

‘Electronic EHIC/entitlement document’

Business and technical requirements

Table of Contents

1	Context.....	3
1.1	The technical proposal	3
2	Roadmap	5
3	Business requirements.....	7
3.1	Request of the electronic EHIC/entitlement document	7
3.2	Issuance of the electronic EHIC/entitlement document	7
3.3	Verification by the healthcare provider/institution in the place of stay	7
3.4	Reimbursement.....	8
3.5	Additional requirements	8
3.6	Business data definition	9
	Version 1	9
	Version 2	17
3.7	The use case	22
	High-level description and goals.....	22
	Detailed description.....	22
4	Structure of the technical part of the document.....	32
5	Logical data model for the electronic attestation	33
5.1	Version 1.0.....	33
5.2	Version 2.0.....	33
6	JSON specifications for the digital credential data model.....	34
6.1	Version 1.....	34
6.2	Version 2.....	39
7	JWT specifications, technical data model.....	46
7.1	Header.....	47
7.2	Payload	48
	Registered claims	48
	Private claims.....	49
	List of claims.....	49
	PersonName type	51
	PersonName type	52
	Serialisation and creation of the Virtual Credential payload	53
7.3	Signature	54
8	QR code specifications.....	55
8.1	QR codes as Verifiable Credentials	55
8.2	Proposed QR code.....	55

8.3	Creating the QR Code.....	56
8.4	Decoding the VC QR code	57
9	PKI (Public Key Infrastructure) - specifications of signatures used within the Verifiable Credential.....	58
9.1	PKI introduction.....	60
9.2	The EESSI Institution Repository (IR).....	60
9.3	Trust List format.....	61
9.4	Security considerations	61
9.5	Key management	63
	Certificate Issuing Authorities.....	64
	EESSI Certificate Profiles	64
	Certificate Profiles.....	64
	(Maximum) validity of a certificate.....	67
9.6	The Key Identifier (KIDs) of the Issuer.....	67
10	Federated trust landscape	69
10.1	The future vision	69
10.2	Version 1.....	69
10.3	Bridge definition.....	70
11	Format of the digital credential document	71
12	Verification APP	73
12.1	Business requirements.....	73
12.2	Validity of the VC.....	74
12.3	Verification of the QR-code.....	75
12.4	Export data interface.....	76
	Version-1	76
	Version-2.....	79
12.5	The verification process	79
12.6	Offline verification.....	80
12.7	Evolution towards the final EUDI solution	81
12.8	Authentication and access	83
	Version 1	83
	Version 2	83
12.9	How the verification app will be deployed/released?	84
12.10	Verification app visuals	84
13	Data protection and other legal considerations/requirements	85
14	Annex I – example of creation and validation of a JWT for electronic EHIC/entitlement document.....	87
14.1	Digital credential data	87
14.2	CREATION OF THE JSON	87
	Version 1	87
	Version 2	88
14.3	Creation of the JWT.....	88
	Version 1	88
	Version 2	89

15	Annex II – example of creation and validation of a PDF with QR code from JWT.....	90
15.1	Step 1 and Step 2 (a schema compliant EHIC JSON payload.)	90
15.2	Step 3: A Signed JSON Webtoken (JWS).	91
15.3	Step 4: the ZLIB compressed Payload	92
15.4	Step 5: The Identification URN added to the Payload.	92
15.5	Step 6: The BASE 45 transcoded Payload.	92
15.6	Step 6: The encoded QR Code.....	93
16	Annex III – example(s) of processes to manage the PKI	94
17	Annex IV – Governance of Identities using EESSI-IR.....	95
18	Annex V - Key Identifier algorithm	96
19	Annex VI – Possible screens of the Verification app.....	97

1 Context

This section describes the context, purpose and goals of the document and how it relates to the broader goal of digitalising the EHIC.

In accordance with its mandate (note AC 148/21REV11), the Ad-hoc group (AHG) analysed a possible way forward on the digitalisation of the EHIC, especially the feasibility and added value of a first step implementation of an electronic EHIC. Discussions with members of the DC4EU consortium were held to ensure alignment with the fully-fledged solution currently being piloted, which will build on the European Digital Identity framework.

This document details the business, legal (data protection) and technical requirements/specifications of the proposed solution, explained in the next paragraph.

Within this whole text we reference to the output document as the ‘Electronic EHIC/entitlement document’, but the Ad-hoc group has not reached an agreement on its final name.

1.1 The technical proposal

This paragraph briefly describes the basic concepts of the proposed solution.

This document proposes an intermediate implementation of the electronic EHIC/entitlement document based on the rendering of its attestation in the format of a PDF, displaying all the data in a human-readable way. Such PDF is enriched with a QR code digitally signed by the Issuer, in order that its validity (i.e. expiration date), integrity and authenticity can be proofed online and offline (i.e. without internet access) using a dedicated verification app.

The proposed solution is meant to be a first step towards a fully-fledged digitalisation of the EHIC that will be based on the European Digital identity (EUDI) wallets and will be responsible to define a comprehensive trust model.

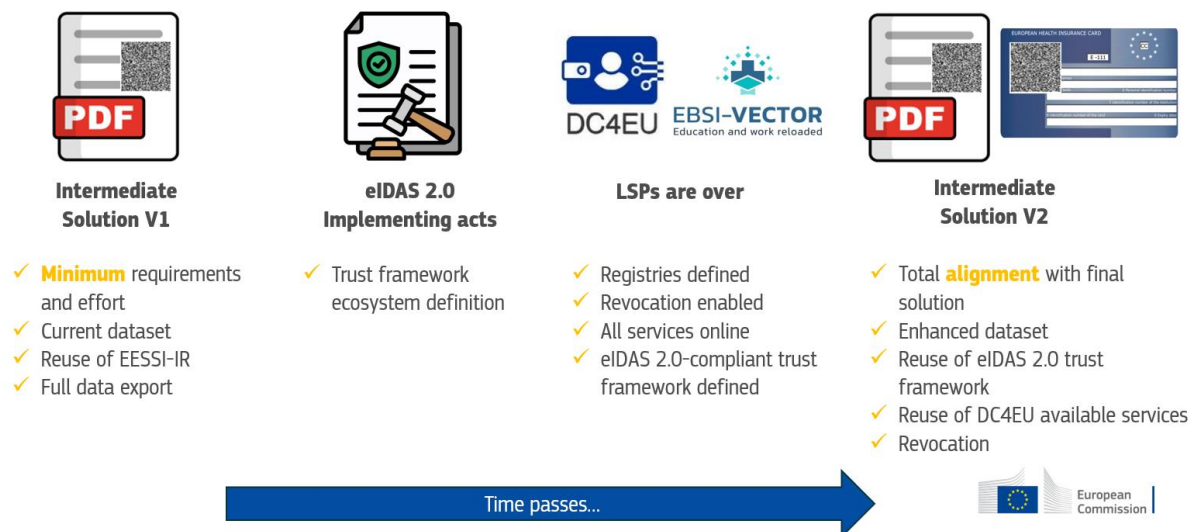
2 Roadmap

As agreed during the discussions in the Ad Hoc Group, the goal of this initiative is to define a technical solution with a **minimum set** of digital features that can provide a first added value to citizens, institutions and Health Care Providers, **as soon as possible**.

To achieve this goal, in its first release (Version 1), this solution needs to be simple, quick and as cheap as possible, focusing on the core added value, i.e. having a digital artefact and the possibility to verify its validity, authenticity and integrity.

Aspects not clearly defined in the current legislative landscape, e.g. the management of already existing trusted frameworks in the eIDAS 2.0 Regulation, or points that are still under discussion in the two pilots, e.g. the definition of trust registries for verifiers and schemas, will not be addressed with new solutions or ideas that could need to be discarded in a second moment. Nevertheless, the solution shall already foresee the possibility, in a second stage (Version 2), to improve the current document and include a set of additional digital features and enhancements that will be implemented together with the final digital EHIC based on EUDI wallets.

The figure below tries to explain the order of the theoretic definition of the Version 1 and Version 2.



*Figure 1 - Definition of the main components of the described solution.
The items do not present the time the solutions will be in place, but the order of their definition*

This approach will allow Member States to perform minimum changes and investments in this first phase and postpone the most important part of developments when adaptations for the final solution will be needed.

The 'electronic EHIC/entitlement document' defined in this document (i.e. in the form of a pdf with QR code and/or potentially as plastic card with QR code) is not in opposition to the EHIC digital solution based on the EUDI digital wallets, but represents a possible first step implementation. A solution to augment the trust of the 'physical' entitlement document (paper/card), as the one suggested here, will be needed once the solution based on the EUDI digital wallets will be in place, as not the entire population will decide to use the digital wallets, but will still have the need to obtain a verifiable proof of their social rights when travelling abroad.

In the following sections of the document we will indicate clearly which choices will be valid for the version 1 of this entitlement document and which ones will be valid for version 2 either creating two different sub-sections ("Version 1" and "Version 2"), or highlighting such information directly in text or tables.

