 and 3 and considers interface 1 (the link between the competent authority's server and the licence holder) specific to each state.

(b) EPLSYS implementation requires that the issuing authority should develop an application for the licence holder: the EPLAPP. This application should be installed in the EPLHD and should allow the licence holder to connect with the IAS, receive and store the licence issued in electronic format (interface 1) and allow the verification of the validity and authenticity of the licence by a licence verifier that may use an EPLRD. This verification is done through interface 2 (offline through a data exchange between devices) or interface 3 (online through a connection with the IAS).

(c) Competent authorities are entitled to decide the level they want to implement when verifying licences issued in electronic format. This means that it is up to the competent authority to decide whether or not it is necessary to provide the licence verifiers with a tool for the verification of

the validity and authenticity of the licences issued in electronic format. This verification tool consists of a second application that can be installed in an EPLRD, which allows engagement with the EPLHD, can understand the information received from the EPLHD and permits verification, both offline (interface 2) and online (interface 3). This application will be called the reading application for licences issued in electronic format (EPLRAP).

(d) The implementation of an EPLSYS does not require the implementing competent authority to develop the EPLRAP, but it does require the development of the verification tools necessary for other verifying authorities to verify the validity and authenticity of the licences issued in electronic format by the implementing competent authority. This means that the licences in electronic format generated by the implementing competent authority should be able to be verified by EPLRAPs of other verifying authorities both offline (interface 2) and online (interface 3). The implementing competent authority may choose not to develop an EPLRAP, but it needs to provide just the same the possibility for other states to verify its licences issued in electronic format through device engagement and by connection to the IAS.

(e) If a competent authority does not develop an EPLRAP, there can only be a visual inspection of licences issued in electronic format. Verification using the EPLRAP provides extra measures of security that make it very difficult to tamper with the licence information of a licence issued in electronic format.

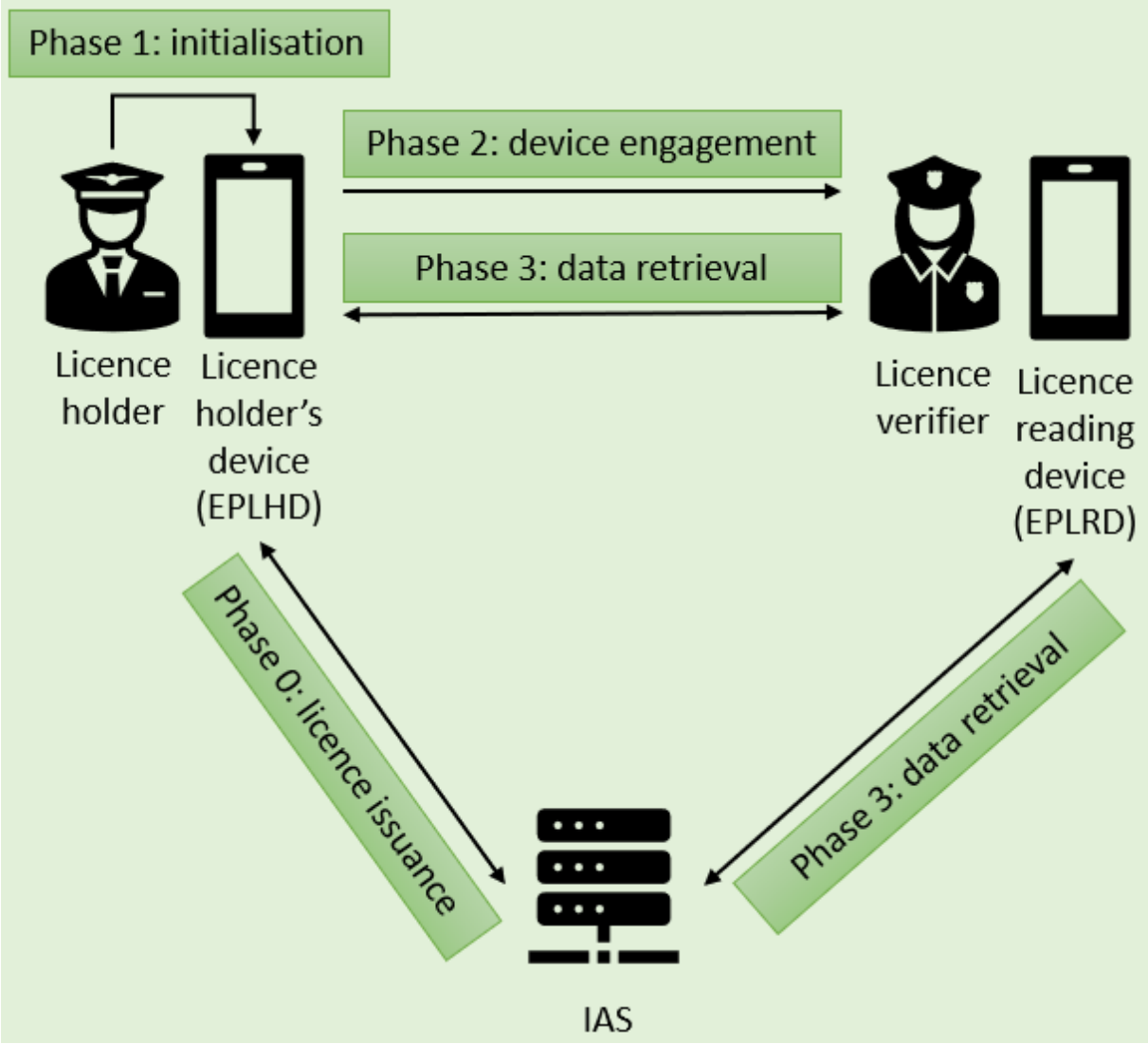
(f) It is important that verifying authorities be aware that they will have to verify licences in electronic format even if they do not implement them. Therefore, they might need an EPLRAP even though they do not issue licences in electronic format.

(g) The EPLHD and EPLRD where the EPLSYS applications will be installed should provide for the information security requirements.

4.2. Data exchange phases

There are the following phases of data exchange: licence issuance, initialisation, device engagement and data retrieval — see Figure 8.

Figure 8 — Data exchange phases



— **Phase 0 — Licence issuance:** This interaction is between the EPLHD and the IAS. In this phase a licence in electronic format is generated and stored in the EPLHD.

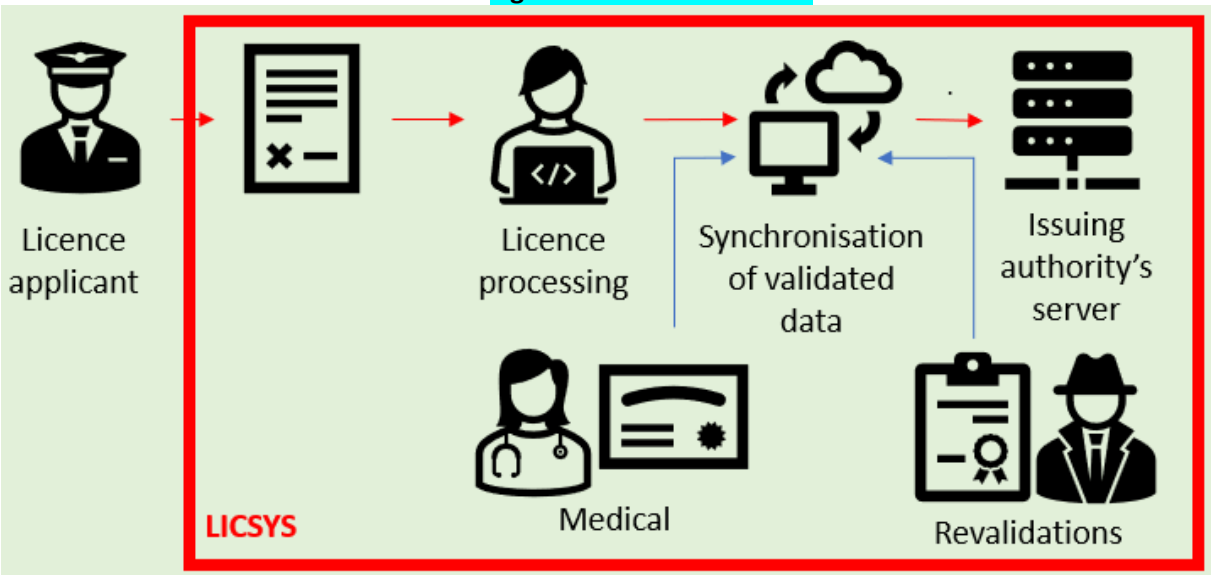
— **Phase 1 — Initialisation:** The licence holder initiates the EPLHD for licence verification. This phase is always initiated by the licence holder. A QR code that contains the information required to set up and secure phases 2 and 3 is generated. The EPLHD gets ready for phase 2.

— **Phase 2 — Device engagement:** The EPLRD reads the QR code generated in phase 1 on the EPLHD, and a message is transferred from the EPLHD to the EPLRD.

— **Phase 3 — Data retrieval:** The licence verifier selects the data retrieval mode and asks the licence holder for consent to access the licence data of the licence issued in electronic format. If consent is granted, this interaction depends on the methodology of the data retrieval: it can be either between the EPLHD and the EPLRD or between the EPLRD and the IAS. The licence information of the licence issued in electronic format is obtained in the EPLRD and verified.

4.2.1. Phase 0: Licence generation

Figure 9 — Data validation



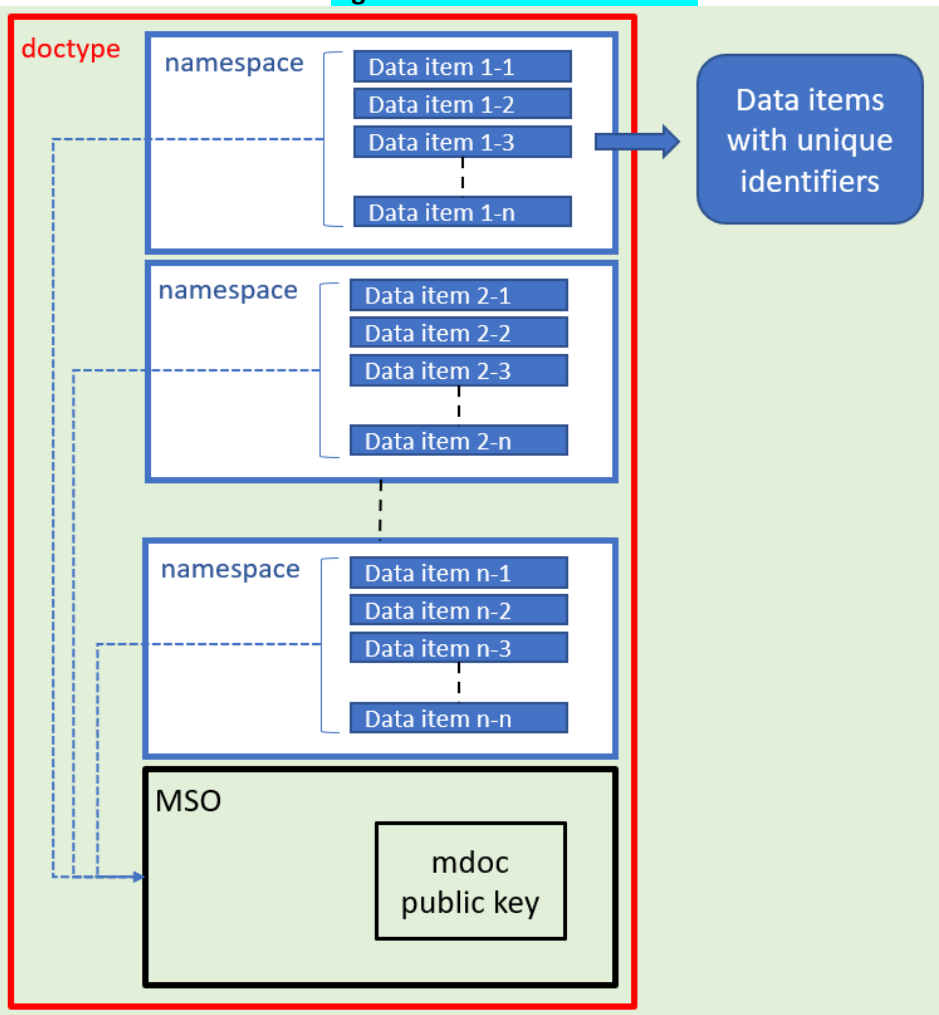
(a) Prior to the generation of the licence issued in electronic format, as explained in Section 0, the data has been validated in the LICSYS and properly stored in the IAS — see Figure 9. At this point, no generation of a licence in electronic format has occurred.

(b) The licence holder should have the EPLAPP installed on the EPLHD, and the EPLAPP must be initialised (see Section 0). The reader should note that the initialisation of the EPLAPP is not the same as the initialisation of 'phase 1: device engagement' when exchanging data.

4.2.1.1. The mdoc of a licence issued in electronic format

(a) A licence issued in electronic format should follow the specification of an mdoc — see Figure 10.

Figure 10 — Mdoc data model



(b) The doctype and namespace are used to encapsulate the document type and the space in which the data elements are defined.

(c) The document type for licences issued in electronic format should be 'int.icao.epl.1'; the number 1 represents the version of the document type. The licence issued in electronic format has a specific data model that might change with time; should this happen, the doctype version will change. The EPLAPP should be ready to work and be updated with new versions of the EPLDM.

