Description pilot digitizing seafarer documents (certificate of competency) by The Netherlands

Version: 1.5

Date: 05-09-2024

Authors: Paul Ras, Arvid van der Bruggen

Contents

Introduction

Purpose of this pilot
In recent years, the options for digitally publishing personal documents, such as CoCs and CoPs, have continued to improve. Advantages of issuing digital documents are (1) a smaller chance of forgeries, (2) less production of physical documents, (3) better enforcement options and (4) a better user experience.

The goal of this pilot is to test the technical platform and the usability for (1) the holder, (2) the verifier and (3) the shipping company. There are 4 research questions defined:

1. The usability of an elicense for a holder. Does the seafarer have any advantages when using an elicense instead of a physical document?
2. The usability of an elicense for the shipping companies? Does a shipping company have any advantages when their personnel is using an elicense instead of a physical document?
3. Improvement for the enforcement options. Is an elicense accepted in other countries and does it bring any advantages while enforcing?
4. Will the introduction of an elicense solution bring new opportunities for the position of the Dutch fleet?

At the end of the pilot, the project team will create a report where these research questions will be answered.

Documents in scope:

For this pilot we include two documents in scope:

- The Certificate of Competence for Dutch seafarers; both for officers and ratings (including fishery)
- The Certificate of Competency for foreign seafarers; officers

Features in scope:

- First release;
- Extension/expand;
- Duplicate.

Duration of the pilot project
The pilot will initially run for a period of 6 months, possible to start from May 1st 2024. During the pilot, it will be evaluated from time to time whether this duration is appropriate.

Adjustments in processes
No changes to the current process are foreseen for the shipping companies that are invited to this project. The shipping company will continue to apply as is and will also continue to receive the normal physical document. Kiwa ensures that the "beneficiary (seafarer)" receives a digital certificate of competency. The beneficiary can share the digital document with the employer in a safe and standardized way, as this is standard functionality of the eLicense solution. To receive a digital document, an employer needs to implement an ISO1803-7 standardized application. Because

both a physical and digital document is provided during the pilot, we ensure that no risks are introduced with regard to continuity.

Regulation

IMO

On 28 June 2023, the IMO published guidelines for the use of electronic certificates https://puc.overheid.nl/nsi/doc/PUC_746307_14/1/ . The pilot complies with these guidelines, so that if the government decides to include the technical platform (see technical details below) of this pilot in the legal framework, the pilot fully complies with Dutch law and regulations.

EMSA

The EMSA has issued a tender to draw up the outlines of an European electronic register. The starting point is a central hub where all issued digital documents are stored and made available to the relevant authorities.

National level

During the revision of the Dutch Seafarers Act, the Ministry of Infrastructure and Water Management (I&W) removed passages from the texts that could impede the issue of digital documents. It is expected that a basis will have to be laid in legislation for the issuance of digital documents. This describes the technical specifications of the system as well the standards on which the digital document is provided. The legislation must be in line with the guidelines of IMO MSC.1/Circ.1665.

Addition 05-09-2024: The text as described above here is officially published by the Dutch government: https://zoek.officielebekendmakingen.nl/trb-2024-4.html

Issuing/re-issuing/revocation/deletion of licenses

Issuing process

Issuing of a digital license will be an addition to the current process of issuing physical licenses. This means that every seafarer who gets a digital license, will also receive a physical license.

Issuing of a digital license is done via the following steps:

1. Seafarer requests a license at the issuing authority, including email address
2. Issuing authority processes request
3. When license is granted, seafarer receives an activation code by email and physical license by mail
4. Seafarer has 7 days to install the eWallet app on a smartphone and activate the digital license in the app

The digital license will be issued based on eIDAS level “Basic” (activation code). This is in line with the current issuance of physical licenses in The Netherlands.

Revocation process

The revocation process for digital licenses will be in line with the current revocation process for physical licenses. If a license needs to be revoked, the deletion process will be used to revoke the digital license from a smartphone of the seafarer.

Deletion process

Deletion of a digital license can only be done by the issuing authority.

Deletion of a digital license is done via the following steps:

1. Issuing authority sends deletion request
2. When the seafarer opens the app/refreshes the app and the smartphone is online, the deletion request is executed and cannot be interrupted by the seafarer. Additional measures to reduce risk when the seafarer is not online are described under here

If the smartphone of the seafarer is not online, the deletion request cannot be performed. During the pilot, the following measures are put in place to reduce the risk:

1. During verification, when the smartphone of the verifier is online, the license status is received from the database of the issuing authority
2. The current process for verification of a physical license stays in place

Verification of licenses

QR code

Verification using a QR code can be performed by using an ISO18013-5 compatible app that has support for the “org.iso.23220.1.eu.europe.emsa.coc” doctype. The “Kiwa eWallet” is such an app. It supports verification in both an online and an offline scenario. Both are described in the ISO18013-5. The app is available in the respective store (Android/iOS).