3 Business requirements

This section describes the business requirements for an intermediate implementation of a digital EHIC, building them on top of those defined in the final report of the first ad-hoc group on the digitalisation of the EHIC (note AC 135/23). This section will focus mainly on the use case scenario and the related user journeys.

3.1 Request of the electronic EHIC/entitlement document

1. The online request of the electronic EHIC/entitlement document needs to be possible, after the proper identification of the person;
2. an automatic acknowledgment of receipt for the request needs to be provided to the requester, unless the electronic EHIC/entitlement document is available and downloadable immediately as soon as the request has been sent;
3. an electronic notification needs to be sent to the person who applied for the document when the electronic EHIC/entitlement document is available (for download), unless the electronic EHIC/entitlement document is available and downloadable immediately after the request has been sent.

3.2 Issuance of the electronic EHIC/entitlement document

1. The document needs to have an EU-common and known visual structure;
2. In addition to the data present on the material EHIC, the following minimum data need to be added:
 - a) date of issuance;
 - b) start date of validity;
3. the electronic EHIC/entitlement document shall be available for the holder on an electronic device (e.g. phone, tablet, computer);
4. the electronic EHIC/entitlement document can be downloaded anytime and anywhere by the entitled person;
5. the content of the electronic EHIC/entitlement document shall be transparent (i.e. it needs to have clear specifications on how to recognise the document as a proof on entitlement and base for the reimbursement).

3.3 Verification by the healthcare provider/institution in the place of stay

1. Possibility to check online and offline the validity, authenticity and integrity of the electronic EHIC/entitlement document;
2. need to provide information to the insured person about the result of the verification of the entitlement document;
3. possibility for the authorised users to export the electronic EHIC/entitlement document dataset and possibility to prove that this has been checked when the

document was presented (e.g. print the information, send the information as attachment to an email or other means - like NFC or Bluetooth - with the information about time (date) when information was checked, reuse the digital information for future proof in reimbursement);

4. possibility for the Verifier to display the information in a different language, when showing/verifying the electronic EHIC/entitlement document.

3.4 Reimbursement

1. The solution should allow for the data in the electronic EHIC/entitlement document to be reused in the national reimbursement systems, e.g. to be injected in the HCP and national institutions systems;
2. possibility to indicate the electronic EHIC/entitlement document number in the reimbursement process and reuse the exported data.

3.5 Additional requirements

1. Definition of a transition period for the implementation;
2. compliance with the General Data Protection Regulation (GDPR) in all steps and data processing operations;
3. inclusivity and accessibility of the solution for all stakeholders, i.e. inclusion of people who will not use the electronic solution;
4. alignment with the future EUDI framework.

3.6 Business data definition

The general rules concerning the data format defined in this paragraph aim to ensure semantic interoperability and allow uniform technical implementations for the electronic EHIC/entitlement document.

The below table lists all the fields to be included in the electronic attestation dataset (one per row).

Each row will indicate the attributes for the field:

- number of the field in the final representation of the document;
- name;
- data type;
- pattern (e.g. date-format) – if applicable;
- description, meaning, purpose;
- data range, characters, character-set;
- length – if applicable;
- min/max values – if applicable;
- mandatory/optional;
- GDPR type of data (whether it may be sensitive for GDPR);
- any reference to specifications/standards to be used for the field with related versions (e.g. ISO code for Countries) – if applicable.

Version 1

Member States using other coding in their systems compared to the ones defined here should map such codes to the described value sets. Member States are responsible for any such mappings.

Relevant decisions of the Administrative Commission will need to be updated accordingly to the foreseen changes in this section.

#	NAME	TYPE	PATTERN	DESCRIPTION	DATA RANGE	LENGTH	MIN-MAX	MANDATORY (Y/N)	GDP (Y/N)	STANDARDS
	Name and given names	Person Name (see table below for details)		Surname(s), forename(s) of the EHIC holder	(see table below for details)	(see table below for details)	//	Y	Y	(see table below for details)
5	Date of birth	Date	DD/MM/YYYY	Date of birth of the holder			m: 01/01/1900 M: 31/12/2099	Y	Y	*
6	Personal Identification number	Text		The personal identification number detail used by the issuing Member State. (In case such number does not exist, the identification number		Max = 20	//	Y	Y	ISO 8859-1 to 4 UTF-8 encoding

				of the person from whom the rights derive shall be used)					
			No full stop is used in the acronym.						
7	Name of the institution	Text	IF THERE IS the NEED TO ABBREVIATE ELEMENTS, THIS MUST BE INDICATED BY A FULL STOP	The acronym of the institution is provided instead of the full name	Max=21 **	//	Y	Y	ISO 8859-1 to 4 UTF-8 encoding
7	Identification number of the institution	Text		Identification code awarded nationally to the 'institution', viz. the competent institution of insurance	Min = 4 Max=10 **	//	Y	Y	ISO 8859-1 to 4 UTF-8 encoding
8	Card Identification number	Text		Logical identification number of the card, aiming at uniquely	Min =20 Max=20	//	Y		EN 1867 from 1997

				identifying the card and assigned to each card by the card issuer				
1	Card Issuer Country	Country code		Identification code of the country having issued the EHIC	See dedicated list in following section	//	Y	ISO 3166-1 (2-letter code)
				Start date of the validity of this credential.		m: 01/01/1900		
10	Start date of validity	Date	DD/MM/YYYY	This date needs to be used to check whether the holder could benefit from healthcare		M: 31/12/2099	Y	*
				End date of the validity of this entitlement		m: 01/01/1900		
9	Expiry date	Date	DD/MM/YYYY			M: 31/12/2099	Y	*

11	Date of issuance	Date	DD/MM/YYYY	Date when this credential was issued	m: 01/01/1900 M: 31/12/2099	Y	*
----	------------------	------	------------	--------------------------------------	--------------------------------------	---	---

* Despite it is not following any standard, the AHG decided to keep dates in this format for the first version of this electronic entitlement document

** The maximum sum of the length of the two field is 25 characters

PersonName data type definition

#	NAME	TYPE	PATTERN	DESCRIPTION	DATA RANGE	LENGTH	MIN-MAX	MANDATORY (Y/N)	GDPR (Y/N)	STANDARDS
3	Surname	Text	If there is the need to abbreviate elements, this must be indicated by a full stop	The surname or primary name(s) of the person addressed in the digital credential. The surname field may include titles, prefix or any other name supplement or prefix		Max = 40	//	Y	Y	ISO 8859-1 to 4 UTF-8 encoding
4	Forename	Text	If there is the need to abbreviate elements, this must be indicated	The forename(s) of the person addressed in the digital credential		Max = 35	//	Y	Y	ISO 8859-1 to 4 UTF-8 encoding

by a full
stop.

Country Code possible values

Here follows the list of the possible values:

"AT", "BE", "BG", "CY", "CZ", "DE", "DK", "EE", "EL", "ES", "FI", "FR", "HR", "HU", "IE", "IS", "IT", "LI", "LT", "LU", "LV", "MT", "NL", "NO", "PL", "PT", "RO", "SI", "SK", "SE", "CH", "UK".

Order and numbering of fields

Following the practice currently used in the plastic version of the EHIC, each field gets a unique number, which is displayed next to its label. Currently the range of fields number is from 3 to 9. Field 1 is the Issuer nationality and 2 is a disused field (which was included for the former form-identifier).

If we wish to keep the numbering of the fields, our suggestion is to keep it as it is for the moment, adding “10” and “11” for the two new fields (“Start date of validity” and “Issuance date”), and then restarting the numbering from “1” in the Version 2 of the PDF, else such numbering can be dismissed.

In the former option, it could be possible to provide in the second page of the PDF a human readable translation of all the labels in all the languages foreseen for the EHIC.

Business rules for dates

The following business rules shall be applied for dates fields above:

- Start date of validity \geq Date of birth
- Date of issuance \geq Start date of validity
- Expiry date \geq Date of issuance

Version 2

Not mentioned fields or rules are subject to no changes compared to Version 1. Changes are highlighted in yellow.

#	NAME	TYPE	PATTERN	DESCRIPTION	DATA RANGE	LENGTH	MIN-MAX	MANDATORY (Y/N)	GDPR (Y/N)	STANDARDS
	Name and given names	Person Name <i>(see table below for details)</i>		Surname(s), forename(s) of the EHIC holder both in generic charset and in machine readable travel documents standard	<i>(see table below for details)</i>	<i>(see table below for details)</i>	//	Y	Y	<i>(see table below for details)</i>
3	Date of birth	Date	YYYY-MM-DD	Date of birth of the holder			m: 1900-01-01 M: 2099-12-31	Y	Y	ISO 8601 date format
6	Card Identification number	Text	See dedicated paragraph Card identification	Logical identification number of the card, aiming at uniquely identifying the card and assigned to each		Min =20 Max=20	//	Y		ISO 8859-1 to 4 UTF-8 encoding

			n number, below the table	card by the card issuer			
8	Start date of validity	Date	YYYY-MM-DD	Start date of the entitlement to receive health care during a temporary stay in a Member State other than the insuring Member State	m: 01/01/1900 M: 31/12/2099	Y	ISO 8601 date format
7	Expiry date	Date	YYYY-MM-DD	End date of the validity of this entitlement	m: 01/01/1900 M: 31/12/2099	Y	ISO 8601 date format
9	Date of issuance	Date	YYYY-MM-DD	Date when the credential was issued	m: 01/01/1900 M: 31/12/2099	Y	ISO 8601 date format

Some MSs were wondering whether a field for the holder's gender should be added in version 2, as it is one of the mandatory attributes to be provided for SED S080 for the reimbursement process.