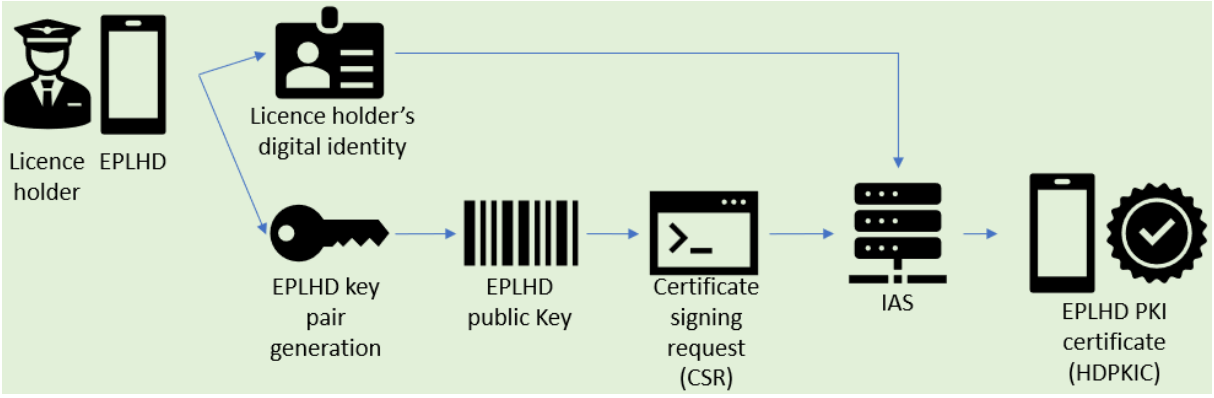
(d) Each namespace of the licence issued in electronic format, as defined in ICAO Doc 10190, is related to one of the groups of information of the common form defined in ICAO Annex 1 (Appendix 4) and contains a list of data items in accordance with the licence or the medical certificate data.

4.2.1.2. Step 1: Device enrolment with the competent authority

To initiate the generation of a licence issued in electronic format, the EPLAPP must enrol the EPLHD with the issuing authority through an interface provided by the issuing authority. This enrolment is

done creating a PKI certificate-signing request (CSR) in the EPLHD and sending it to the IAS, as shown in Figure 11:

Figure 11 — Step 1 of licence issuance in electronic format



(a) The EPLAPP generates a public/private key pair for the EPLHD, to be used only for this specific licence issued in electronic format.

(b) The public key generated in (a) is included in a CSR.

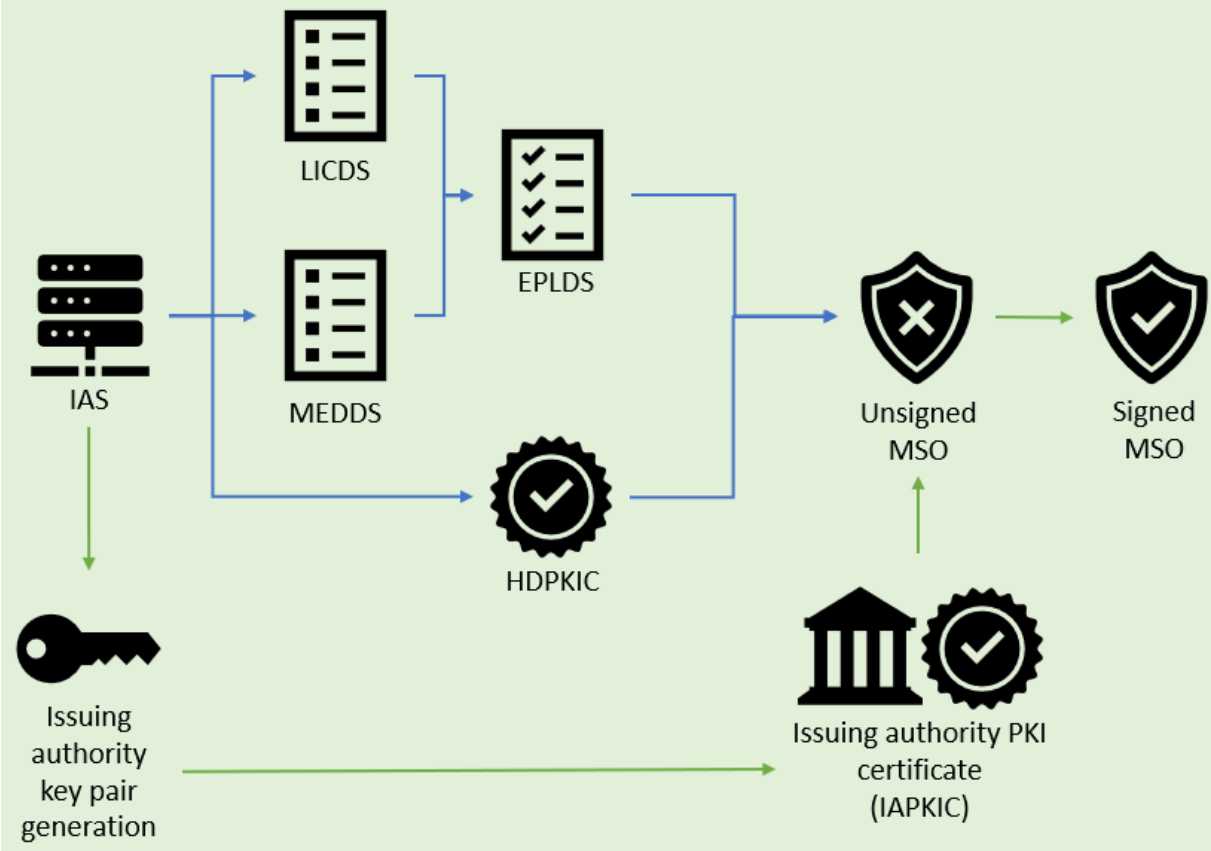
(c) The licence holder's digital identity and the CSR are sent to the IAS.

(d) The IAS issues and signs the holder device PKI certificate (HDPKIC). The HDPKIC represents the EPLHD identity and will allow the licence issued in electronic format to be linked to the EPLHD where the key pair was generated. This avoids the possibility that the licence issued in electronic format can be cloned in another EPLHD.

(e) The HDPKIC is stored with the licence holder's record in the IAS.

4.2.1.3. Step 2: Mobile security object generation

Figure 12 — Step 2 of licence issuance in electronic format



(a) The EPLSYS in the IAS should search for any already existing licence of the same type issued in electronic format for the holder (for example, a licence in electronic format was generated in another EPLHD) — see Figure 12. If so, the existing licence in electronic format should be invalidated before the new licence in electronic format is generated.

(b) The licence data set and the medical data set are obtained from where they are stored in the IAS. The information must be processed as it is organised in the valid data model, putting every piece of information in the corresponding namespace and data item. The EPLDS is obtained.

(c) The EPLDS and the HDPKIC are included in the mobile security object (MSO).

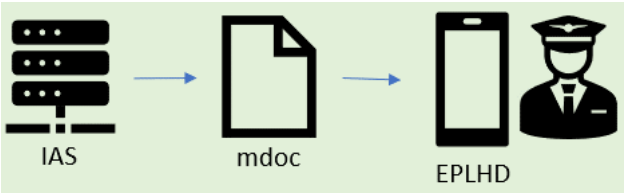
(d) ISO 18013-5 requires the use of two public/private key pairs in the mdoc: one for the EPLHD (generated in step 1) and another one for the issuing authority. The authorities must generate a unique key pair for each individual licence issued in electronic format.

(e) The IAPKIC, which is a PKI certificate containing the issuing authority public key, is generated, and it is signed by the issuing authority.

(f) The MSO is signed with the private key of the IAPKIC.

4.2.1.4. Step 3: Delivery of the licence issued in electronic format

Figure 13 — Step 3 of the generation of the licence issued in electronic format



(a) The mdoc is generated, including the IAPKIC, the information about the EPLDS and the MSO. The mdoc is returned to the EPLHD — see Figure 13. The licence issued in electronic format is stored in the EPLAPP and ready to be displayed and verified.

(b) The EPLAPP may encrypt the mdoc information using the HDPKIC, so the privacy of the licence holder is protected.

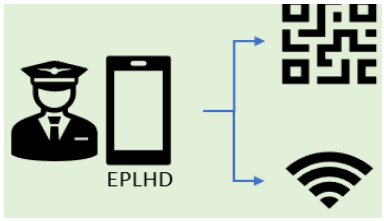
4.2.2. Phase 1: Initialisation

(a) The initialisation consists of preparing the EPLHD for the next phase (device engagement). The EPLSYS shall admit initialisation only using a QR code.

(b) The QR code contains the 'engagement message', which should follow the structure defined in Section 8.2.1.1 of ISO 180136-5 and contains information such as device retrieval technologies (offline retrieval); server retrieval technologies (online retrieval); server retrieval token; and protocol info.

(c) The licence holder will initiate the initialisation, actively requesting the EPLAPP to create the QR code. Once it is generated, the EPLHD should open the connections to allow the request from an EPLRD — see Figure 14.

Figure 14 — Phase 1: Initialisation



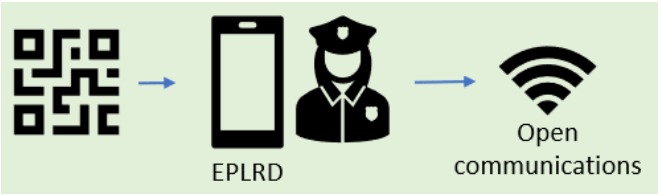
4.2.3. Phase 2: Device engagement

(a) The verification of the authenticity and validity of the licences issued in electronic format is done using wireless short-range peer-to-peer communication between the EPLHD and the EPLRD. The devices exchange information in two phases, the device engagement being the first one of them — see Figure 15. This phase determines the technical characteristics for the later retrieval phase:

(1) The EPLRD, using the EPLRAP, reads the code generated in the EPLAPP.

(2) The EPLRD opens the communications to start the next phase.

Figure 15 — Phase 2: Device engagement



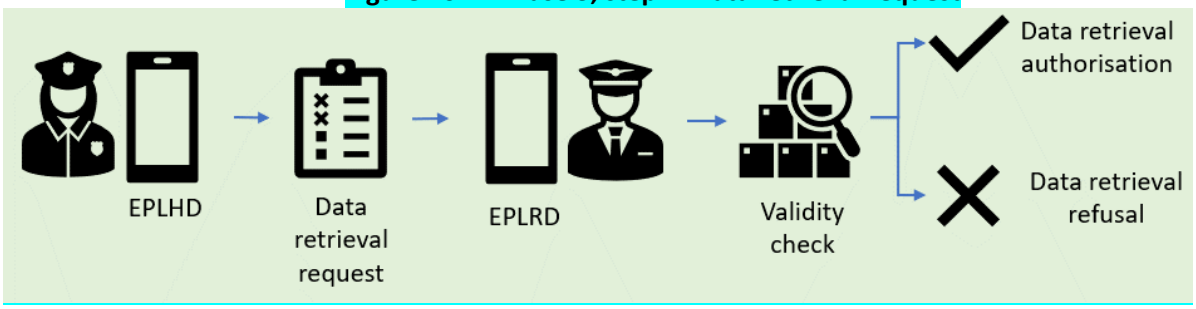
(b) During this phase, the engagement message is transferred from the EPLHD to the EPLRD by means of a QR code containing the information required to set up and secure the data retrieval. The information exchanged includes the capabilities of the EPLHD for the subsequent data retrieval (technologies usable: Bluetooth low energy, Wi-Fi aware (optional) and online) and parameters for a session initiation (cipher suites, keys). The message contains the security information used to initiate device retrieval and the token used to initiate server retrieval. Following transfer of the device engagement message, the information contained in the message is used to hand off the retrieval of the licence issued in electronic format to a separate channel (phase 3).

(c) The EPLRD may have an automatic timeout in case the engagement cannot be completed within a certain time (not less than 30 seconds is recommended). The EPLHD may terminate the engagement and the data retrieval at any time.

4.2.4. Phase 3: Data retrieval

4.2.4.1. Step 1: Data retrieval request

Figure 16 — Phase 3, step 1: Data retrieval request



(a) Once the devices are engaged, the verifier will generate in the EPLRAP a data retrieval request (see Figure 16), whereby the licence verifier notifies the holder of the licence which information from the EPLDS is to be retrieved and which retrieval method will be used.

(b) The data retrieval request is received by the EPLHD, and the EPLAPP will proceed to verify the validity of the data retrieval request.

(c) If the data retrieval request validation is successful, then the licence holder shall be able to authorise the data retrieval or refuse it.

(d) When the licence holder receives a data retrieval request from a verifier, the EPLAPP must carry out a few verification steps to assess whether the data retrieval request is valid, as follows:

(1) The EPLAPP gets the RDPKIC from the data retrieval request.

(2) The EPLAPP verifies that the RDPKIC is not expired and that it is signed with the verifier's IAPKIC.

(3) The EPLAPP verifies that the RDPKIC is not included in the PKI certificate revocation list of the verifier's authority (it would be so in case of a security key compromise, for instance).

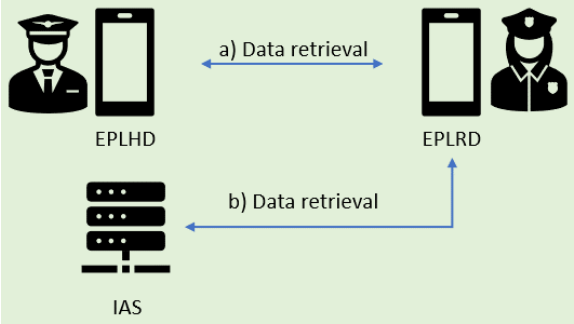
(4) The EPLAPP verifies that the verifier's IAPKIC is included in the trust list by following the steps described in Section 11.1.12 of ICAO Doc 10190.

(e) If any of these checks fail, an appropriate error indication is displayed in the EPLAPP, and the communication session should be terminated.

(f) If the validation of the data retrieval request is successful, the licence holder can proceed with the authorisation of data retrieval.

4.2.4.2. Step 2: Data retrieval

Figure 17 — Phase 3, step 2: Data retrieval



(a) The data retrieval methods available (see Figure 17) should be:

(1) device retrieval: the licence issued in electronic format is transferred from the EPLHD to the EPLRD (offline);

(2) server retrieval: the licence issued in electronic format is transferred from the IAS to the EPLRD (online).

(b) It is recommended that the first attempt at data retrieval be the device retrieval option and, if unsuccessful, only then is the server retrieval attempted.