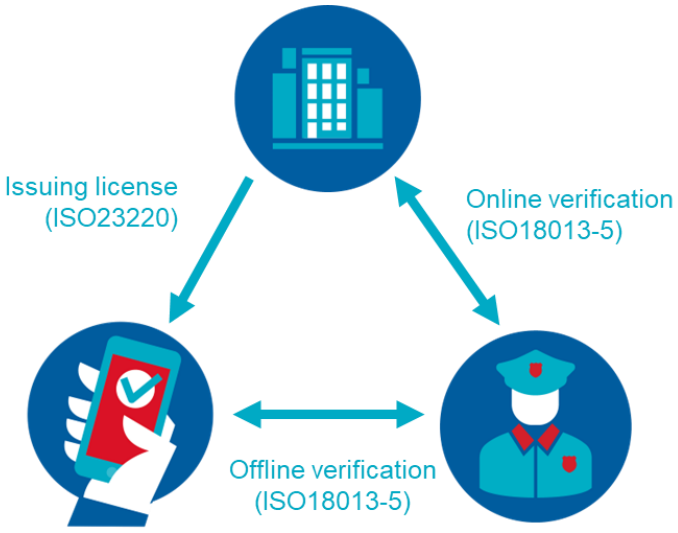

Figure 1: Overview verification steps

The seafarer will show an QR code to the verifier. The smartphone of the verifier will check whether it has an internet connection, and then choose the correct process of verification.

<u>Option 1: the smartphone of the verifier has an internet connection</u>

When the smartphone of the verifier has an internet connection, it will retrieve the latest version of the digital license from the database of the issuing authority.

<u>Option 2: the smartphone of the verifier does not have an internet connection</u>

When the smartphone of the verifier does not have an internet connection, it will verify the digital license that is on the smartphone of the holder. When doing so, it can verify the integrity and validity, but it does not know if it is the latest version of the digital license. If the verifier wants to

know if the license is the latest version, the issuing authority should be contacted using the current processes.

If both processes fail, the verifier can continue with a visual inspection.

Visual inspection

Visual inspection of a digital license can be performed on the smartphone of the seafarer. Dutch digital licenses will be issued to the “Kiwa eWallet”. An visual example of the digital license can be found in the annex of this document.

If the verifier does not trust the validity or integrity of the digital license and cannot use the QR code for verification, the standard procedures for verification of physical licenses apply.

Technical information

ISO18013-5 for verification

During the pilot, digital licenses can be verified based on an implementation of the protocol and trust framework described in the ISO18013-5[1]. For offline verification, a Bluetooth implementation of the protocol is implemented in the Kiwa eWallet.

ISO23220-3 (draft) for issuance

During the pilot, digital licenses will be issued based on an implementation of the protocol and trust framework described in the ISO23220-3 (draft)[2].

Supported devices

To issue and verify digital licenses, an eWallet is used. This is a smartphone app that supports Bluetooth and NFC and runs on the following operating systems:

- iOS (minimum current OS version -1)
- Android (minimum Android 9)

[1] ISO/IEC 18013-5:2021 - Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

[2] ISO/IEC WD TS 23220-3 - Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 3: Protocols and services for issuing phase

Datamodel

This datamodel is the first version for the mdoc created by Kiwa and it is an initial draft. There are four doctypes:

- For the Certificate of Competency name is set as “org.iso.23220.1.eu.europe.emsa.coc”
- For the Certificate of Competency - endorsment name is set as “org.iso.23220.1.eu.europe.emsa.cec”
- For the Certificate of Competency for fishery the name is set as “org.iso.23220.1.eu.europe.emsa.coc-stcw-f”.
- For the Certificate of Proficiency, the name is set as “org.iso.23220.1.eu.europe.emsa.cop”.

The datamodel for “org.iso.23220.1.eu.europe.emsa.coc”, “org.iso.23220.1.eu.europe.emsa.coc-stcw-f”, “org.iso.23220.1.eu.europe.emsa.cop” is described in the table under here.

Identifier	Meaning	Definition	Encoding format	COC
family_name	Family name	Last name, surname, or primary identifier, of the mdoc holder. The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
given_name	Given names	First name(s), other name(s), or secondary identifier, of the mdoc holder.The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
birth_date	Date of birth	Day, month and year on which the mdoc holder was born. If unknown, approximate date of birth	full-date	M
issue_date	Date of issue	Date when mdoc was issued	tdate or full-date	M
issue_place	Place of issue	Place where the document was issued	tstr	O
expiry_date	Date of expiry	Date when mdoc expires	tdate or full-date	M
issuing_country	Issuing country	Alpha-2 country code, as defined in ISO 3166-1, of the issuing authority’s country or territory	tstr	M