PersonName data type definition

Compared to Version 1, the Version 2 will increase the size of Name and Surname fields to accommodate the needs of some Member States. The new size still needs to be defined.

It could also be considered to have a dedicated field for titles or any other name supplement or prefix, in order not to pollute the surname field.

Moreover, there was a suggestion not to limit the character-set just to the current subset of Latin extensions, but to include all the Latin extensions and also Greek and Cyrillic characters. The discussion is left open, but the digitalisation is a great opportunity to deal with such a need from some Member States.

To make the name and surname always readable by any European citizen, even in a different country, using a different set of characters, there is the idea to add two new fields, containing the standardisation of name and surname in ISO/IEC 7501-1, as it happens currently with passports.

Open points for discussions are highlighted in yellow.

#	NAME	TYPE	PATTERN	DESCRIPTION	DATA RANGE	LENGTH	MIN - MAX	MANDATORY (Y/N)	GDPR (Y/N)	STANDARDS
1	Surname	Text		The surname or primary name(s) of the person addressed in the digital credential		Max = XX	//	Y	Y	Unicode (Latin script, Greek script, Cyrillic script, European Latin script extensions) UTF-8 encoding

1B	Standardised surname	Text	The surname(s) of the person, transliterated to ICAO 9303, i.e. ISO/IEC 7501-1	Max = XX	//	Y	Y	ICAO 9303, i.e. ISO/IEC 7501-1
2	Forename	Text	The forename(s) of the person addressed in the digital credential	Max = YY	//	Y	Y	Unicode (Latin script, Greek script, Cyrillic script, European Latin script extensions) UTF-8 encoding
2B	Standardised forename	Text	The forename(s) of the person, transliterated to ICAO 9303, i.e. ISO/IEC 7501-1	Max = YY	//	Y	Y	ICAO 9303, i.e. ISO/IEC 7501-1

Business rules for dates

Further additional controls on dates can be suggested by Member States for the Version 2, based on their national rules. Additional constraints could also be envisaged for the dates range.

Card identification number

The card identification number shall follow a common structure and format easing human- and/or machine-interpretability of information and may relate to elements such as the Issuing Institution.

A suggested solution to modify it for the version 2 is reported below, to increase the security of the card. A cost/benefit analysis is still needed, to understand whether it could be a useful improvement.

The following metrics can be defined:

- *Modularity* - the degree to which the code is composed of distinct building blocks that contain semantically different information;
- *Human-interpretability* - the degree to which the code is meaningful, or can be interpreted by the human reader;
- *Globally unique* - the Country or Authority identifier is well-managed, and each country (authority) is expected to properly manage its segment of the namespace by never recycling or re-issuing identifiers. The combination of this ensures that each identifier is globally unique.

Pattern rules:

- a) *First part* - 10 characters that identify the card issuer, and in compliance with the standard EN 1867:1997;
- b) *Second part* - 8 characters constituting of a unique card identifier per Issuer;
- c) *Code suffix/Checksum* - The checksum must not be relied upon for validating the card and is not technically part of the identifier, but is used to verify the integrity of the Card Identification Number. This checksum should follow the ISO-7812-1 (LUHN-10)¹ summary of the entire UCI in digital/wire transport format.

Backwards-compatibility should be ensured: Member States that over time change the structure of their identifiers must ensure that any two identifiers that are identical represent the same entitlement document. Or, in other words, Member States cannot recycle identifiers.

This logical card ID number must enable the information carried by the card to be checked against the information held by the issuing organisation for the same logical number, for example to reduce the risk of fraud, or to identify errors in data entry when processing the information of the card for claim reimbursement purposes.

¹ The Luhn mod N algorithm is an extension to the Luhn algorithm (also known as mod 10 algorithm), which works for numeric codes and is used for example for calculating the checksum of credit cards. The extension allows the algorithm to work with sequences of values in any base (in our case alpha characters).

3.7 The use case

The following use case illustrates the 'journey' of a citizen needing to access unplanned necessary healthcare abroad and the necessary processes or IT tools supporting the introduction of an electronic EHIC/entitlement document.

High-level description and goals

An insured person needs to access medically necessary, state-provided, healthcare during a temporary stay in any of the 27 EU countries, Iceland, Liechtenstein, Norway and Switzerland or the United Kingdom. In order to be treated under the conditions of the EU social security coordination rules, the person needs to prove to the healthcare provider that s/he is insured in another Member State (i.e. the competent Member State).

The goals of "Accessing unplanned necessary healthcare abroad" use case are:

- for insured persons, to be able to prove their entitlement to unplanned necessary healthcare abroad in a reliable and simple manner;
- for healthcare providers, to be able to verify the authenticity, integrity and validity of the person's entitlement document;
- for institutions at the place of temporary stay of the insured person and the competent institutions responsible for reimbursement of healthcare costs, to reduce doubts about the insured persons' entitlement to sickness benefit in individual cases, to speed up reimbursement of the costs incurred and reduce the administrative burden.

Detailed description

Current procedure for accessing unplanned healthcare abroad

The EU social security coordination Regulations² ensure that insured persons temporarily staying in a Member State other than the one competent for their sickness coverage (health insurance) are entitled to sickness benefits in kind which become necessary on medical grounds during their stay, considering the nature of the benefits and the expected length of stay (Article 19 of Regulation (EC) No 883/2004). The benefits should be provided on the same terms and at the same costs as those applicable to persons insured under the legislation of the country of stay. Following

² Regulation (EC) No 883/2004 on the coordination of social security systems and Regulation (EC) No 987/2009 laying down the procedure for implementing Regulation (EC) No 883/2004. These Regulations also apply to Norway, Iceland, Liechtenstein and Switzerland. Specific rules are in place in the agreements with the United Kingdom.

the provision of healthcare services, the cost will be reimbursed by the competent Member State to the Member State of stay.

The procedure to follow to access unplanned necessary care abroad is set out in Article 25 of Regulation (EC) No 987/2009. To receive benefits in kind in the Member State of stay, the insured person needs to present to the healthcare provider in the Member State of stay a document issued by the competent Member State indicating the insured person's entitlement to sickness benefits in kind. This document is the European Health Insurance Card (EHIC). The issuing process of the EHIC varies significantly across countries and in some of them the EHIC is automatically issued to all insured people. The EHIC is either a standalone card or integrated in a national health insurance card. Therefore, steps may differ from Country to Country.

If the insured person does not have such a document, s/he or the Member State of stay via its institution should contact the competent Member State to obtain a Provisional Replacement Certificate (PRC) of the EHIC. This contact can either be between the person and the home country (e.g. by phone, email), or between the Member States through the Electronic Exchange of Social Security Information (EESSI) system.

If the insured person has actually borne the costs of all or part of the benefits in kind provided and if the legislation applied by the institution of the place of stay enables reimbursement of those costs to an insured person, he may request reimbursement to the institution of the place of stay. If the person did not have to pay for the treatment, the reimbursement of the costs will take place between the Member States (via dedicated message exchanges through EESSI).

In case the person could not present an EHIC nor a PRC when the treatment is provided, or if there are doubts about the validity of such document, the healthcare provider will charge the full cost of the treatment. After having returned home, the insured person can request reimbursement from their competent institution.