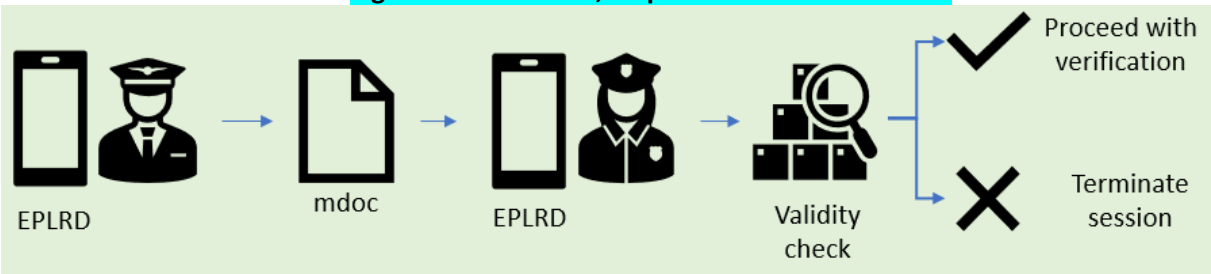
(c) The data retrieval works in a request/response type of communication. The EPLRAP sends a request for data elements and the EPLAPP (or IAS) responds with the requested data. The retrieval of data works in a session, and only those elements of the EPLDS that are requested by the verifier are transmitted once the licence holder has approved the request.

(d) Licences issued in electronic format may have additional data elements that can be defined by each issuing authority, and they might not be interoperable with reading devices from other states. If the EPLHD cannot recognise a requested data element, it will be ignored and the EPLRD might inform the licence verifier about the data elements that will not be returned.

(e) The data retrieval differs depending on the data retrieval option the licence verifier specifies in the data retrieval request.

4.2.4.2.1. Device data retrieval

Figure 18 — Phase 3, step 2: Device data retrieval



(a) Once the data retrieval request is authorised by the licence holder, the licence issued in electronic format is transferred from the EPLHD to the EPLRD — see Figure 18.

(b) When an EPLRD receives the licence issued in electronic format from an EPLHD, the EPLRAP verifies that:

(1) the IssuerSigned element contains the MSO;

(2) the MSO is signed by a non-expired IAPKIC and that the IAPKIC is included in the trust list following the steps of Section 11.1.1.2 of ICAO Doc 10190;

(3) the DeviceSigned element contains the HDPKIC;

(4) the HDPKIC is not included in the PKI certificate revocation list of the issuing authority.

(c) If any of those checks fail, an appropriate error indication is displayed by the EPLRAP and further information exchange should be terminated.

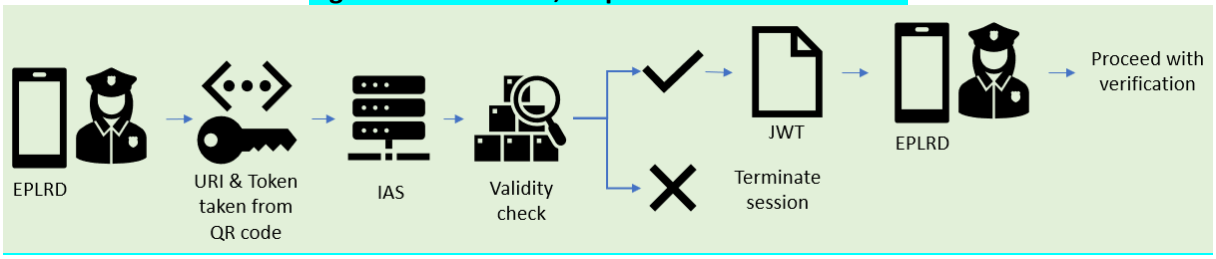
(d) The data elements of the licence issued in electronic format should be returned in the namespaces of the EPLDM defined in ICAO Doc 10190. The elements of the MSO should always be returned as IssuerSigned elements; if they were returned in the DeviceSigned data, the licence issued in electronic format should be considered invalid.

(e) The elements of the licence issued in electronic format should be verified to conform to the encoding format and maximum size as defined in ICAO Doc 10190.

(f) In order to ensure the integrity of the data value for each data element, the reader application should calculate the message digest for each data value using the digest algorithm specified in the MSO. The structure of the MSO is described in Section 9.1.2.4 ‘Signing method and structure for MSO’ in ISO 18013-5.

4.2.4.2.2. Server retrieval

Figure 19 — Phase 3, step 2: Server data retrieval



(a) The licence information of the licence issued in electronic format is transferred from the IAS to the EPLRD.

(b) Section 6.3.2.5 of ISO 18013-5 contemplates two server retrieval options: web application programming interface (API) and OpenID Connect. ICAO Doc 10190 limits the options to web API. Therefore, both the EPLHD and the EPLRD must support web API retrieval, the structure of which is defined in Section 8.2.1.2 of ISO 18013-5. It includes three fields:

(1) Version, currently 1;

(2) Issuer uniform resource locator (URL), as defined in Section 8.3.3.2.1 of ISO 18013-5;

(3) Server retrieval token.

(c) Secure retrieval of data of the licence issued in electronic format using server retrieval relies on a well-designed server retrieval token. The token and a universal resource identifier (URI) for accessing the issuing authority's EPLSYS are sent from the EPLHD to the EPLRD — see Figure 19. The EPLRD will use the token in response to the server retrieval request and does not need to verify or understand it, but the issuing authority receiving the request should perform validation of the authenticity and integrity of it. Each competent authority will be able to determine the format of the server retrieval token; however, they should:

(1) be of a short duration;

(2) be used only once (single use);

(3) uniquely identify the licence holder;

(4) include consent for release of specific elements of the licence issued in electronic format;

(5) include digital device signature authenticating the licence holder.

(d) ISO 18013-5 supports transfer of the server retrieval token during both device engagement and data retrieval, but ICAO Doc 10190 specifies that the server retrieval token must be sent in the device engagement phase and not in the data retrieval phase.

(e) The EPLRD obtains the issuer URL contained in the device engagement message, to establish a connection with the competent authority. The EPLRAP should verify the URL against the distinguished name field in the IAPKIC in the ICAO master trust list, to ensure that the URL is not spoofed. The communications between the EPLRD and the IAS should be secured using transport layer security (TLS) with mutual authentication.

(f) The issuing authority should validate the TLS PKI certificate presented by the EPLRD, and the EPLRD should validate the TLS PKI certificate presented by the issuing authority.

(g) The token provides authorisation from the licence holders for the licence verifiers to access licence data issued in electronic format. A valid token is required for server retrieval. If the validation of the token fails, the competent authority should not return licence data issued in electronic format to the EPLRD.

(h) The issuing competent authority should verify that the fields that are requested by the reader have been approved for disclosure by the holder.

(i) The server response for Web API is described in Section 8.3.2.2.2.2 of ISO 18013-5, and it includes three fields:

(1) Version: always 1 as defined by ISO 18013-5;

(2) Documents: it will contain the licence issued in electronic format as a Java web token (JWT);

(3) DocumentErrors: The EPLRAP should process error codes contained here.

(j) The Java simple object notation (JSON) web signature should be protected using a Java simple object notation (JSON) web signature as specified in ISO 18013-5 Section 9.2.2. The EPLRD should validate the JWS as described in ISO 18013-5 Section 9.3.2.

4.3. Chain of trust

(a) Both the EPLAPP and EPLRAP should download the latest EPL master trust list from ICAO to the device where they have been installed, and should check the electronic signature of the trust list to ensure its integrity.

(b) Each IAPKIC in the trust list will contain the URL distribution point value that points to the licence holder's and verifier's PKI certificate revocation lists for that state. These lists should be downloaded every 24 hours to the EPLHDs and EPLRDs to ensure that the revocation list is up to date and available for the verification process.

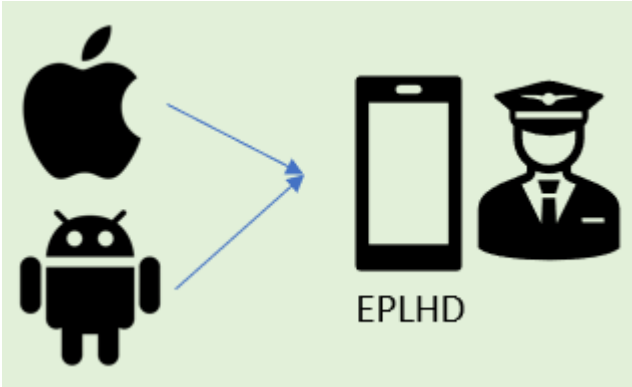
(c) In order to construct a valid chain of trust, the steps indicated in Section 11.1.1.2 of ICAO Doc 10190 are followed.

4.4. EPLAPP

The EPLAPP will be installed in the EPLHD and will allow an appropriate way to identify the licence holder, generate and store one or several licences issued in electronic format, and synchronise the existing licences information issued in electronic format in the application. It will also have some functionalities that allow the licence holder to generate a one-time QR code that will allow engagement with an EPLRD and the retrieval of licence data of the licences issued in electronic format.

4.4.1. Downloading and installing the EPLAPP

Figure 20 — EPLAPP operating systems

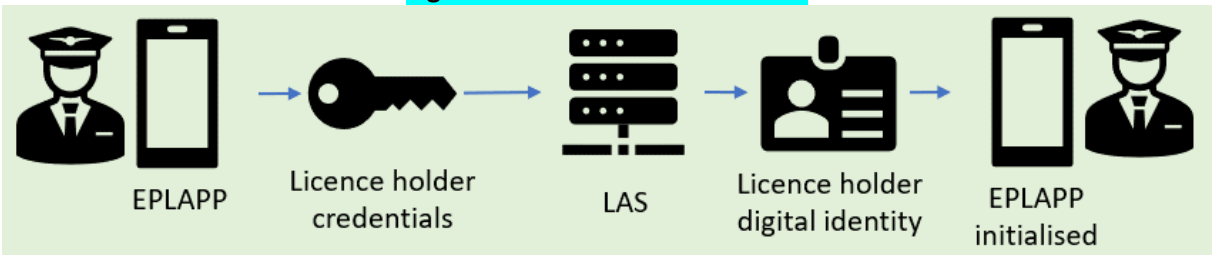


(a) Each issuing authority will need to publish its national EPLAPP for at least Android and iOS systems — see Figure 20.

(b) Once downloaded, the application will be installed like any market application for those operating systems.

4.4.2. Initialising the EPLAPP

Figure 21 — EPLAPP initialisation



(a) Any instance of an EPLAPP installed on a new device will need to follow an initialisation process — see Figure 21. The purpose of this process is to ensure the proper identification of the licence holder and to link the new EPLHD to the licence holder. The process of initialisation requires an internet connection to be available.

(b) The first time the licence holder signs in to an instance of an EPLAPP installed on a specific EPLHD, the licence holder needs to be properly identified. If the licence holder is in possession

of a digital certificate that already provides a digital identity, it can be used to log in to the EPLAPP.

(c) When the licence holder does not possess a digital identity, the licence holder should present themselves to the issuing authority, which, once the licence holder has been properly identified, will create the digital identity of the licence holder and provide credentials to log in to the EPLAPP.

(d) Issuing authorities could also consider the use of an approved vetting and proofing process that can create digital credentials for the licence holder. This process can be established using a method such as two-factor authentication using a username and password followed by a one-time token.

(e) All issuing authorities will need to prepare the EPLAPP to identify the licence holder using the EU Digital Identity Wallet of the holder and use it as the digital identity of the licence holder.

(f) Once the licence holder has logged in, the EPLAPP will verify the holder digital identity in the IAS and link the instance of the EPLAPP to the licence holder.

(g) The EPLAPP will send a confirmation that the initialisation process has successfully finalised. In the event of a failure, it will send a notification of any error that has occurred.

Once the initialisation process has successfully finalised, the EPLAPP will be available for use. Otherwise, the EPLAPP will have all its functionalities blocked and no information will be able to be seen or managed in the application.

4.4.3. Actions on the licence issued in electronic format

The EPLAPP needs to provide the licence holder with several actions to perform on the licence issued in electronic format, such as:

(a) View licence issued in electronic format**:** The licence issued in electronic format has been downloaded into a device and is ready to be used. Pressing the button leads the holder to view the licence issued in electronic format.

(b) View licence issued in electronic format in accordance with ICAO format**:** The information in the licence issued in electronic format should always be available in English. However, Member States can use up to eight additional national languages.

(1) The EPLDM described in ICAO Doc 10190 allows the issuing authority to specify national privileges for the licence issued in electronic format. These national privileges might not follow a standardised taxonomy, might have very particular characteristics, might make no sense outside the issuing state or might not be available in English, since the authority is not obliged to translate them. Therefore, it could happen that an EPLRD from another state is not able to read or process the information about the national ratings.

(2) For these reasons, the EPLAPP needs to provide a standardised display of the licence issued in electronic format (that is, in English and lacking national privileges should they not be understood by EPLRDs from other states), which is considered the ICAO format and is compliant with ICAO specifications. Therefore, the EPLAPP must provide for each type of licence the possibility of displaying the licence issued in electronic format in this

ICAO format. The button in the EPLAPP that allows the generation of this format is required to have the ICAO logo.

(c) Generate licence issued in electronic format**:** The Member State has made this type of licence available as a licence issued in electronic format, but the licence issued in electronic format has never been generated yet. Pressing this button will start the licence generation as described in phase 0 (see Section 0).

(d) Update licence issued in electronic format: The licence issued in electronic format has been downloaded to an EPLHD, but the EPLAPP detects that there have been changes in the EPLDS, so the generation of a new licence in electronic format is required. The EPLAPP needs to indicate to the licence holder that a new licence issued in electronic format should be generated.

It is important that the licence holder manually initiate the generation of the new licence in electronic format, because it will be in the process of generation that the former licence issued in electronic format will be invalidated. It could cause problems, especially for aircrew licences, because if this licence were invalidated without the knowledge of the licence holder, and there were a process of verification, the licence holder would not know that the stored new licence issued in electronic format was no longer valid and might be in a situation where there would be no option to update it. Therefore, the former licence in electronic format should be valid until the new licence in electronic format is generated.