issuing_authority	Issuing authority	Issuing authority name. The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
issuing_authority_logo	Logo of issuing authority	A reproduction of the issuing authority logo. See 7.2.2 ISO18013-5	See 7.2.2 ISO18013-5	M
document_name	Name of the document	The name of the document that is the base of the DocType	tstr	M
document_number	Document number	The number assigned or calculated by the issuing authority. The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
portrait	Portrait of mdoc holder	A reproduction of the mdoc holder's portrait. See 7.2.2 ISO18013-5	bstr	M
capacities	Functions / Capacities / Limitations	Array of capacities of the holder	See 7.2.4 of ISO18013-5 for setup	M
capacity_code	Capacity code	Category code as per MERCHANT SHIPPING (STCW CONVENTION 2010) REGULATIONS	tstr	M
codes	Array of code info belonging to the <category> code	Array of code info	See 7.2.4 of ISO18013-5 for setup	M
code	Code as part of the array of codes	Code as per MERCHANT SHIPPING (STCW CONVENTION 2010) REGULATIONS	tstr	M
remarks	Remarks of the capacity	Remarks of the capacity in which the seafarer can work	tstr	M
family_name_issuing_officer	Familiy name issuing officer	Last name, surname, or primary identifier, of the issuing officer. The value shall only use latin1b	tstr	M

		characters and shall have a maximum length of 150 characters.		
given_name_issuing_officer	Given name issuing officer	First name(s), other name(s), or secondary identifier, of the issuing officer.The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
signature_usual_mark_issuing_officer	Image of signature issuing officer	A reproduction of the signature of the issuing officer. See 7.2.2 ISO18013-5	See 7.2.2 ISO18013-5	M
title_issuing_officer	Title of the issuing officer	The value shall only use latin1b characters and shall have a maximum length of 150 characters	tstr	M
stcw_code		Code as per MERCHANT SHIPPING (STCW CONVENTION 2010) REGULATIONS	tstr	M

M = mandatory, O = optional

The datamodel for the “org.iso.23220.1.eu.europe.emsa.cec” is described under here:

Identifier	**Meaning**	**Definition**	**Encoding format**	**CEC**
family_name	Family name	Last name, surname, or primary identifier, of the mdoc holder. The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M

given_name	Given names	First name(s), other name(s), or secondary identifier, of the mdoc holder.The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
birth_date	Date of birth	Day, month and year on which the mdoc holder was born. If unknown, approximate date of birth	full-date	M
issue_date	Date of issue	Date when mdoc was issued	tdate or full-date	M
issue_place	Place of issue	Place where the document was issued	tstr	O
expiry_date	Date of expiry	Date when mdoc expires	tdate or full-date	M
issuing_country	Issuing country	Alpha-2 country code, as defined in ISO 3166-1, of the issuing authority's country or territory	tstr	M
issuing_authority	Issuing authority	Issuing authority name. The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
issuing_country_coc	Issuing authority of the original CoC	Issuing authority name. The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
issuing_authority_logo	Logo of issuing authority	A reproduction of the issuing authority logo. See 7.2.2 ISO18013-5	See 7.2.2 ISO18013-5	M
document_name	Name of the document	The name of the document that is the base of the DocType	tstr	M

document_number	Document number	The number assigned or calculated by the issuing authority. The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
document_number_issuing_country_coc	Document number of the original CoC	The number assigned or calculated by the issuing authority. The value shall only use latin1b characters and shall have a maximum length of 150 characters.		
portrait	Portrait of mdoc holder	A reproduction of the mdoc holder's portrait. See 7.2.2 ISO18013-5	bstr	M
capacities	Functions / Capacities / Limitations	Array of capacities of the holder	See 7.2.4 of ISO18013-5 for setup	M
capacity_code	Capacity code	Category code as per MERCHANT SHIPPING (STCW CONVENTION 2010) REGULATIONS	tstr	M
codes	Array of code info belonging to the <category> code	Array of code info	See 7.2.4 of ISO18013-5 for setup	M
code	Code as part of the array of codes	Code as per MERCHANT SHIPPING (STCW CONVENTION 2010) REGULATIONS	tstr	M
remarks	Remarks of the capacity	Remarks of the capacity in which the seafarer can work	tstr	M
family_name_issuing_officer	Familiy name issuing officer	Last name, surname, or primary identifier, of the issuing officer. The value shall only use latin1b characters and shall have a maximum length of 150 characters.	tstr	M
given_name_issuing_officer	Given name issuing officer	First name(s), other name(s), or secondary	tstr	M

		identifier, of the issuing officer.The value shall only use latin1b characters and shall have a maximum length of 150 characters.		
signature_usual_mark_issuing_officer	Image of signature issuing officer	A reproduction of the signature of the issuing officer. See 7.2.2 ISO18013-5	See 7.2.2 ISO18013-5	M
title_issuing_officer	Title of the issuing officer	The value shall only use latin1b characters and shall have a maximum length of 150 characters	tstr	M
stcw_code		Code as per MERCHANT SHIPPING (STCW CONVENTION 2010) REGULATIONS	tstr	M

API for list of valid certificates

Any verification app supporting the ISO18013-5 can verify the doctype "org.iso.23220.1.eu.europe.emsa.coc" or "org.iso.23220.1.eu.europe.emsa.cop" using the datamodel described in the former chapter. The valid signing certificates of the issuing authority can be requested at "*api.digitalcertification.kiwa.com/verifier/signer-certificates*". One can request access and documentation to this API by sending an email to NL.Elicense-support@kiwa.com.

References

Annex

Example digital license