Accessing unplanned necessary healthcare abroad

Before the travel

Context: a person plans to travel abroad for a temporary stay in another Member State and requests the EHIC

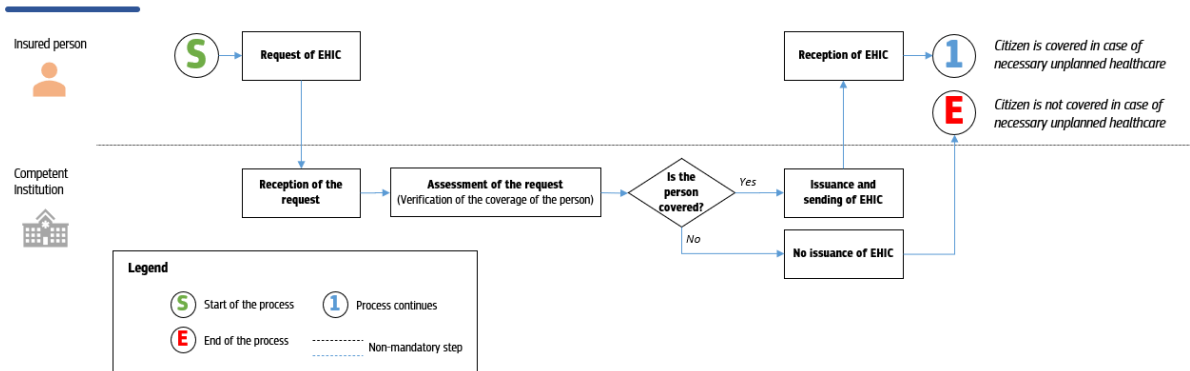


Figure 2 - As-is - Workflow before the travel



Accessing unplanned necessary healthcare abroad

During the person's stay abroad

Context: a person travels abroad for a temporary stay in another Member State and requires necessary healthcare treatment

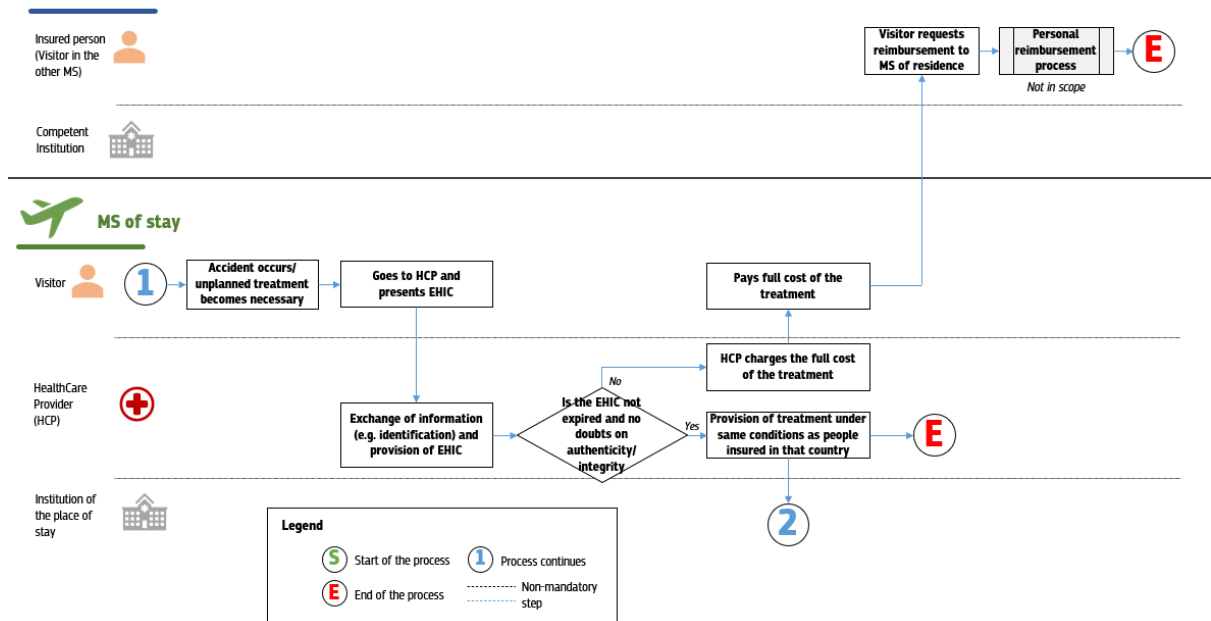


Figure 3 - As-is - Workflow during the person's stay abroad



Accessing unplanned necessary healthcare abroad

After the treatment

Context: a person travels abroad for a temporary stay in another Member State and gets unplanned healthcare



Competent MS

Insured person
(Visitor in
other MS)

Competent
Institution



MS of stay

Visitor

HealthCare
Provider
HCP

Institution of the
place of stay /
Liaison body of the
place of stay

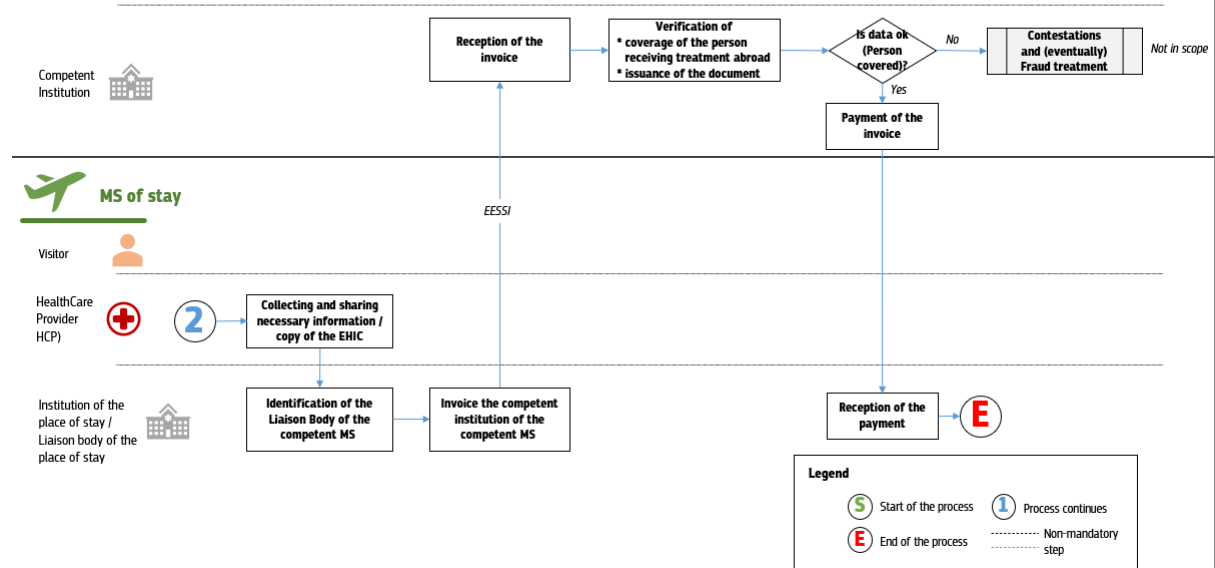


Figure 4 - As-is - Workflow after the treatment

'To-be' user journey for a possible intermediate implementation of the digital EHIC

The user journey described here below is meant to provide a high-level explanation of the interactions among the various actors involved in the process of requesting, issuing, sharing and verifying the 'electronic EHIC/entitlement document'. Steps may differ from Country to Country.

Main actors and their roles

Actor	Description
Insured person	The person seeking unplanned necessary healthcare (sickness benefits in kind) during a temporary stay in a Member State other than the one competent for his or her healthcare coverage.
Competent Member State	The Member State where the person has health insurance or is covered by the public healthcare scheme.
Competent institution	The institution responsible for the healthcare costs of the person at the time of the application for benefit.
Institution issuing the 'electronic EHIC/entitlement document'	The health insurance institution designated to issue the 'electronic EHIC/entitlement document' in the competent Member State.
Member State of stay	The Member State where the insured person is seeking unplanned necessary healthcare.
Healthcare provider or other authorised verifiers	The doctor, hospital, or any other type of healthcare provider which is providing the sickness benefits under the public healthcare scheme of the Member State of temporary stay.
Liaison bodies of the Member States involved	The bodies in the Member States responsible for the reimbursement process

Steps

- A person plans to travel abroad for a temporary stay in another Member State (regardless of the purpose of the travel, e.g. for work, holiday, studies).
- The person requests online or offline the 'electronic EHIC/entitlement document' from his/her health insurance institution. To do that, s/he can either access directly the institution's portal or visit the [Your Europe website](#), which will redirect her/him to that portal³; else the citizen can also go to a physical desk. The EHIC proves that the issuing Member State is responsible for the healthcare costs of the person is insured in the issuing Member State, therefore, is entitled to benefits in kind, which become necessary on medical grounds during a temporary stay abroad.
- The health insurance institution of the competent Member State checks the request and decides on the issuance of the 'electronic EHIC/entitlement document':
 - an acknowledgment of receipt of the request is sent to the requester, if the document is not issued automatically once the request is sent;
 - in case the document is not issued once the request is sent, a notification is delivered to the requester as soon as the document is available;
 - the document is issued in a pdf format, enriched by an electronically readable and digitally signed QR-code, and shared with the requester;
 - a communication is sent to the person in case of refusal to issue the document, with an explanation for the denial (according to national rules).
- When the person is abroad and seeks unplanned necessary care, s/he shows the 'electronic EHIC/entitlement document' stored in her/his smartphone to the healthcare provider. A printed copy may also be presented, if the person does not want/cannot provide the electronic version, without any change in the verification process.
- The healthcare provider automatically checks (online or, if needed, offline), via a verification app, the validity of the 'electronic EHIC/entitlement document' and whether the document has been issued by the competent institution and it has not been tampered. Revocation feature is not taken in consideration for this first step towards the digitalisation of the EHIC.
- The healthcare provider downloads a proof that the 'electronic EHIC/entitlement document' has been controlled, together with a date and the result of the control.