(e) Transfer licence issued in electronic format: The licence issued in electronic format has been downloaded to another device. The licence holder can decide to transfer the licence to this device, which will invalidate the licence issued in electronic format in the first device and generate a new licence in electronic format in the current device.

4.4.4. Availability of the licence issued in electronic format

(a) There might be cases where the licence holder will not be able to request the generation of the licence in electronic format in the EPLAPP. In these cases, an indication of 'EPL not available' should be shown to the licence holder.

(b) The message 'EPL not available' could be due to any of the following situations:

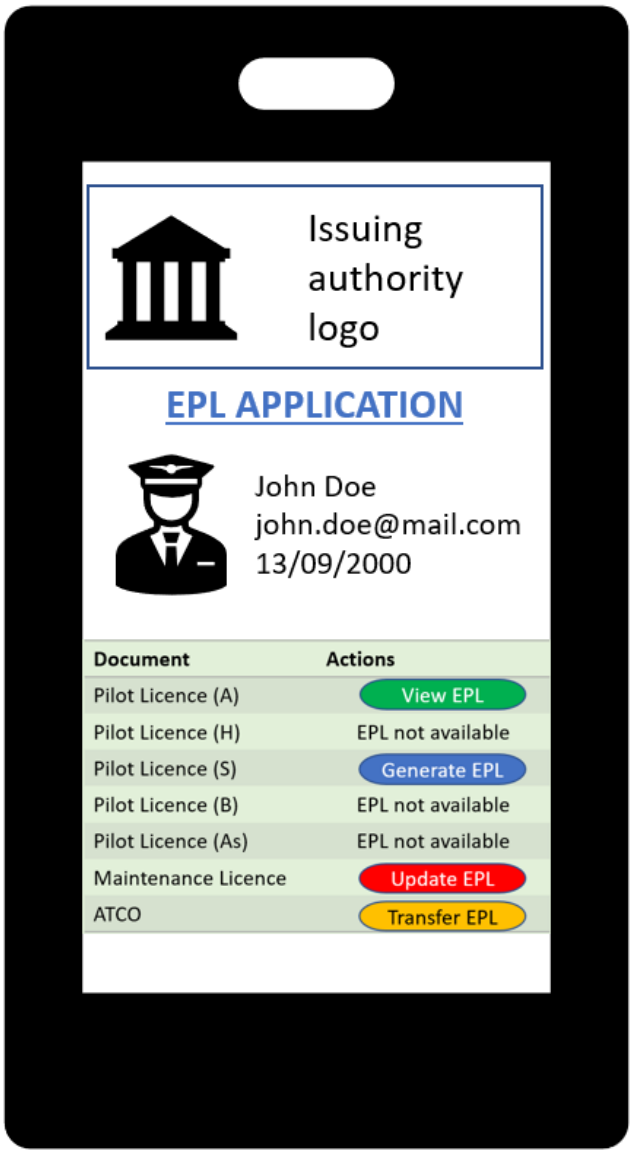
(1) The competent authority has decided not to use the electronic format for this particular type of licence.

(2) The licence holder does not possess that type of licence.

(3) The licence holder possesses that type of licence, but the licence holder possesses a physical version of the licence, so the licence in electronic format cannot be generated.

4.4.5. List of licences

Figure 22 — EPLAPP home page



(a) This section contains a proposal for competent authorities about how the EPLAPP home page could work, but Member States may decide on a different solution that best suits their purposes.

(b) **Error! Reference source not found.**' proposes that the home page of EPLAPP contain the identification data of the licence holder and a list of all the licences the licence holder has. Each licence issued in electronic format is an independent entity, which might have been issued subject to a different regulation, but, if the licence holder has five different licences, it will be costly for the issuing authority to develop and maintain one independent EPLAPP for each type of licence. The list of licences in this example allows all the types of licences to be listed in a single application, and each type of licence has an associated action that depends on the status of the licence.

(c) If the EPLAPP uses such a list, the issuing authority will only be required to develop and maintain a single EPLAPP.

(d) Every time the list is loaded, there will be a synchronisation of the licence information of each type of licence, so the synchronisation date of each type of licence should be updated.

(e) When developing the EPLAPP, it should be taken into consideration that the application must be able to function properly offline. If the EPLHD is online, the list of licences and available actions can be synchronised as appropriate. If the EPLHD is not online, only the licences issued in electronic format stored on this specific device will be listed.

4.4.6. Accessing a licence issued in electronic format

When a licence issued in electronic format is stored in an instance of the EPLAPP, the action 'View EPL' will be available. Pressing the button will lead to the licence information of the licence issued in electronic format and the actions that can be taken on that specific licence issued in electronic format, such as:

(a) Manual synchronisation: This action will not be available in offline mode. When selected, the EPLAPP will look for any changes in the licence issued in electronic format and update the date of last synchronisation. If necessary, the licence information of the licence issued in electronic format will be updated by the generation of a new licence in electronic format.

(b) Deactivate the licence issued in electronic format: This action will allow the holder of the licence issued in electronic format to deactivate it in the instance of the EPLAPP on which it is stored. Therefore, the licence issued in electronic format will be invalidated.

When the licence holder decides to erase the licence issued in electronic format from an instance of EPLAPP, such deletion:

(1) should delete all information, including log information, and any metadata that could impart information about the erased licence in electronic format;

(2) should not require approval by the issuing authority;

(3) should be available to a licence holder via a request from the issuing authority.

Issuing authorities should consider making it possible to delete a licence in electronic format from an EPLHD remotely, for security reasons (such as the EPLHD being stolen).

(c) Generate QR: When the licence must be verified by a licence verifier, the licence holder must generate the QR that will allow the device engagement with the EPLRD. This action will allow the generation of the QR code.

4.4.7. Background with moving image

As a security measure, licences issued in electronic format should have security features such as a moving image that allow the verifiers to be certain they are not viewing a static image.

4.4.8. Audit log

The EPLAPP should be capable of maintaining an audit log. The licence holder should be able to decide whether to make use of this log or not. The audit log and related settings should be accessible only to the licence holder.

The audit log will keep a record of all the transactions concerning the licence issued in electronic format (sharing licence information of the licence holder with a verifier for the licence issued in electronic format) and communication actions between the EPLHD and the competent authority.

4.5. EPLRAP

(a) The EPLRAP will be installed on the EPLRD and will allow the staff of competent authorities to retrieve data from a licence issued in electronic format (or directly from an IAS) and proceed with the necessary verification of the data, such as the validity of the signature and the validity of the EPLDM that has been retrieved.

(b) Member States that decide to develop an EPLRAP should follow the specifications of this AMC.

(c) The EPLRAP should only be installed on devices that belong to the verifying authority, and not on the personal devices of the verifying authority staff. The competent authorities should provide their staff with the tools required to fulfil their tasks.

4.5.1. EPLRAP functional requirements

The EPLRAP shall include at least the following functional requirements:

(a) It needs to be able to request, receive and verify the integrity and authenticity of a licence issued in electronic format whether online connection is present or not for either the EPLHD or the EPLRD.

(b) A user of EPLRAP not associated with the issuing authority needs to be able to verify the integrity and authenticity of a licence issued in electronic format.

(c) The reader needs to be enabled to confirm the link between the person presenting the licence issued in electronic format and the licence holder.

(d) The interface between the licence issued in electronic format and the EPLRAP needs to support the selective release of the licence data issued in electronic format to the reader.

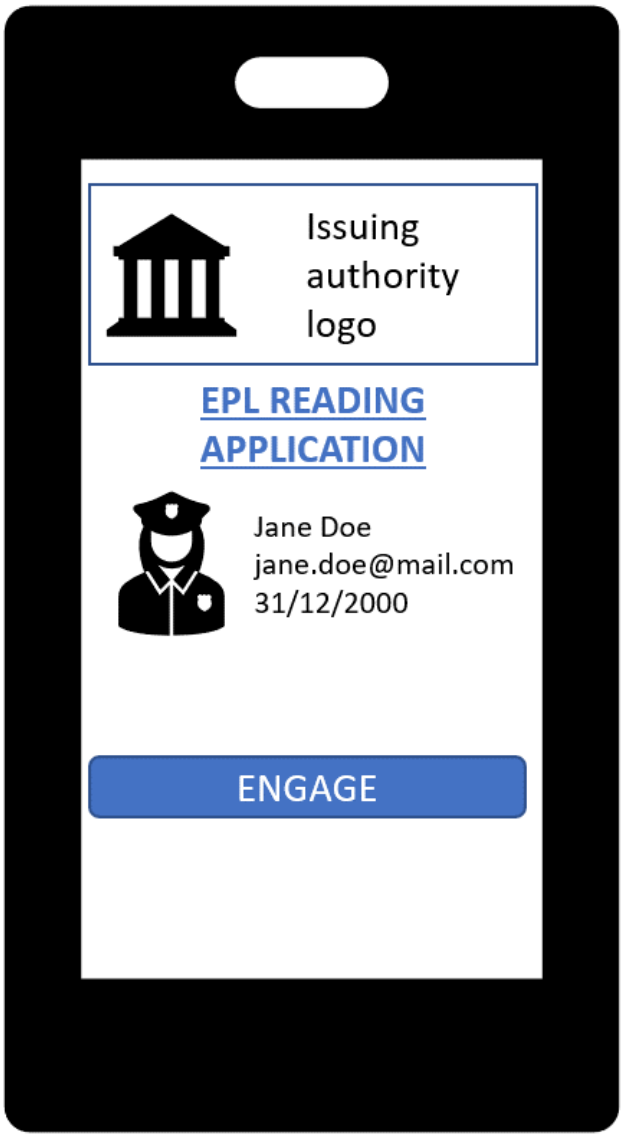
4.5.2. Downloading and installing EPLRAP

(a) Each verifying authority can decide to develop its own EPLRAP in any operating system that best suits the authority's purposes. Unlike the EPLAPP, the verification application will be developed to be used only by the verifying authority's staff. Therefore, it can be developed in accordance with the verifying authority's requirements provided it complies with the specifications of this AMC.

(b) The ability to download the application should not be publicly available. The verifying authority can install the EPLRAP on the devices of the staff who need to perform verification of the licence issued in electronic format.

4.5.3. Reading licence issued in electronic format with EPLRAP

Figure 23 — EPLRAP home page



(a) The home page of the EPLRAP will have the user's basic information — see Figure 23. It does not need to have personal data; the officer/inspector number or any other type of identification the authority considers necessary should be enough.

(b) Under the person's details, there should be an 'Engage' button that will activate the EPLRD camera to read the QR code generated in the EPLAPP. Once the code is read, the EPLRAP will manage the information from the QR code and proceed with the device engagement (see Section 0).

(c) With the devices engaged, the licence verifier should send a request to the EPLHD, specifying the data to be retrieved from the licence issued in electronic format. By default, the EPLRAP will have the following requests available:

(1) Inspection data retrieval: This request will contain the minimum data set necessary to proceed with a ramp inspection, as defined by ICAO.

(2) Full licence data retrieval: This request will contain all the licence information of the licence issued in electronic format.

(3) Customised data retrieval: This option will allow the licence verifier to choose which items of the licence issued in electronic format to request to be retrieved from the licence issued in electronic format.

(d) Once the set of data to be requested has been selected, the licence verifier needs to indicate the data retrieval mode (device retrieval or server retrieval).

(e) With the selections defined, the EPLRAP will generate the data retrieval request and send it to the EPLHD. Only if the licence holder authorises the data retrieval will the licence information of the licence issued in electronic format be retrievable.

(f) The EPLRAP should display the licence information of the licence issued in electronic format in accordance with the data dissemination option authorised by the licence holder.

4.5. Data retention

(a) The information should be kept only during the time necessary for the inspection and accident/incident processes and be removed within 24 hours from the end of the verification process. Appendix D to ICAO Doc 10190 specifies the policy on data retention in EPLRDs.

(b) If a verifying authority requires to keep data from the licence issued in electronic format, the licence holder, who will be properly informed, should be notified and agree in writing.

5. DATA MODEL

5.1 EPLDS

(a) All types of licences issued in electronic format should be compliant with the common EPLDS that has been defined in the applicable Regulation. Table 2 lists how the licence data of the licence issued in electronic format is structured, and has the following structure:

— Section: Defines a portion of a licence that contains specific data units that have a logical relation with each other

— Data unit: Piece of licence data of the licence issued in electronic format that defines specific information.

(b) However, not all the data units of the EPLDS are included in the MSO signed by the IAPKIC. In the column 'MSO', those data units to be included in the MSO are specified. In addition, the column 'Presence' determines which data units are mandatory (M), which ones are optional (O) and which ones are mandatory as long as they are applicable (M*). For example, medical limitations are mandatory if there are any, but are not mandatory if there are none or if a certain type of licence does not require to have medical information associated with it.

Table 2 — EPLDS

Section	Data unit	Data unit description	MSO	Presence
General	I	Name of state	Yes	M
	II	Title of licence	Yes	M
	III	Serial number of licence	Yes	M
Personnel information	IVa	Photograph of holder	Yes	M
	IVb	Name of holder in full	Yes	M
	IVc	Date of birth	Yes	M
	V	Address of holder	Yes	M
	VI	Nationality of holder	Yes	M
	VII	Script signature of holder	No	M*
Issuing authority	VIII	Authority and conditions under which the licence is issued	Yes	M
	IX	Certification concerning validity and authorisation for holder to exercise privileges appropriate to the licence	Yes	M
	X	Electronic signature of officer issuing the licence and the date and time of issue	No	
	XIa	Seal or stamp of authority issuing the licence	Yes	M
	XIb	Date and time of last synchronisation with the server of the national competent authority	No	
	XIc	Machine-readable code to retrieve authentication data	No	
Rating	XII	Ratings	Yes	M

Remarks	XIII	Remarks, i.e. special endorsements relating to limitations and endorsements on privileges, including endorsement of language proficiency, and other information required pursuant to Article 39 of the Chicago Convention	Yes	M*
	XIV	Any other details desired by the state issuing the licence	Yes	M*
Medical assessment	XVa	Class (1, 2 or 3)	Yes	M*
	XVb	Expiry date	Yes	M*
	XVc	Special medical limitations	Yes	M*
	XVd	Other information associated with the medical assessment as determined by the medical authority	Yes	M*
Additional supplementary information	XVIa	Other information associated with the licence	Yes	M*
	XVIb	Other information associated with the licence	Yes	M*
	XVIc	Other information associated with the licence	Yes	M*

5.2. EPLDM

(a) The data model needs to be followed in order to guarantee the interoperability of licences issued in electronic format around the world.