³ In those countries where the EHIC is issued automatically and/or it integrated in/provided on the back of the national cards, persons should be able to request/get an 'electronic EHIC/entitlement document'.

- The healthcare provider downloads a copy of the 'electronic EHIC/entitlement document' data in the form it prefers (human readable or machine readable) to be kept/reused for the reimbursement phase.
- The insured person receives the unplanned necessary healthcare treatment under the same conditions as people insured in the Member State of stay.
- The healthcare provider forwards the reimbursement request to the institution in its own Member State (Member State of stay) and receives reimbursement according to national rules. The healthcare provider will include in the reimbursement request the exported data/digital copy of the 'electronic EHIC/entitlement document'.
- The Member State of stay (via its liaison body) requests reimbursement from the competent Member State in accordance with the reimbursement rules set out in Regulations 883/2004 and 987/2009. This reimbursement request is sent to the Liaison Body of the competent Member State through EESSI.
- The competent member States reimburses the cost of treatment to the Member State of stay.



Accessing unplanned necessary healthcare abroad

Before the travel



Competent MS

Context: a person **not using digital wallets** plans to travel abroad for a temporary stay in another Member State and request the electronic entitlement

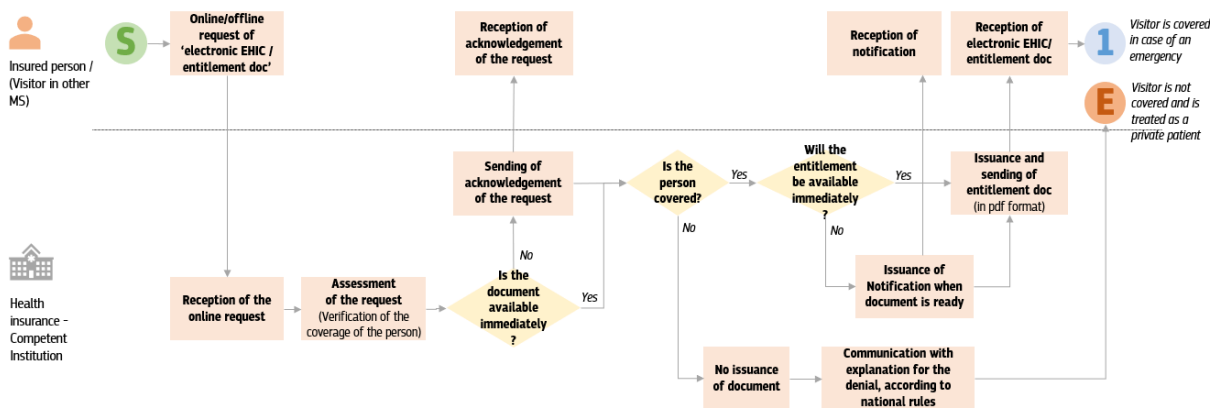


Figure 5 - To-be - Workflow before the travel



Accessing unplanned necessary healthcare abroad

During the person's stay abroad

Context: a person **not using digital wallets** is abroad and needs access to unplanned healthcare

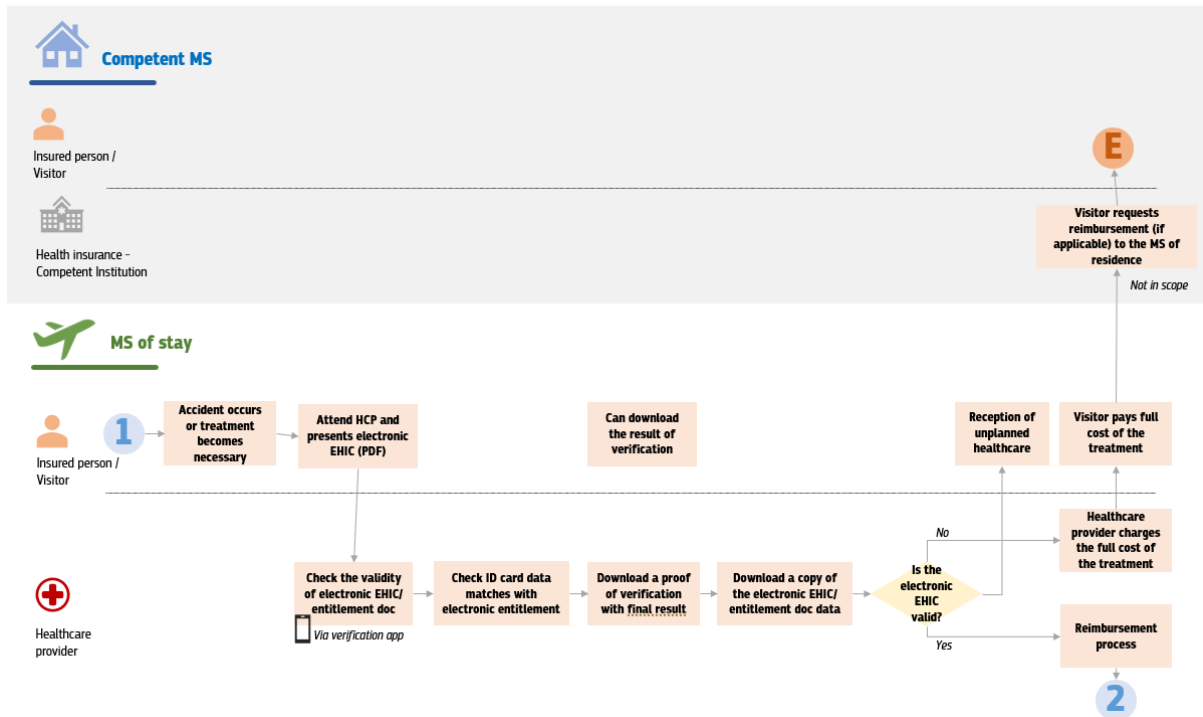


Figure 6 - To-be - Workflow during the person's stay abroad



Accessing unplanned necessary healthcare abroad

After treatment

Context: The provision of the healthcare gives rise to a reimbursement request

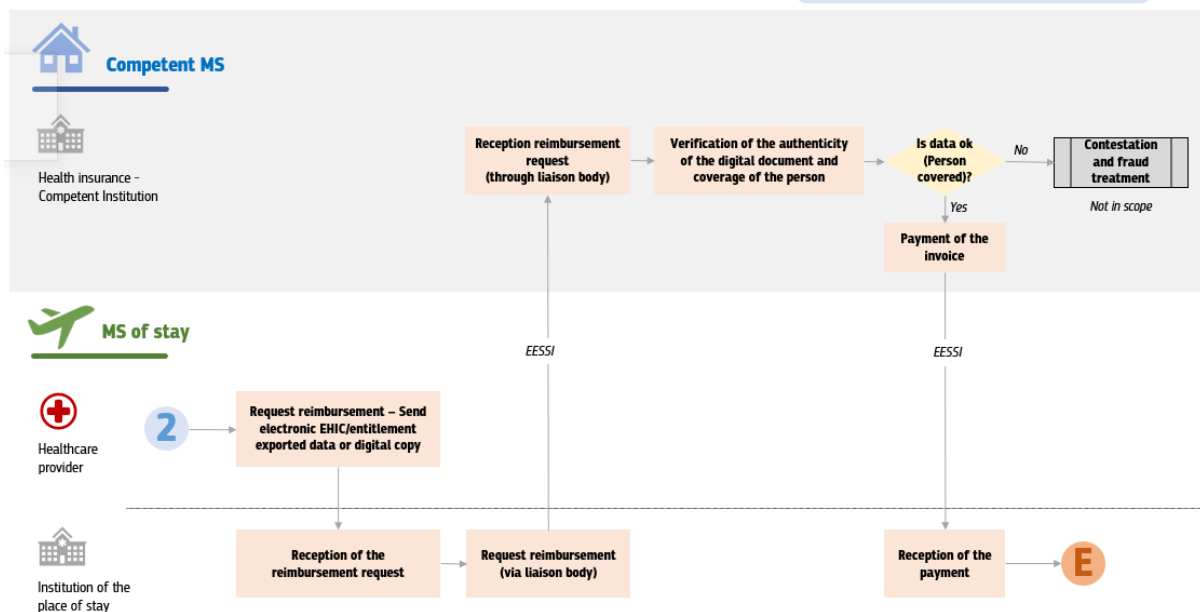


Figure 7 - To-be - Workflow after treatment

Verification app workflows

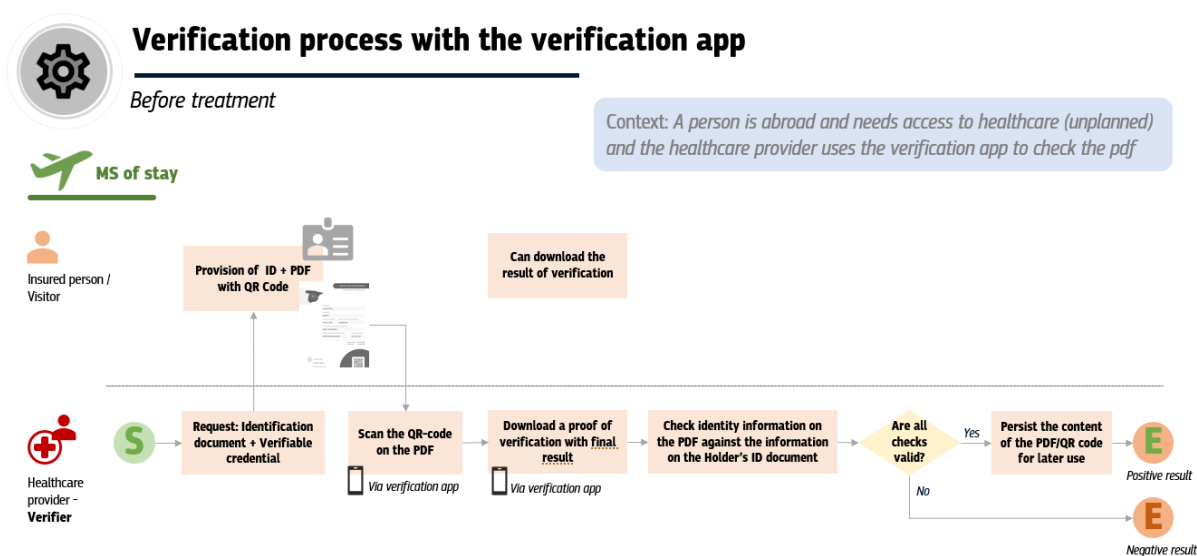
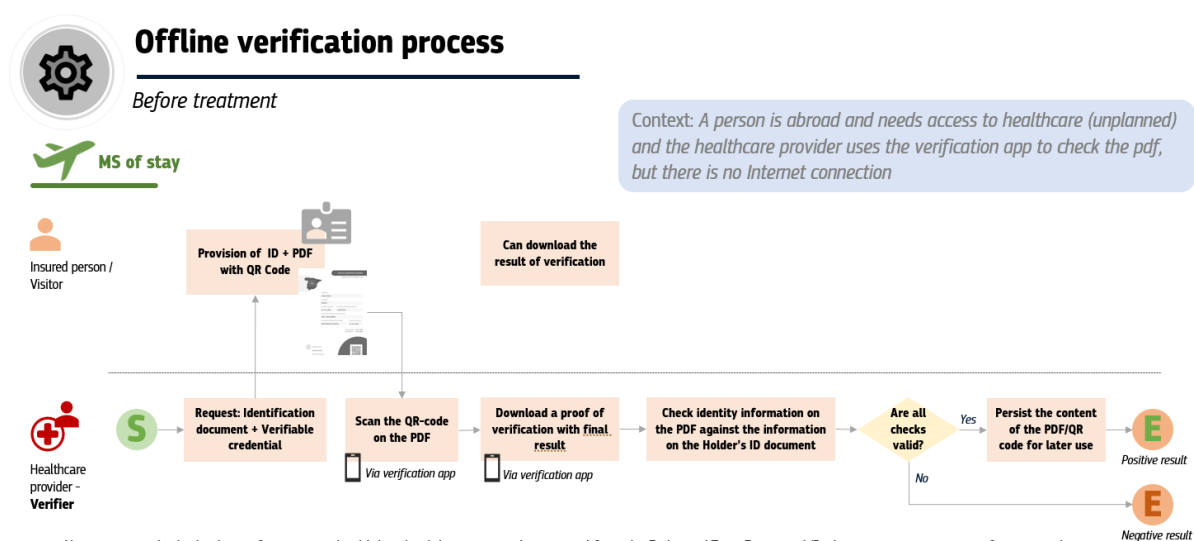


Figure 8 - To-be - Workflow for verification of the digital entitlement using the app (online)



Note: as a standard rule, the verification app should download the cryptographic material from the Federated Trust Framework/Bridge service upon every verification made. However, this approach would require an active internet connection to carry out the full verification process.

To overcome this problem, the verification app may download the necessary cryptographic material (snapshot) at regular intervals, e.g. every night, and store it locally in a cache. This would allow the verification app to work completely in offline mode, if internet connection is not available, including when checking the trustworthiness of the issuer's digital certificate.

Figure 9 - To-be - Workflow for verification of the digital entitlement using the app (offline – no internet)



Manual verification process

Before treatment



MS of stay



Insured person /
Visitor



HealthCare
Provider -
Verifier

Context: A person is abroad and needs access to healthcare (unplanned) the HCP does not want to use the verification app and proceeds with a manual check of the pdf – **This path is not recommended**

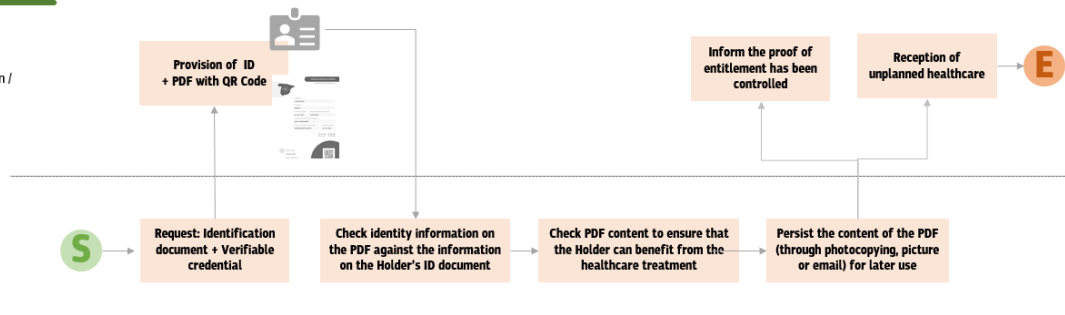


Figure 10 - To-be - Workflow for "manual" verification of the digital entitlement (not recommended)

4 Structure of the technical part of the document

This section explains how the following technical part of document is structured, i.e. following the logical steps to build the final outcome, i.e. the pdf with the QR code.

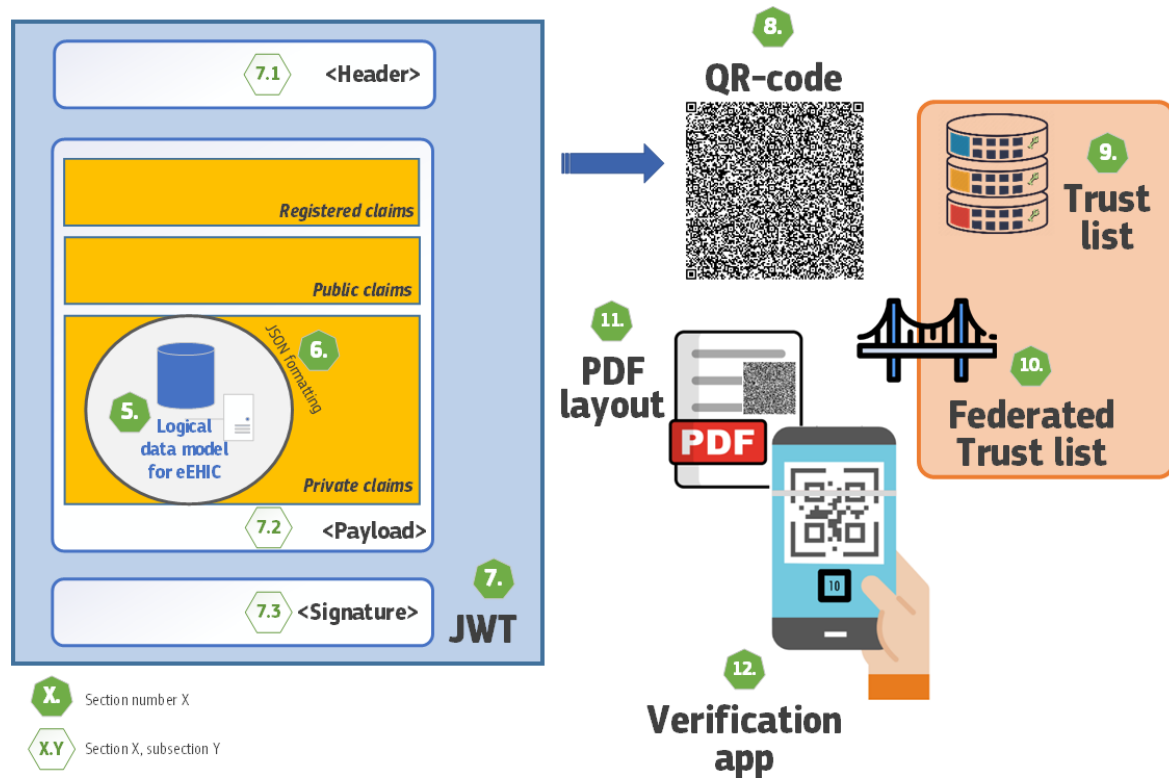


Figure 11 - Main components of the proposed solution and dedicated sections of the document where they are described

5 Logical data model for the electronic attestation

This section lists and details all the business data to be included in the digital credential under a business point of view (details for the business data available in 0 -

Business data [definition](#)).