(b) The licence issued in electronic format will consist of an mdoc that is divided into several namespaces, each one related to one of the sections of the EPLDS and composed of several items that provide the licene information.

(c) The doctype for a licence issued in electronic format is int.icao.epl.X, where 'X' reflects the version of the licence issued in electronic format. It is expected that the licence issued in electronic format will be subject to changes due to amendments and new requirements that may apply in the future. In the first version of the doctype, X = 1, and it will be increased with future versions. Each namespace is directly related to a section of the EPLDS.

(d) Table 3 provides the namespaces.

Table 3 — Namespaces of the licence issued in electronic format

Namespace	EPLDS section	Data units
int.icao.epl.general.1	General	Name of state, title of licence, serial number of licence
int.icao.epl.personnel.1	Personnel information	Photograph of holder, name of holder, date of birth, address of holder, nationality of holder, script signature of holder
int.icao.epl.authority.1	Issuing authority	Name of authority, conditions under which the licence is issued, certification concerning validity and authorisation for holder to exercise privileges, signature of

		the officer issuing the licence, seal of the authority, date and time of last synchronisation, machine-readable code to retrieve authentication data
int.icao.epl.ratings.1	Ratings	List of ratings of the licence
int.icao.epl.remarks.1	Remarks	List of remarks
int.icao.epl.medical.1	Medical assessment	Medical certificate class, expiry date, medical limitations
int.icao.epl.additional.1	Additional supplementary information	Any other relevant licence information related to the licence

(e) The following sections of this AMC define how the information in each data unit should be formalised in the EPLDM. A single data unit may be composed of one or more items; for example, some data units have one item with the information in English and another item with the information in national languages other than English, so the EPLDM can provide the means to use up to eight languages in addition to English. All the information from the EPLDM in English conforms to what is called the ICAO version, which is the one expected to be used by states other than the issuing state.

(f) Each item will be determined by the following components:

(1) Its own identifier, which makes it possible to uniquely identify the item and allows a verifier to select which items will be included in either the device retrieval request or the server retrieval request as specified in Section 0.

(2) An encoding format that defines how the item is encoded. The concise data definition language as defined in RFC 8610 is used where possible, and ISO 180136-5 Section 7.2.1 provides encoding formats for data retrieval for concise binary object representation and Java simple object notation.

(3) A maximum size, which limits the size an item can have.

These components will be specified in the following subchapters of this AMC.

5.2.1. Namespace int.easa.epl.general.1

The namespace int.icao.epl.general.1 includes elements I, II and III of the EPLDS. This namespace has been adapted into int.easa.epl.general.1 so that it allows the introduction of several titles in a licence issued in electronic format, in contrast to int.icao.epl.general.1, which permits the incorporation of only one title.

5.2.1.1. Data unit I — name of state

The ‘name of state’ data unit provides the name of the issuing state. It is composed of the items in Tables 4–6.

Table 4 — state_fullname.english

Identifier	state_fullname.english	**Presence**	M
Description	Full name of state. Expressed in English. UTF-8-encoded basic Latin characters		
Encoding format	tstr	**Maximum size**	128 B

Table 5 — state_fullname.national

Identifier	state_fullname.national	**Presence**	O
Description	Full name of state. Expressed in national language. ITF-8-encoded full Unicode character set		

Encoding format	[*NationalStateName]
	
	NationalStateName = {
	language : tstr
	state_fullname : tstr
	}
		Maximum size	Array length: 8
			Language: 3 B
			state_fullname: 512 B

Table 6 — state_countrycode

Identifier	state_countrycode	**Presence**	M
Description	2-letter code of the issuing state as defined in ICAO Doc 9303 Part 3		
Encoding format	tstr	**Maximum size**	2 B

5.2.1.2. Data unit II — title of licence

List of titles linked to the licence, when applicable. This data unit is composed of the items in Tables 7 and 8.

Table 7 — title.english

Identifier	title.english	**Presence**	M
Description	Title or titles of the licence, as defined in each regulation. Expressed in English. UTF-8-encoded Latin characters		

Encoding format	[*EnglishLicenceTitle]
	
	EnglishLicenceTitle = {
	title : tstr
	titleissuance: full-date
	}
		Maximum size	Array length: 5
			title: 1 024 B
			titleissuance: 64 B

Table 8 — title.national

Identifier	title.national	**Presence**	O
Description	Title or titles of licence, as defined in each regulation. Expressed in national language. UTF-8-encoded full Unicode character set		

Encoding format	[*NationalLicenceTitle]
	
	NationalLicenceTitle = {
	language : tstr
	languagetitle: [*LanguageTitle]
	}
	
	Languagetitle = {
	title : tstr
	titleissuance: full-date
	}
		Maximum size	Array length: 8
			language: 3 B
			
			languagetitle:
			Array length: 5
			title: 1 024 B
			titleissuance: 64 B

5.2.1.3. Data unit III — serial number of the licence

This gives the serial number of the licence as defined by each applicable regulation. It is composed of the items in Tables 9 and 10.

Table 9 — serial_number.english

Identifier	Serial_number.english	**Presence**	M
Description	Serial number of the licence. UTF-8-encoded basic Latin characters		
Encoding format	tstr	**Maximum size**	128 B

Table 10 — serial_number.national

Identifier	serial_number.national	**Presence**	O
Description	Serial number of the licence. Expressed in national language. UTF-8-encoded full Unicode character set		
Encoding format	[*NationalSerialNumber] NationalSerialNumber = { language : tstr serial_number : tstr	**Maximum size**	Array length: 8 Language: 3 B Serial_number: 128 B

	}		

5.2.2. Namespace int.easa.epl.personnel.1

The namespace int.icao.epl.general.1 includes data units IVa, IVb, IVc, V and VI of the EPLDS. This namespace has been adapted because, unlike int.icao.epl.general.1, it does not include either the picture (IVa) or the address (V) of the holder of the licence in electronic format.

The signature of the holder of the licence in electronic format (VII) is included in the personnel section of the EPLDS but is not included in the MSO; therefore, it is not included in the EPLDM.

5.2.2.1. Data unit IVb — name of the holder of the licence in electronic format

The 'name of holder in full' data unit provides the name of the licence holder. It is composed of the items in Tables 11–14.

Table 11 — name.latin.primary

Identifier	name.latin.primary	**Presence**	M
Description	Primary name of the holder of the licence issued in electronic format. UTF-8-encoded basic Latin characters Restrictions and recommendations are defined in ICAO Doc 9303 Part 3. If the national characters are not Latin-based, a transcription or transliteration into Latin characters shall be provided.		
Encoding format	tstr	**Maximum size**	512 B

Table 12 — name.latin.secondary

Identifier	name.latin.secondary	**Presence**	M
Description	Secondary name of the holder of the licence issued in electronic format. UTF-8-encoded basic Latin characters. Restrictions and recommendations are defined in ICAO Doc 9303 Part 3. If the national characters are not Latin-based, a transcription or transliteration into Latin characters shall be provided.		
Encoding format	tstr	**Maximum size**	512 B

Table 13 — name.national.primary

Identifier	name.national.primary	**Presence**	O
Description	Primary name of the holder of the licence issued in electronic format. UTF-8-encoded full Unicode character set		
Encoding format	[*NationalNamePrimary]	**Maximum size**	Array length: 8 Language: 3 B

	NationalNamePrimary = {
	language : tstr
	primary_name: tstr
	}
			primary_name: 1 024 B

Table 14 — name.national.secondary

Identifier	name.national.secondary	**Presence**	O
Description	Secondary name of the holder of the licence issued in electronic format. UTF-8-encoded full Unicode character set		

Encoding format	[*NationaNameSecondary]
	
	NationalNameSecondary= {
	language : tstr
	secondary_name : tstr
	}
		Maximum size	Array length: 8
			Language: 3 B
			secondary_name:
			1 024 B

5.2.2.2. Data unit IVc — date of birth

Table 15 — dob

Identifier	dob	**Presence**	M
Description	Year, month and day on which the holder of the licence issued in electronic format was born		
Encoding format	Full-date	**Maximum size**	10 B

5.2.2.3. Data unit VI – nationality of holder

Table 16 — nationality.english

Identifier	nationality.english	**Presence**	M
Description	Nationality of the holder of the licence issued in electronic format. Expressed in English. UTF-8-encoded Latin characters		
Encoding format	tstr	**Maximum size**	64 B

Table 17 – nationality.national

Identifier	nationality.national	**Presence**	O
Description	Nationality of the holder of the licence issued in electronic format. Expressed in national language. UTF-8-encoded full Unicode character set		

Encoding format	[*NationalNationality]
	
	NationalNationality = {
	language : tstr
	nationality : tstr
	}
		Maximum size	Array length: 8
			Language: 3 B
			nationality: 256 B

Table 18 — nationality.countrycode

Identifier	nationality.countrycode	**Presence**	O
Description	Nationality of the holder of the licence issued in electronic format as 2-letter code as defined in ICAO Doc 9303 Part 3		
Encoding format	tstr	**Maximum size**	2 B

5.2.3. Namespace int.easa.epl.authority.1

5.2.3.1. Data unit VIII — authority and conditions under which the licence is issued

Table 19 — licensing.authority.latin

Identifier	licensing.authority.latin	**Presence**	M
Description	Name of the licensing authority. Expressed in English. UTF-8-encoded Latin characters. Translation to English is recommended		
Encoding format	tstr	**Maximum size**	256 B

Table 20 — licensing.authority.national

Identifier	licensing.authority.national	**Presence**	O
Description	Name of the licensing authority. Expressed in national language(s). UTF-8 encoded using full Unicode character set		

Encoding format	[*NationalLicensingAuthority]
	
	NationalLicensingAuthority = {
	language : tstr
	licensing_authority : tstr
	}
		Maximum size	Array length: 8
			Language: 3 B
			Licensing_authority: 512 B

Table 21 — licensing.conditions.english

Identifier	licensing.conditions.english	**Presence**	M
Description	Conditions under which the licence is issued. Expressed in English. UTF-8-encoded Latin characters. Translation to English is recommended.		
Encoding format	tstr	**Maximum size**	256 B

Table 22 — licensing.authority.national

Identifier	licensing.authority.national	**Presence**	M
Description	Name of the licensing authority in the national language/working language of the licensing authority, UTF-8 encoded using full Unicode character set		

Encoding format	[*NationalLicensingAuthority]
	
	NationalLicensingAuthority = {
	language : tstr
	licensing_authority : tstr
	}
		Maximum size	Array length: 8
			Language: 3 B
			Licensing_conditions: 512 B

5.2.3.2. Data unit IX — certification concerning validity and authorisation for the holder to exercise privileges appropriate to the licence

Table 23 — certification.english

Identifier	certification.english	**Presence**	M
Description	Certification concerning validity and authorisation for the holder to exercise privileges appropriate to the licence. Expressed in English. UTF-8-encoded Latin characters. Translation to English is recommended.		
Encoding format	tstr	**Maximum size**	256 B

Table 24 — certification.national

Identifier	certification.national	**Presence**	O
Description	Certification concerning validity and authorisation for the holder to exercise privileges appropriate to the licence. Expressed in national language(s). UTF-8 encoded using the full Unicode character set		
Encoding format	[*NationalCertification] NationalCertification = { language : tstr NationalCertification : tstr	**Maximum size**	Array length: 8 Language: 3 B nationalcertification: 512 B

	}		

5.2.3.3. Data unit X — electronic signature of officer issuing the licence and the date and time of such issue

This data unit is not included in the MSO; therefore, it is not included in the EPLDM.

5.2.3.4. Data unit XIa — seal or stamp of authority issuing the licence

This data unit is excluded from the MSO as per EASA specifications.

5.2.3.5. Data unit XIb — date and time of last synchronisation with the server of the issuing authority

This data unit is not included in the MSO; therefore, it is not included in the EPLDM.

5.2.3.6. Data unit XIc — machine-readable code to retrieve authentication data

This data unit is not included in the MSO; therefore, it is not included in the EPLDM.

5.2.4. Namespace int.easa.epl.ratings.1

(a) The namespace int.icao.epl.ratings.1 includes data unit XII of the EPLDS. This namespace has been adapted because of the prevalence of personnel licences in the ICAO specifications, the difficulty of linking remarks and the instrument rating (for pilot licences) to a certain class or type rating.

(b) The list of ratings is provided by an array where each rating makes use of a row of the array, and its particularities are provided as attributes of the rating. Table 25 provides a visual example for the ratings array, where each column is an attribute of the rating.

Table 25 — EASA ratings array

Rating No	archetype	endorsement	valid_since	valid_until	ir_valid_until	other1	other2
1							
2							
3							
4							
…							
64							

(c) The rating number is not an attribute; it has been added for comprehension purposes, reflecting the fact that each rating of the licence makes use of a row of the array and that the number of rows in the array is limited to 64.

(d) The meaning of each one of the attributes is as follows:

(1) archetype:

The archetype defines which kind of rating is being provided. It can be seen as a grouping of ratings of the same nature. For example, an archetype ‘fcl_type’ can be defined to classify all the type ratings of a pilot licence (A320, A340, B737, etc). Therefore, the archetype is a classification of the ratings by their nature.

(2) endorsement:

The endorsement attribute contains the code or value used to endorse a rating. Together with the archetype value, the rating endorsed on the licence is completely identified, because it is known what kind of rating is being endorsed and what its value is. Table 26 provides some examples of this with different types of licences.