5.1 Version 1.0

The data structure and formats are kept as similar as possible to the current physical EHIC, to require minimum changes and effort to have a digital version of the entitlement as soon as possible.

5.2 Version 2.0

The data structure and formats are updated to be aligned with the final digitalisation based on EUDI wallets and to exploit to the maximum the opportunity of the digitalisation of the entitlement.



Figure 12 - Data model schema

6 JSON specifications for the digital credential data model

This section defines the digital credential data model (defined in section above) as a JSON Schema, the supported versions and standards.

The ability to read and interpret Electronic Attestations, issued by any issuer, requires a common data structure and agreement on the significance of each data field of the payload. To facilitate such interoperability, a common coordinated data structure is defined using a 'JSON' schema that constitutes the framing of this Entitlement document.

6.1 Version 1

The JSON file is available in the Ad-hoc group Teams repository.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "$id": "ehic-schema.json",
  "title": "electronic EHIC/entitlement document",
  "description": "Data Type for the electronic EHIC/entitlement document",
  "type": "object",
  "allOf": [
    {
      "properties": {
        "hn": {
          "title": "Name and given names",
          "description": "Surname(s), forename(s) of the EHIC holder both
            in generic charset and in machine readable travel
            documents standard",
          "$ref": "#/$defs/person_name"
        },
        "dob": {
          "title": "Date of birth",
          "description": "Date of Birth of the holder",
          "type": "string",
          "pattern": "^(29[/-]02[/-]
            ]((19|20)([2468][048]|[13579][26]|0[48])|2000)|((0[1-
            9]|12)[0-9]|30)[/-(0[469]|11)[/-(19|20)[0-9]{2}|(0[1-
            9]|12)[0-9]|3[01])[/-(0[13578]|1[02])[/-(19|20)[0-
            9]{2}|(0[1-9]|1[0-9]|2[0-8])[/-]02[/-(19|20)[0-9]{2}))$"
        },
        "hi": {
          "title": "Personal Identification number",
          "description": "The personal identification number detail used by
            the issuing Member State. (In case such number does not
            exist, the identification number of the person from whom
            the rights derive shall be used)",
          "type": "string",
          "maxLength": 20
        },
        "ii": {
          "title": "Identification number of the institution",
          "description": "Identification code awarded nationally to the
            'institution', viz. the competent institution of
            insurance",
          "type": "string",
          "minLength": 4,
          "maxLength": 10
        },
        "in": {
```

```

        "title": "Name of the institution",
        "description": "The acronym of the institution is provided
                        instead of the full name",
        "type": "string",
        "maxLength": 21
    },
    "ci": {
        "title": "Card Identification number",
        "description": "Logical identification number of the card",
        "type": "string",
        "minLength": 20,
        "maxLength": 20
    },
    "ic": {
        "title": "Card Issuer Country",
        "description": "Identification code of the country having issued
                        the EHIC",
        "type": "string",
        "$ref": "#/$defs/countryCode"
    },
    "sd": {
        "title": "Entitlement Start date",
        "description": "Start date of the entitlement to receive health
                        care during a temporary stay in a Member State other than
                        the insuring Member State",
        "type": "string",
        "pattern": "^(29[/-]02[/-
                        ]((19|20)([2468][048]|[13579][26]|0[48])|2000)|((0[1-
                        9]|12)[0-9]|30)[/-(0[469]|11)[/-(19|20)[0-9]{2}|(0[1-
                        9]|12)[0-9]|3[01])[/-(0[13578]|1[02])[/-(19|20)[0-
                        9]{2}|(0[1-9]|1[0-9]|2[0-8])[/-]02[/-(19|20)[0-9]{2}))$"
    },
    "ed": {
        "title": "Expiry date",
        "description": "End date of the validity of the card",
        "type": "string",
        "pattern": "^(29[/-]02[/-
                        ]((19|20)([2468][048]|[13579][26]|0[48])|2000)|((0[1-
                        9]|12)[0-9]|30)[/-(0[469]|11)[/-(19|20)[0-9]{2}|(0[1-
                        9]|12)[0-9]|3[01])[/-(0[13578]|1[02])[/-(19|20)[0-
                        9]{2}|(0[1-9]|1[0-9]|2[0-8])[/-]02[/-(19|20)[0-9]{2}))$"
    },
    "id": {
        "title": "Date of issuance",
        "description": "Date when the document was issued",
        "type": "string",
        "pattern": "^(29[/-]02[/-
                        ]((19|20)([2468][048]|[13579][26]|0[48])|2000)|((0[1-
                        9]|12)[0-9]|30)[/-(0[469]|11)[/-(19|20)[0-9]{2}|(0[1-
                        9]|12)[0-9]|3[01])[/-(0[13578]|1[02])[/-(19|20)[0-
                        9]{2}|(0[1-9]|1[0-9]|2[0-8])[/-]02[/-(19|20)[0-9]{2}))$"
    }
},
"required": [
    "ic",
    "hn",
    "dob",

```

```

        "hi",
        "ii",
        "in",
        "ci",
        "sd",
        "ed",
        "id"
    ]
},
{
    "description": "Contraint that the combined length of the
                    'Identification number of institution' and the 'Name of
                    the institution' fields must not exceed 25 characters",
    "anyOf": [
        {
            "properties": {
                "ii": {
                    "maxLength": 10
                },
                "in": {
                    "maxLength": 15
                }
            }
        },
        {
            "properties": {
                "ii": {
                    "maxLength": 9
                },
                "in": {
                    "maxLength": 16
                }
            }
        },
        {
            "properties": {
                "ii": {
                    "maxLength": 8
                },
                "in": {
                    "maxLength": 17
                }
            }
        },
        {
            "properties": {
                "ii": {
                    "maxLength": 7
                },
                "in": {
                    "maxLength": 18
                }
            }
        },
        {
            "properties": {
                "ii": {

```

```

        "maxLength": 6
      },
      "in": {
        "maxLength": 19
      }
    },
    {
      "properties": {
        "ii": {
          "maxLength": 5
        },
        "in": {
          "maxLength": 20
        }
      }
    },
    {
      "properties": {
        "ii": {
          "maxLength": 4
        },
        "in": {
          "maxLength": 21
        }
      }
    }
  ]
},
"$defs": {
  "person_name": {
    "description": "Person name: The person's name consisting of a
      separate surname and a forename",
    "type": "object",
    "properties": {
      "fn": {
        "title": "Surname",
        "description": "The surname or primary name(s) of the person
          addressed in the EHIC",
        "type": "string",
        "maxLength": 40,
        "examples": [
          "d'Červenková Panklová"
        ]
      },
      "gn": {
        "title": "Forename",
        "description": "The forename(s) of the person addressed in the
          EHIC",
        "type": "string",
        "maxLength": 35,
        "examples": [
          "Jiřina-Maria Alena"
        ]
      }
    }
  }
},

```

```

    "required": [
      "fn",
      "gn"
    ]
  },
  "countryCode": {
    "title": "Country Code",
    "description": "Identification code of the country (2 digit ISO
                    country code (ISO 3166-1)), with the addition of UK for
                    GB",
    "enum": [
      "AT",
      "BE",
      "BG",
      "HR",
      "CY",
      "CZ",
      "DK",
      "EE",
      "FI",
      "FR",
      "DE",
      "EL",
      "HU",
      "IS",
      "IE",
      "IT",
      "LV",
      "LI",
      "LT",
      "LU",
      "MT",
      "NL",
      "NO",
      "PL",
      "PT",
      "RO",
      "SK",
      "SI",
      "ES",
      "SE",
      "CH",
      "UK"
    ]
  }
}

```

6.2 Version 2

The JSON file is available in the Ad-hoc group Teams repository .

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "$id": "ehic-schema.json",