Table 26 — Examples of archetypes and endorsements

Type of licence	Archetype	Endorsement
ATCO	atc_rating	ACP
	atc_rating_endorsement	ACP/OCN
	atc_instructor	OJTI

(3) valid_since:

The valid_since attribute specifies the date on which the endorsement starts to be valid. This is, it can be the date when a rating was endorsed, revalidated or renewed.

(4) valid_until:

This is the date on which the rating endorsed ceases to be valid. It will have no value for non-expiring ratings.

(5) ir_valid_until:

This is the date on which the instrument rating associated with the rating endorsed expires, if applicable.

(6) other1:

The other1 column specifies other information associated with the rating, with a preference for privileges linked to the rating that is being endorsed.

(7) other2:

The other2 column specifies other information associated with the rating, with a preference for the limitations linked to the rating that is being endorsed.

(e) Each type of licence requires a certain degree of standardisation in both taxonomy and methodology when endorsing ratings in licences issued in electronic format. The archetypes available, as well as the taxonomy and methodology of endorsement are provided in AMC1 Point 3.1 of Appendix I to Annex VI (Part-ARA).

(f) Therefore, the data model for ratings would be as in Table 27 and Table 28.

Table 27 — ratings.english

Identifier	ratings.english	**Presence**	M
Description	Ratings entered on or associated with the licence. Expressed in English. UTF-8-encoded basic Latin characters		
Encoding format	[*Rating]	**Maximum size**	Array length: 64

	Rating = {
	archetype : tstr
	endorsement : tstr
	valid_from : full-date
	valid_until : full-date
	ir_date : full-date
	other_1 : tstr
	other_2 : tstr
	}		

Table 28 — ratings.national

Identifier	ratings.national	**Presence**	O
Description	Ratings entered on or associated with this licence. Expressed in national language / working language. UTF-8-encoded full Unicode character set		

Encoding format	[*NationalRatings]
	
	NationalRatings = {
	language : tstr
	Ratings : [*Rating]
	}
	
	Rating = {
	archetype : tstr
	endorsement : tstr
	valid_from : full-date
	valid_until : full-date
	ir_date : full-date
	other_1 : tstr
	other_2 : tstr
	}
		Maximum size	Array length: 8
			language: 3 B
			
			Ratings length: 64

5.2.5. Namespace int.easa.epl.remarks.1

The namespace int.icao.epl.remarks.1 includes data units XIII and XIV of the EPLDS. This namespace has been adapted into the namespace int.easa.epl.remarks.1 because, unlike int.icao.epl.remarks.1, it does not include language proficiency. Section XIV has been developed to allow the endorsement of national ratings.

5.2.5.1. Data unit XIII – remarks

Data unit XIII – remarks is composed of the items in Tables 29 and 30.

Table 29 — remarks.english

Identifier	remarks.english	**Presence**	M*
Description	Remarks. Expressed in English. UTF-8-encoded Latin characters		
Encoding format	tstr	**Maximum size**	512 B

Table 30 — remarks.national

Identifier	remarks.national	**Presence**	O
Description	Remarks. Expressed in national language(s). UTF-8-encoded full Unicode character set		

Encoding format	[*NationalRemarks]
	
	NationalRemarks = {
	language : tstr
	remarks : tstr
	}
		Maximum size	Array length: 8
			Language: 3 B
			remarks: 1 024 B

5.2.5.2. Data unit XIV — state remarks

This section should specify any other remarks that the issuing authority considers necessary. It is considered that all the remarks should be in Section XIII and this section could provide the national ratings that the holder might have. It is composed of the items in Tables 31 and 32.

Table 31 — state_remarks.english

Identifier	State_remarks.english	**Presence**	M*
Description	National ratings entered on or associated with the licence. Expressed in English. UTF-8-encoded basic Latin characters		
Encoding format	[*NationalRating] NationalRating = { archetype : tstr endorsement : tstr	**Maximum size**	Array length: 64

	valid_from : full-date valid_until : full-date ir_date : full-date other_1 : tstr other_2 : tstr }		

Table 32 — state_remarks.national

Identifier	state_remarks.national	**Presence**	O
Description	National ratings entered on or associated with this licence. Expressed in national language / working language. UTF-8-encoded full Unicode character set		

Encoding format	[*NationalRatingsList]
	
	NationalRatingsList = {
	language : tstr
	NationalRatings : [*NationalRating]
	}
	
	NationalRating = {
	archetype : tstr
	endorsement : tstr
	valid_from : full-date
	valid_until : full-date
	ir_date : full-date
	other_1 : tstr
	other_2 : tstr
	}
		Maximum size	Array length: 8
			language: 3 B
			
			National Ratings length: 64

5.2.6. Namespace int.icao.epl.medical.1

No changes from ICAO specifications.

5.2.7. Namespace int.icao.epl.additional.1

No changes from ICAO specifications.

5.2.8. Namespace int.easa.epl.acronyms.1

This namespace has been included in order to facilitate comprehension for verifiers from third countries who are not familiar with the taxonomy defined in the EU regulations and associated AMC and GM.

5.2.8.1. Data unit – acronyms list

Table 33 — acronyms.english

Identifier	acronyms.english	**Presence**	O
Description	List of acronyms used in the licence with an explanatory description. Expressed in English. UTF-8-encoded Latin characters		

Encoding format	[*Acronym]
	
	Acronym = {
	code : tstr
	description : tstr
	}
		Maximum size	Array length: 25
			code: 10 B
			description: 256 B

Table 34 — acronyms.national

Identifier	Acronyms.english	**Presence**	O
Description	List of acronyms used in the licence with an explanatory description. Expressed in national language(s). UTF-8 encoded using the full Unicode character set		

Encoding format	[*NationalAcronym]
	
	NationalAcronym = {
	language : tstr
	acronyms : [*Acronym]
	}
	
	Acronym = {
	code : tstr
	description : tstr
	}
		Maximum size	Array length: 8
			Language: 3 B
			
			Array length: 25
			code: 10 B
			description: 256 B

6. IMPACT OF THE IMPLEMENTATION OF AN EPLSYS

6.1. Impact on the LICSYS when implementing an EPLSYS

(a) The LICSYS is independent from the EPLSYS, so there is no need for the LICSYS to use specific technologies of follow any specific data model. The issuing authorities can make use of solutions that best suit their purposes.

(b) However, prior to deciding any implementation of an EPLSYS, they should be aware of the implications that it can have for their LICSYS and assess whether they are ready and willing to proceed with the implementation.

6.1.1. Need to store the data as structured data

(a) The EPLSYS requires that all the information in the licence issued in physical format and medical certificates be transferred to an mdoc that follows the EPLDM. Therefore, the information should be stored in the LICSYS as structured data and thus contain all the information about the EPLDS. For example, the licence holder's date of birth is displayed in the licence issued in electronic format, so the database of the LICSYS should have a specific field for this information in order to use it to feed the information to the licence issued in electronic format. A more problematic example could be the issuing authority officer's electronic signature; usually LICSYSs used for licences issued in physical format do not need to store this signature, because this licence is signed once the licence has been printed and it is signed outside the LICSYS, but if an EPLSYS is implemented, this signature is electronic and must be stored in the LICSYS.

(b) It is not necessary that the LICSYS follow the EPLDM, even though the information from the LICSYS is transferred to the mdoc, because the issuing authority, when developing the EPLSYS, can use a process that transforms the LICSYS data model into the EPLDM. A LICSYS with a data model aligned with the EPLDM would facilitate the transfer of information between the two systems, but it is not necessary.

(c) The competent authorities should take into consideration that the EPLDM might change with time, so they should prepare their systems to be ready to work with different versions of the EPLDM.

6.1.2. Licence issuance format record

(a) If a competent authority decides to use both the physical format and the electronic format for a type of licence, the LICSYS will need to keep a record of the format used for each licence that has been issued in order to avoid the possibility that a licence in electronic format can be generated when a licence in physical format exists and vice versa.

(b) The competent authority cannot issue the same type of licence in electronic and physical format to the same individual.

6.1.3. Digital identification of the LICSYS users and traceability

(a) The EPLDS has information that comes from different data sources and is validated by people in different roles in the issuing authority (officers, medical assessors, examiners).

(b) The validation of the data is performed in the LICSYS and it will need to trace what information is changed or validated, by whom and when. This requires a log of the actions performed by its users.

(c) Internal users of the issuing authority might have access by means of a username and a password, but external users should be properly identified and access the LICSYS with at least two-factor verification in order to guarantee a proper level of security when accessing the LICSYS.

(d) Alternative and superior verification procedures can be applied, as long as they provide at least an equivalent level of security.

6.1.4. Need to use electronic signatures in order to validate the data

(a) The validation of the data is executed by the electronic signature of an issuing officer, an examiner or a medical assessor, each one responsible for the pertinent subset of licence data of the licence issued in electronic format. Therefore, the LICSYS must be able to operate with the use of electronic signatures.

(b) The electronic signature of the issuing officer is required to conform to recognised standards and have an appropriate level of security. In the EU context, the recognised standard is provided by Regulation (EU) No 910/2014[1] (eIDAS Regulation), and the appropriate level of security is at least an advanced signature.

(c) It is highly recommended that examiners and medical assessors also use electronic signatures, but they could use other forms of electronic signatures. In this case, at least a two-factor verification process or one that provides a higher level of security should be used.

6.1.5. Authorisation of access to data held by the issuing authority

(a) Without the implementation of an EPLSYS, the data on the IAS can be managed only by internal users of the issuing authority, or possibly by a controlled number of external users within the Member State.

(b) When licences issued in electronic format are used, the information in the IAS will be frequently accessed by external users, either for the generation of licences issued in electronic format or for its verification by verifiers and other verifying authorities from third countries.

(c) The EPLSYS will not work if this access is not permitted via web services that allow these external users to access the data. However, granting external parties access to the IAS has an impact on the security measures the issuing authority will have to implement.

6.1.6. Access to LYCSYS for examiners and medical assessors from other Member States

(a) Under the EU regulatory framework, a licence holder might be examined for a certain rating or have a medical assessment in a Member State other than the Member State issuing the licence. This information cannot be reflected in the licence issued in electronic format until it is received and inserted in the LICSYS of the issuing authority, causing a detrimental effect on the holder of a licence issued in electronic format.

(b) Third countries normally are not affected when using licences issued in electronic format, since the general rule is that all examiners and medical assessors belong to the same issuing authority.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

(c) The industry demands that the EPLSYS be at least as agile as the current LICSYS, so any issuing authority that wants to implement an EPLSYS should be willing to provide the means for examiners and medical assessors from other Member States to feed into their systems any new information affecting one of their licences and transfer the information to the licence in electronic format without unnecessary delays.

(d) Each issuing authority can decide how to grant this access to its LICSYS, but it will need to provide appropriate means of identification and signing.

(e) If the issuing authority detects any irregularity in the data provided by an examiner or medical assessor from another Member State, it should invalidate the licence issued in electronic format, and a new licence in electronic format should be generated in accordance with the valid data.

6.1.7. Use of the issuing authority's public key infrastructure certificate

(a) Licences issued in electronic format are automatically generated by the IAS when the licence holder sends a request for its generation, and are electronically signed with the IAPKIC. Issuing authorities willing to implement an EPLSYS also need to be willing to use the IAPKIC in automation.

(b) In some Member States, the use of the IAPKIC may require the approval of the government or some kind of national approval process.

6.2. Impact on the issuing authority's procedures when implementing an EPLSYS

(a) An assessment of the impact on the issuing authority's procedures caused by the implementation of an EPLSYS should be carried out in order to identify which procedures should be adapted.

(b) When an EPLSYS is implemented, the concepts of issuance, suspension and revocation of licences should be reviewed because the introduction of electronic documents comes with certain conventions within the digital world that challenge the standard practices with physical documents.

GM1 ATCO.AR.D.002(d) Licences issued in electronic format and establishment of an electronic personnel licence system

VERIFICATION OF THE AUTHENTICITY AND VALIDITY OF THE LICENCES ISSUED IN ELECTRONIC FORMAT

(a) The verification described under this point allows the reader to confirm that the information in the licence is authentic, meaning that it was issued by the competent authority mentioned in the licence, and is valid, meaning that it contains the data that was applicable at the time it was generated.

(b) Verifying the authenticity and validity of licences issued in electronic format may happen in two ways:

(1) By using a reading device registered with the authority that issued the licence when an internet connection is available. Alternatively, when no internet connection is available,

by using a reading device registered with the authority that issued the licence that is linked with the list of the valid issuing authority public key infrastructure (PKI) certificates.

In such cases, verifying the authenticity and validity of the licence of the holder is done by reading the machine-readable code included under field XIc of the licence.

The issuing authority PKI certificates are used to sign all licences in electronic format; they attest to the authenticity and validity of the licences in real time, when the licence is verified with internet connection available or at the time they were downloaded from the authority's server when the verification happens offline.

When it is expected that the verification will happen offline, the person authorised to verify the authenticity and validity of licences on behalf of the competent authority can ensure that they will be in possession of the most recent version of the list of the valid issuing authority PKI certificates.

(2) By reading the information contained in the licence of the holder when no internet connection is available and the authorised person is not in possession of the list of the valid issuing authority PKI certificates.

In such situations, the authorised person can compare the latest synchronisation date of the licence with the current date.

Using the information available, it can be assessed whether the information in the licence presented by the holder is up to date.

The person authorised to verify the authenticity and validity of licences can request support in accessing information in the authority's server if there is any doubt that the licence presented is outdated. The authorised person may also decide to verify the authenticity and validity of the licence again when internet connection is available within a reasonable time frame as defined in the competent authority's administrative procedures.

The update status of a licence can also be indicated by a notification system developed by the issuing authority stating that the latest update has not yet been manually triggered by the licence holder and, thus, that the licence information is outdated.

AMC1 ATCO.AR.D.002(h) Licences issued in electronic format and establishment of an electronic personnel licence system

PROCEDURE FOR LIMITATION, SUSPENSION OR REVOCATION OF A LICENCE ISSUED IN ELECTRONIC FORMAT

The procedure should describe the actions undertaken by the competent authority to ensure that the limitation, suspension or revocation of a licence issued in electronic format is properly reflected in the licence contained in the holder's device application.

Such actions should happen at the level of the electronic personnel licence system established by the competent authority to:

— in cases of limitation, notify the holder and request that they generate a new instance of the licence displaying only those categories, subcategories or ratings not subject to limitation;

— in cases of suspension or revocation, notify the holder and request that they update their licence, hereby deleting the current instance of the licence contained in the application and preventing the generation of new instances.

In cases of limitation or suspension of the licence, the procedure should include the generation of a new instance of the licence on the date such limitation or suspension ends.

Alternatively, the competent authority may display a permanent indication regarding the applicable limitation, suspension or revocation of the licence without which the licence cannot be displayed by the holder.

ATCO.AR.D.003 Change of competent authority

[…]

(c) The receiving competent authority shall, without undue delay, exchange the licence and medical certificate provided that it has received and processed all documents specified in point (a). Upon the exchange of the licence and medical certificate, the receiving competent authority shall immediately request the licence holder to surrender ~~to~~ ~~it~~ the licence issued by the transferring competent authority and the associated medical certificate, if issued in a physical format.

[…]

(f) In the case of a transfer of a licence issued in electronic format, the receiving competent authority and the transferring competent authority shall coordinate the revocation and reissue.

AMC1 ATCO.AR.B.010 Changes to the management system

COMPREHENSIVE RISK ASSESSMENT — ELECTRONIC PERSONNEL LICENCE SYSTEM

(a) The electronic personnel licence system will inherently introduce new risks within the management system (either safety management system, information security management system or the integrated management system). To address such new risks, the introduction of an electronic personnel licence system should entail a comprehensive risk assessment, and the risks identified should be adequately mitigated in each phase of the project.

(b) Such risk assessment should be an integral part of the competent authority's process for the management of changes.

ANNEX IV (Part ATCO.MED)

ATCO.MED.A.046 Suspension or revocation of a medical certificate

(a) Upon revocation of the medical certificate issued in physical format, the holder shall immediately return ~~the~~ this medical certificate to the licensing authority.

(b) Upon suspension of the medical certificate issued in physical format, the holder shall return ~~the~~ this medical certificate to the licensing authority on request of the authority.

APPENDIX 1 TO ANNEX II — ~~Format for licence~~(Student) air controller licence — EASA Forms 152 and 156

~~**AIR TRAFFIC CONTROLLER LICENCE**~~

1. General requirements for the (student) air controller licence

1.1. The competent authority shall issue each (student) air traffic controller licence in only one of the following two formats:

(a) the physical format, referred to in point 2 of this Appendix, or;

(b) the electronic format, referred to in point 3 of this Appendix.

1.2. When the competent authority uses both formats to issue (student) air traffic controller licences, it shall establish a procedure for changing from one format to the other.

1.3. Each licence holder shall have a unique licence holder number, established on the basis of a national identifier and an alpha-numeric designator.

1.4 The (student) air traffic controller licence shall be issued in English and any language(s) determined by the competent authority).

2. Requirements for the (student) air traffic controller licence issued in physical format

2.1. The (student) air traffic controller licence issued in physical format shall be issued in accordance with the format and content of EASA Form 152.

2.2. The (student) air traffic controller licence issued in physical format in accordance with this Regulation shall conform to the following specifications:

(a) Content. The item number shall always be printed in association with the item heading. Items I to XI are the 'permanent' items, and items XII to XIV are the 'variable' items which may appear on a separate or detachable part of the main form as prescribed below. Any separate or detachable part shall be clearly identifiable as part of the licence.

1. Permanent items:

(I) name of State of licence issue;

(II) title of licence;

(III) serial number of the licence with the United Nations (UN) country code of the State of licence issue and followed by '(Student) ATCO Licence' and a code of numbers and/or letters in Arabic numerals and in Latin script;

(IV) name of holder in full (in Latin script, even if the script of the national language(s) is other than Latin);

(IVa) date of birth;

(V) ~~holder's address, if required by the competent authority~~ reserved;

(VI) nationality of holder;

(VII) ~~signature of holder~~ - reserved;

(VIII) competent authority;

(IX) certification of validity and authorisation for the privileges granted, including the dates when they were first issued;

(X) signature of officer issuing the licence and the date of such issue;

(XI) seal or stamp of the competent authority.

2. Variable items:

(XII) ratings and endorsements (unit endorsements and licence endorsements, including language proficiency endorsements) with expiry dates (only for endorsements);

~~(XIII) remarks: language proficiency endorsements; and~~

~~(XIV) any other details required by the competent authority.~~

(b) The licence shall be accompanied by a valid medical certificate, except when only STDI privileges are exercised.

(c) Material. First quality paper ~~and/~~or other suitable material, including plastic cards, shall be used to prevent or readily show any alterations or erasures. Any entries or deletions in the form will be clearly authorised by the competent authority.

~~(d) Language. Licences shall be written in English and, if required by Member States, in national language(s) and other languages as deemed appropriate.~~

Cover page

Competent authority's name and logo (English and any language(s) determined by the competent authority) EUROPEAN UNION (English only) (STUDENT) AIR TRAFFIC CONTROLLER LICENCE [English and any language(s) determined by the competent authority] Issued in accordance with Commission Regulation (EU) 2015/340 This licence complies with ICAO Standards [English and any language(s) determined by the competent authority] **EASA Form 152 Issue ~~2~~3**		Requirements ([1]) 'European Union' to be 'deleted for non-EU Member States. Size of each page shall be one eighth A4.

([1]) *Requirements:*

The pages referring to the instructions on how the (Student) ATCO Licence has to be filled in are intended for use by the competent authority or the assessor specifically authorised to revalidate or renew the unit endorsements. Initial issues of ratings, rating endorsements, language endorsements, instructor and/or assessor endorsement will always be entered by the competent authority. Revalidation or renewal of unit endorsements will be entered by the competent authority or by the authorised assessors.

Page 2

I	**Name of State of issue:**		**Requirements:** **In bold type**
II	**Title of licence:**		**In very bold type**
III	Serial number of the licence:		The serial number of the licence, in Arabic numerals, will always start with the UN country code of the State of the licence issue, followed by '(Student) ATCO Licence'
IV	Name of ~~the~~ holder in full:		In Latin script also if script of national language is other than Latin
IVa	Date of birth:		dd-mm-yyyy ~~Standard date format is to be used, i.e. day/month/year in full (e.g., 31.01.2010)~~
V	RESERVED ~~Holder's address, if desired by the competent authority:~~ ~~Street, town, area, postal code~~		
VI	Nationality of holder:		Indicated by the UN country code of the State
VII	RESERVED ~~Signature of holder:~~		
VIII	Competent ~~A~~authority:		
X	Signature of officer issuing the licence and date of issue		
XI	Seal or stamp of issuing competent authority		

Page 3

<table>
<tr>
<td>IX</td>
<td>
Validity of privileges:
The holder is entitled to exercise the privileges of the following rating(s) and rating endorsement(s), when validated:
<table>
<tr><th>Rating(s)</th><th>Date of first issue</th></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>
<table>
<tr><th>Rating endorsement(s)</th><th>Date of first issue</th></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>
</td>
<td>
Requirements:

English and any language(s) determined by the competent authority.

The date of first issue of a rating and/or rating endorsement shall be the date of successful completion of the training relevant to that rating and/or rating endorsement.
</td>
</tr>
</table>

Page 4

XIIa Unit endorsements with expiry dates

The holder is entitled to exercise the privileges of the ~~following~~ rating(s) and rating endorsement(s) at the air traffic service unit(s) for which current unit endorsement(s) is (are) held as detailed below, only if the holder fulfils the requirements in ATCO.A.015:

Unit (ICAO indicator)	Sector/ Position	Rating/ Endorsement	Expiry date	Signature/stamp of the authority or licence number and signature of the assessor

Note: Field XIIa is not applicable for a Student ATCO Licence.

<table>
<tr>
<td>XIIb</td>
<td>Licence endorsements:

The holder is entitled to exercise the privileges of the following endorsement(s)

<table>
<tr><td>OJTI /STDI /Assessor endorsement</td><td>Expiry date</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

<table>
<tr><td>Language proficiency endorsement(s): [language(s)/level]</td><td>Expiry date</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>
</td>
<td>Requirements: N/A</td>
</tr>
</table>

~~XIII~~	~~**REMARKS:**~~ ~~*Language proficiency endorsement(s): [language(s)/level/expiry date]*~~	~~Language proficiency endorsement(s), level and expiry date shall be included.~~ ~~All additional licensing information to be entered here.~~

3. Requirements for the (student) air traffic controller licence issued in electronic format

3.1. The (student) air traffic controller licence issued in electronic format shall be issued in accordance with the format and content of EASA Form 156 and replicate the information contained in the records of the competent authority.

3.2. The (student) air traffic controller licence issued in electronic format shall have the electronic signature of the officer issuing the licence and the most recent date and time of issue.

3.3. The electronic signature shall be at least an advanced signature issued in accordance with Regulation (EU) No 910/2014.

3.4. The (student) air traffic controller licence issued in electronic format shall include a feature identified with the acronym 'ICAO' that allows it to display its contents in English.

3.5. The (student) air traffic controller licence issued in electronic format shall contain suitable active security features to differentiate it from a static image.

The competent authority issuing the licence in electronic format shall insert information in EASA Form 156 as follows:

— The competent authority shall determine the information to be inserted in the place of content between brackets ('[]'). When not applicable, it shall insert the words 'Not applicable'.

— The content of EASA Form 156 which is not between brackets ('[]') shall be inserted as such.

— IVa, V, VII and XIa shall be left blank.

— Completing Sections XVIa, XVIb, XVIc and XVIc is optional.

	Content requirements	Format requirements
I	European Union (*) [Name of Member State]	[Name of Member State] in bold type
II	(STUDENT) AIR TRAFFIC CONTROLLER LICENCE Issued in accordance with Commission Regulation (EU) 2015/340	All content in very bold type
III	Licence No [Member State code]	The Member State code shall be the United Nations country code of the Member State of the competent authority that issues the licence, followed by '(Student) ATCO Licence' The serial number of the licence ([XXXX]) shall be in Arabic numerals.
IVa		
IVb	Name of holder in full: [Name]	[Name] in Latin script also if script of national language is other than Latin
IVc	Date of birth of holder: [Date]	The date format shall be: dd-mm-yyyy (day-month-year)
V		
VI	Nationality of holder: [Nationality]	

VII		
VIII	[Name of Competent Authority]	
IX	Certification of validity and authorisation for the privileges granted, including the dates when they were first issued	Rating and rating endorsement with their date of first issue. The date of issue of a rating and/or rating endorsement shall be the date of successful completion of the training relevant to that rating and/or rating endorsement.
X	Electronic signature of officer issuing the licence: [Signature] Date and time of such issue: [Date] [Time]	[Date] in dd-mm-yyyy format (day-month-year) [Time] in hh:nn:ss (hours:minutes:seconds) 24-hour format
XIa		
XIb	Date and time of last synchronisation with the server of the issuing competent authority: [Date] [Time]	[Date] in dd-mm-yyyy format (day-month-year) [Time] in hh:nn:ss (hours:minutes:seconds) 24-hour format
XIc	Machine-readable code to retrieve authentication data: [Code]	
XII	Rating(s) and endorsement(s) with their expiry dates	Unit (ICAO indicator), sector/position, rating, rating/licence endorsement(s), expiry date Ratings and endorsements on the licence shall be inserted in accordance with a documented taxonomy.
XIII	*Reserved*	*Text in italics*

XIV	*Reserved*	*Text in italics*
XVa	Medical Class	Class 3
XVb	Expire date	dd-mm-yyyy (day-month-year)
XVc	Special medical limitation, if any [Text]	
XVd	Other information associated with the medical certificate	
XVIa	Other information associated with the licence as determined by the issuing competent authority: [Text]	
XVIb	Other information associated with the licence as determined by the issuing competent authority: [Text]	
XVIc	Other information associated with the licence as determined by the issuing competent authority: [Text]	

EASA Form 156 Issue 1

AMC1 Point 1.2 of Appendix 1 to Annex II — (Student) air traffic controller licence

PROCEDURE FOR CHANGING FROM ONE LICENCE FORMAT TO ANOTHER

The procedure should describe the triggering events, time and conditions associated with the format change for a licence already issued by the authority.

Changing the format of a licence means either:

— generating a licence in electronic format to replace a licence in physical format for the same holder; or

— producing a licence in physical format to replace a licence in electronic format for the same holder.

The events triggering the change of format of a licence may include the strategy adopted by the competent authority to issue licences in a specific format for one licence holder, a defined group of licence holders, or all licence holders.

Those events may also include any practical aspect justifying the use of one format rather than the other. Such practical aspects could be related to the appropriate use of that licence by the licence holder or the ability of the competent authority to issue licences as intended.

The time at which the format of a licence is changed should be predefined. It may be a date chosen by the competent authority or be associated with any processing of the licence for other purposes, such as:

— the addition of a new rating, rating endorsement or endorsements in the licence;

— the issuance of the licence in physical format due to administrative reasons.

The conditions under which the format of a licence is changed should include:

— the withdrawal of the existing licence issued in physical format or the invalidation of the existing licence in electronic format before the new licence is generated or produced, as applicable;

— the means through which the licence holder is notified of such change and can obtain the new licence.

AMC1 Point 3.1 of Appendix 1 to Annex II — (Student) air traffic controller licence

TAXONOMY FOR RATINGS AND ENDORSEMENTS IN (STUDENT) AIR TRAFFIC CONTROLLER LICENCES ISSUED IN ELECTRONIC FORMAT

(Student) air traffic controller licences issued in electronic format need to be readable by verifying devices worldwide to achieve interoperability.

For that purpose, a common information structure that any device can process should be established, so that reading applications developed by other authorities other than the issuing authority will be effective.

Therefore, licences issued in electronic format should be endorsed using a list of values specific to the rating or endorsement (hereinafter referred to as endorsements) being included in or endorsed on the licence.

In addition, as licences may contain more than one rating or endorsement, an array is necessary to list all the applicable endorsements.

The values and the array are defined and structured through the namespace ‘int.easa.epl.ratings.1’ in AMC1 ATCO.AR.D.002, with the attributes shown in Table 1.

Table 35 — EASA endorsement array

Rating #	archetype	endorsement	valid_since	valid_until	ir_valid_until	other1	other2
1							
2							
3							
4							
...							
64							

Note: The rating number (#) is not part of the array but is presented to reflect that each rating makes use of a row and that the array is limited to 64 ratings or endorsements.

For each rating and endorsement, each column of the array contains information as defined in the list of values set out in Parts 1, 2, 3 and 4 of this AMC.

1. Archetypes for (student) air traffic control licences

All ratings and endorsements belong to an archetype, which can be seen as a grouping of endorsements with similar characteristics and a common information type.

Table 2 — ATCO archetypes

Archetype	Description
atc_rating	Group of ATC rating
atc_rating_endorsement	Group of ATC rating endorsements
atc_unit_endorsement	Group of ATC unit endorsements
atc_instructor	Group of instructor ratings
atc_assessor	Group of assessor ratings
radiotelephony	Group of radiotelephony ratings
language_proficiency	Group of language proficiency ratings

2. Title taxonomy

Table 3 — Titles taxonomy for (student) air traffic control licences

Endorsement	Description
SATCO	Student air traffic controller licence
ATCO	Air traffic controller licence

3. Rating taxonomy

Table 4 — Ratings taxonomy for (student) air traffic control licences

Endorsement	Description	Standardised privileges/limitations	Comments
ADV	Aerodrome control visual		Article 8
ADC	Aerodrome control		ATCO.B.010
APP	Approach control procedural		ATCO.B.010

APS	Approach control surveillance		ATCO.B.010
ACP	Area control procedural		ATCO.B.010
ACS	Area control surveillance		ATCO.B.010
ADC/ SUR	Aerodrome control surveillance		ATCO.B.015
APS/ PAR	Precision approach radar		ATCO.B.015
APS/ SRA	Surveillance radar approach		ATCO.B.015
ACP/ OCN	Oceanic control		ATCO.B.015
ACS/ OCN	Oceanic control		ATCO.B.015
XXXX/ YYYYY	XXXX: ICAO location indicator YYYYY: sector or position code as defined by the Member State (if applicable)		ATCO.B.020
OJTI	On-the-job training instructor		ATCO.C.005
STDI	Synthetic training device instructor		ATCO.C.005
Assessor	Assessor		ATCO.C.045
AAA	ISO code		
RT	Radiotelephony		Appendix 1 to Annex II — Format for licence
Level number	Level number of language proficiency		ATCO.B.30 Accepted values: 4, 5 and 6

4. Endorsement methodology

Ratings shall be endorsed specifying their attributes as shown in Table 5.

Table 36 — Ratings endorsement methodology for (student) air traffic control licences

archetype	endorsement	valid_since	valid_until	ir_date	other_1	other_2
atc_rating	ADV	dd/mm/yyyy Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_rating	ADC	dd/mm/yyyy Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_rating	APP	dd/mm/yyyy Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_rating	APS	dd/mm/yyyy Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_rating	ACP	dd/mm/yyyy Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_rating	ACS	dd/mm/yyyy Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_rating_endorsement	ADC/SUR	dd/mm/yyyy Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_rating_endorsement	APS/PAR	dd/mm/yyyy	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used

		Date of first obtention				
atc_rating_ endorsement	**APS/SRA**	**dd/mm/yyyy** Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_rating_ endorsement	**ACP/OCN**	**dd/mm/yyyy** Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_rating_ endorsement	**ACS/OCN**	**dd/mm/yyyy** Date of first obtention	This attribute is not used	This attribute is not used	This attribute is not used	This attribute is not used
atc_unit_ endorsement	**XXXX/YYYY** One row for each unit endorsement Here the unit/sector or position codes are specified	This attribute is not used	**dd/mm/yyyy** Date of expiration	This attribute is not used	Here the rating and rating endorsements associated with the unit are specified	This attribute is not used
atc_ instructor	**OJTI**	This attribute is not used	**dd/mm/yyyy** Date of expiration	This attribute is not used	This attribute is not used	This attribute is not used
atc_ instructor	**STDI**	This attribute is not used	**dd/mm/yyyy** Date of expiration	This attribute is not used	This attribute is not used	This attribute is not used
atc_ assessor	**Assessor**	This attribute is not used	**dd/mm/yyyy** Date of expiration	This attribute is not used	This attribute is not used	This attribute is not used

Radio-telephony	**RT(A)**	**dd/mm/yyyy** Date of obtention, revalidation or renewal, as applicable	**dd/mm/yyyy** Date of expiring as applicable	This attribute is not used	**LAN1, LAN2, LAN3…** ISO 639-2 codes for languages (3 letters)	Limitations, if applicable, go here.
language_ proficiency	**LAN** ISO 639-2 codes for languages (3 letters)	**dd/mm/yyyy** Date of obtention, revalidation or renewal, as applicable	**dd/mm/yyyy** Date of expiring	This attribute is not used	**4,** **5,** **6** Language proficiency level as applicable	This attribute is not used

GM1 Point 3.1 of Appendix 1 to Annex II — (Student) air controller licence — EASA Forms 152 and 156

ELECTRONIC PERSONNEL LICENCE SYSTEM

(a) Implementing the electronic personnel licence system

(1) The issuance of electronic personnel licences by Member States is optional.

However, the *Convention on International Civil Aviation* (Doc 7300), Annex 1 – Personnel Licensing mentions the obligation for all ICAO States to recognise them.

(2) The electronic personnel licence system can be scalable to the needs of each Member State, its service providers, licence holders and applicants.

An efficient electronic personnel licence system will be achieved through thoughtful planning and implementation, ensuring that it meets not only requirements of the *Convention on International Civil Aviation* (Doc 7300) and its Annexes, but also the applicable national and European regulations.

(3) When implementing an electronic personnel licence system, Member States may also take into consideration its integration with already existing licensing systems, including, but not limited to:

(i) initial issuance of the licence;

(ii) licence conversion, suspension or revocation;

(iii) integration with the software used by the competent authority; and

(iv) links to other IT frameworks required (e.g. other Member State entities, organisations), when applicable.

(4) Prior to introducing the electronic personnel licence system, Member States may consider the following aspects:

(i) Regulatory framework

Member States need to determine whether the current national regulatory framework would allow the implementation of the electronic personnel licence system regulations (e.g. privacy laws, relevant information technology regulations, data protection). If not, Member States may need to amend their current national regulations or introduce new regulations.

(ii) Risk analysis

The electronic personnel licence system will inherently be exposed to new risks. In order to address new risks, the introduction of the system may be driven by the results of a risk assessment in each phase of the project. A risk assessment could be a part of the Member State's integrated risk management that would allow the identification and evaluation of common risks, as well as the development of an action plan that addresses key risks and effective mitigation of those risks.

The electronic personnel licence system may be incorporated in the information security management system of the competent authority or in a suitable equivalent, which is used by the competent authority. Guidance on conducting risk assessments is provided in the Safety Management Manual (ICAO Doc 9859).

(iii) Resources

Competent authorities need to ensure that they have sufficient resources to introduce and maintain an electronic personnel licence system. This includes financial resources, as well as human resources.

If the competent authority does not have qualified personnel to develop and maintain the electronic personnel licence system, some of the work may be outsourced.

A competent authority may invest time and resources not only in implementation, but also in equipment and technology, the work environment, employees and operating systems.

The competent authority may be prepared to invest in the systems and processes, as well as to develop policies that provide optimal global interoperability and performance of the electronic personnel licence system.

(iv) Service providers and licence holders

Competent authorities need to consider how the electronic personnel licence system will affect their service providers, licence holders and applicants.

(5) It is recommended that the competent authority prepare a comprehensive project initiation document defining the scope, the impact on the existing national licensing

system, a risk assessment, the electronic personnel licence system features and other elements.

(6) While developing the electronic personnel licence system, it is advisable to consider the potential scalability of the system in terms of how the system could be applied to other licensing or certification areas, in order to capitalise on the work involved and the know-how developed by the Member State during the implementation of the electronic personnel licence system.

(7) It is advisable to conduct a post-implementation analysis of the electronic personnel licence system in order to capture the lessons learned and the benefits of the realisation of the project.

(b) Features of the electronic personnel licence system

(1) The electronic personnel licence system typically consists of the following major parts:

(i) a server-based licence management system with a user interface management system;

(ii) (an) application(s) installed on (a) self-contained mobile electronic visual display device(s); and

(iii) a system to support surveillance activities by the Member State's own inspectors and by inspectors from other competent authorities.

(2) The purpose of the application installed on a self-contained mobile electronic visual display device is to provide the licence holder with a means to show the approved and updated privileges conferred upon the individual by the competent authority.

Secure communication between the electronic personnel licensing system of the competent authority and the self-contained mobile electronic visual display device can be via internet or other electronic means as deemed appropriate by the issuing competent authority.

(3) In addition, the electronic personnel licence system can enable authorised persons to perform verification.

(c) Expected level of performance

Competent authorities intending to introduce an electronic personnel licence system may ensure the following:

(1) a high degree of security preventing forgery, data leaking and other security events;

(2) a highly reliable delivery of the correct information, at the right time and to the right person;

(3) the ability to detect corrupted data and service interruptions, and to initiate timely corrective actions;

(4) the ability of the electronic personnel licence system to be used for verification purposes in circumstances where electronic access to the information is not possible; and

(5) robust contingency arrangements to manage unexpected events; for example, in the event of a primary component outage of the electronic personnel licence system within the competent authority, a process to transfer to back-up systems in order to maintain the availability of the data.

(d) Electronic personnel licence system elements

The electronic personnel licence system may include the following:

(1) infrastructure for processing, storage, network communications, security and other enabling software and hardware;

(2) data access to provide secure licence information resource support for services related to the electronic personnel licences, licence holders and persons authorised to verify the authenticity and validity of the licences as well as a comprehensive level of integration with the regulatory information management system of the competent authority;

(3) a business application to provide services for the issue, conversion, suspension, limitation or revocation of (student) air traffic controller licences issued in electronic format, and for the display, query, verification and record-keeping of the electronic personnel licences;

(4) a user-friendly interface which provides correct data to the right addresses when needed.

The system architecture of the electronic personnel licence system may be supported by security controls in layers providing role-based access to data, as well as by operations and the maintenance support functions.

The integration of these controls and functions may be aligned with relevant and appropriate standards and specifications, as well as regulatory system integration standards and requirements. It is recommended not to implement single points of failure in any of the layers.

(e) Compliance with the applicable national and EU regulations, including privacy and personal data protection

The electronic personnel licence system is subject to compliance with the applicable national and EU regulations, including the privacy and data protection laws.

In reviewing the privacy and data protection laws, Member States may consider the following:

(1) What is personal data?

(2) What personal data is collected and for what purposes?

(3) How is personal data retained?

(4) With whom will personal data be shared and for what purposes?

(5) How long is personal data retained?

(6) Is there any international transfer of personal data? Where? Under which legal basis?

(7) How can data subjects access, update, delete or correct their personal data?

(8) What steps are taken to ensure the security of personal data?

(9) Whom can data subjects contact to exercise their rights in accordance with national and EU regulations on personal data protection?

(10) What is the complaint process?

(f) Security specifications

(1) Member States intending to implement an electronic personnel licence system may ensure a high degree of security to prevent forgery, data leaking and other security events. Information security as well as compliance with the applicable national and EU regulations concerning information security may be considered during all phases.

(2) The main areas of security risks may include:

(i) loss or inauthenticity of data (e.g. invalidity, spoofing);

(ii) network or device malware infection; and

(iii) protection of private data.

(3) A risk assessment may be performed by the competent authority in order to identify the major risks associated with an electronic personnel licence system. In addition, it is recommended that a register of identified risks be maintained to minimise the likelihood that the competent authority will lose sight of its known risks.

(g) Training and supporting guidance material

(1) The development of training and supporting guidance material, appropriate to their roles and responsibilities, are recommended for all personnel who may interact with the electronic personnel licence system. Such personnel may include licence applicants and holders, competent authority personnel, inspectors (both domestic and foreign) and electronic personnel licence system personnel.

Possible training and guidance topics could include:

(i) the use of the electronic personnel licence system, including its features and capabilities;

(ii) the online and offline verification of the authenticity and validity of the electronic personnel licences, including the use of any tools or applications, as well as the description of included features (e.g. active security features to differentiate it from a static image);

(iii) contingency actions, including cases of loss of or damage to the self-contained mobile electronic visual display device used for the electronic personnel licences;

(iv) any other training and guidance that a Member State may find to be necessary.

(2) In addition to the topics identified in point (1), it is recommended that personnel whose responsibilities include verifying, adding, deleting, amending or approving amendments to electronic personnel licence data also receive regularly updated training in the following subjects:

(i) administration of the electronic personnel licence system, including record-keeping, maintenance and troubleshooting;

(ii) security training and awareness; and

(iii) training in monitoring of emerging risks.

AMC1 Point 3.2 of Appendix 1 to Annex II — (Student) air controller licence — EASA Forms 152 and 156

ELECTRONIC SIGNATURES IN THE LICENCES ISSUED IN ELECTRONIC FORMAT

The electronic signatures in licences issued in electronic format should be affixed in accordance with the specifications of Section 5.1.4 of AMC1 ATCO.AR.D.002.

GM1 Point 3.5 of Appendix 1 to Annex II — (Student) air controller licence — EASA Forms 152 and 156

ACTIVE SECURITY FEATURES OF LICENCES ISSUED IN ELECTRONIC FORMAT

Active security features include dedicated visual effects triggered by specific actions such as tilting the device, shaking it, or touching the screen.

Such visual effects typically cannot be replicated using images of the licence captured through a screenshot or another device.