```

```
"title": "electronic EHIC/entitlement document",
"description": "Data Type for the electronic EHIC/entitlement document",
"type": "object",
"allOf": [
  {
    "properties": {
      "hn": {
        "title": "Name and given names",
        "description": "Surname(s), forename(s) of the EHIC holder both in
          generic charset and in machine readable travel documents
          standard",
        "$ref": "#/$defs/person_name"
      },
      "dob": {
        "title": "Date of birth",
        "description": "Date of birth of the holder",
        "type": "string",
        "pattern": "^(19|20)\\d\\d(-\\d\\d){2}$",
        "format": "date"
      },
      "hi": {
        "title": "Personal Identification number",
        "description": "The personal identification number detail used by
          the issuing Member State. (In case such number does not exist,
          the identification number of the person from whom the rights
          derive shall be used)",
        "type": "string",
        "maxLength": 20
      },
      "ii": {
        "title": "Identification number of the institution",
        "description": "Identification code awarded nationally to the
          'institution', viz. the competent institution of insurance",
        "type": "string",
        "minLength": 4,
        "maxLength": 10
      },
      "in": {
        "title": "Name of the institution",
        "description": "The acronym of the institution is provided instead
          of the full name",
        "type": "string",
        "maxLength": 21
      }
    }
  }
]
```



```
    },
    "ci": {
      "title": "Card Identification number",
      "description": "Logical identification number of the card",
      "type": "string",
      "minLength": 20,
      "maxLength": 20
    },
    "ic": {
      "title": "Card Issuer Country",
      "description": "Identification code of the country having issued  
the EHIC",
      "type": "string",
      "$ref": "#/$defs/countryCode"
    },
    "sd": {
      "title": "Entitlement Start date",
      "description": "Start date of the entitlement to receive health  
care during a temporary stay in a Member State other than the  
insuring Member State",
      "type": "string",
      "pattern": "^(19|20)\\d\\d(-\\d\\d){2}$",
      "format": "date"
    },
    "ed": {
      "title": "Expiry date",
      "description": "End date of the validity of the card",
      "type": "string",
      "pattern": "^(19|20)\\d\\d(-\\d\\d){2}$",
      "format": "date"
    },
    "id": {
      "title": "Date of Issuance",
      "description": "Date when the document was issued",
      "type": "string",
      "pattern": "^(19|20)\\d\\d(-\\d\\d){2}$",
      "format": "date"
    }
  },
  "required": [
    "ic",
    "hn",
    "dob",
```

```
        "hi",
        "ii",
        "in",
        "ci",
        "sd",
        "ed",
        "id"
    ]
},
{
    "description": "Constraint that the combined length of the
        'Identification number of institution' and the 'Name of the
        institution' fields must not exceed 25 characters",
    "anyOf": [
        {
            "properties": {
                "ii": {
                    "maxLength": 10
                },
                "in": {
                    "maxLength": 15
                }
            }
        },
        {
            "properties": {
                "ii": {
                    "maxLength": 9
                },
                "in": {
                    "maxLength": 16
                }
            }
        },
        {
            "properties": {
                "ii": {
                    "maxLength": 8
                },
                "in": {
                    "maxLength": 17
                }
            }
        }
    ]
}
```

```
    },
    {
      "properties": {
        "ii": {
          "maxLength": 7
        },
        "in": {
          "maxLength": 18
        }
      }
    },
    {
      "properties": {
        "ii": {
          "maxLength": 6
        },
        "in": {
          "maxLength": 19
        }
      }
    },
    {
      "properties": {
        "ii": {
          "maxLength": 5
        },
        "in": {
          "maxLength": 20
        }
      }
    },
    {
      "properties": {
        "ii": {
          "maxLength": 4
        },
        "in": {
          "maxLength": 21
        }
      }
    }
  ]
}
```

```

],
"$defs": {
  "person_name": {
    "description": "The person's name consisting at least of a separate
      standardised surname, or a standardised forename, or both -
      with standardisation done according to the rules defined in
      ICAO Doc 9303 Part 3",
    "anyOf": [
      {
        "required": [
          "fnt"
        ]
      },
      {
        "required": [
          "gnt"
        ]
      }
    ],
    "type": "object",
    "properties": {
      "fn": {
        "title": "Surname",
        "description": "The surname or primary name(s) of the person
          addressed in the EHIC",
        "type": "string",
        "maxLength": 40,
        "examples": [
          "d'Červenková Panklová"
        ]
      },
      "fnt": {
        "title": "Standardised surname",
        "description": "The surname(s) of the person, transliterated to
          ICAO 9303",
        "type": "string",
        "pattern": "^[A-Z<]*$",
        "maxLength": 40,
        "examples": [
          "DCERVENKOVA<PANKLOVA"
        ]
      },
      "gn": {

```

```
    "title": "Forename",
    "description": "The forename(s) of the person addressed in the
                    EHIC",
    "type": "string",
    "maxLength": 35,
    "examples": [
        "Jiřina-Maria Alena"
    ]
},
"gnt": {
    "title": "Standardised forename",
    "description": "The forename(s) of the person, transliterated to
                    ICAO 9303",
    "type": "string",
    "pattern": "^[A-Z<]*$",
    "maxLength": 35,
    "examples": [
        "JIRINA<MARIA<ALENA"
    ]
}
},
"countryCode": {
    "title": "Country Code",
    "description": "Identification code of the country (2 digit ISO country
                    code (ISO 3166-1)), with the addition of UK for GB",
    "enum": [
        "AT",
        "BE",
        "BG",
        "CY",
        "CZ",
        "DE",
        "DK",
        "EE",
        "EL",
        "ES",
        "FI",
        "FR",
        "HR",
        "HU",
        "IE",
        "IS",
```

```
        "IT",  
        "LI",  
        "LT",  
        "LU",  
        "LV",  
        "MT",  
        "NO",  
        "NL",  
        "PL",  
        "PT",  
        "RO",  
        "SE",  
        "SI",  
        "SK",  
        "CH",  
        "UK"  
    ]  
}  
}
```

7 JWT specifications, technical data model

Definition of the JWT that contains the eEHIC/entitlement document credentials, including supported versions/standards (examples of instances / validations are available in “Annex I – example of creation and validation of a JWT for ”)

The eEHIC credentials are technically rendered in form of a **Signed JWT** (JSON Web Token), which is referred to as a **JWS** (JSON Web RFC 7515). This choice also follows the technical specifications by the EUDI framework, which consider JSON as one of the possible keystone technologies for its electronic attestation of attributes.

As represented in the schema below, the JWS consists of three sections, a *Header*, a *Payload*, and a *Signature*. These sections will be described hereunder, each one in a dedicated paragraph.

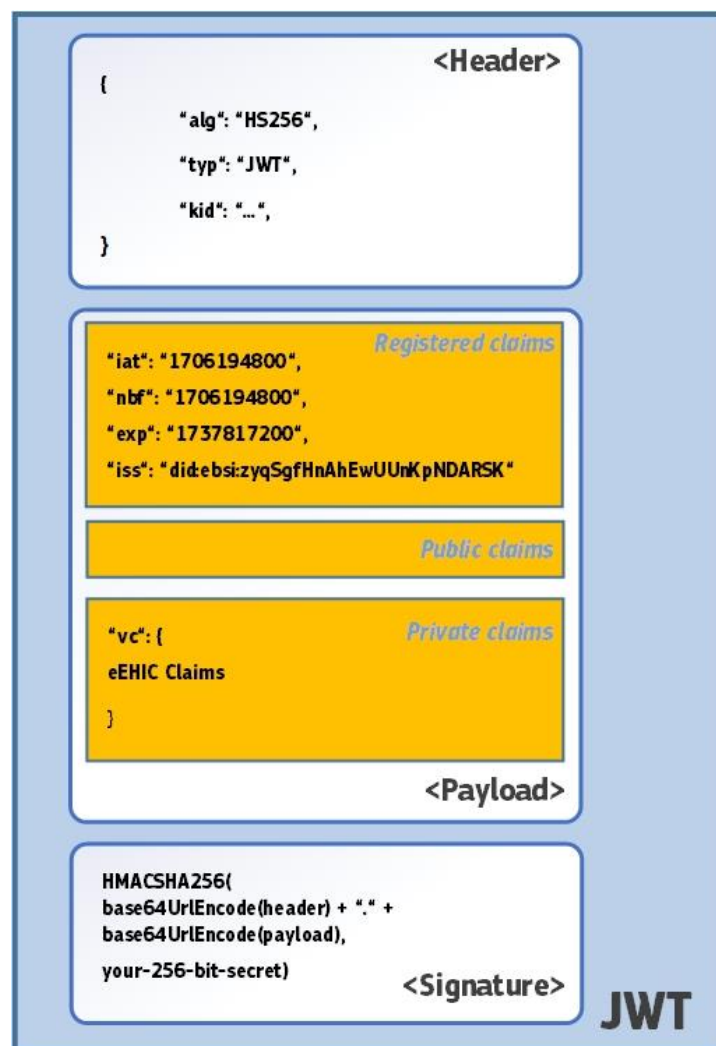


Figure 13 - Schema of the JWT structure with sample data

7.1 Header

The header section stores:

- the Type of the token (“typ”);
- the Signature Algorithm (“alg”);
- a Key Identifier (“kid”), needed to detect the key used to place the signature under the token.

Each of them is described in a dedicated paragraph below.

Signature Algorithm

The *Signature Algorithm* identifies the algorithm that is used to sign the JWT.

This algorithm will be one of the following: *ES256*, *ES256K*, *Ed25519* and *EdDSA*.

For the signing process of the attestations we propose to use the *ES256* algorithm. We recommend defining as secondary algorithm the *Ed25519*.

Type

The *Type* identifies the technical type of the credential. In our case, this will be always filled in with the value “JWT”, as described in section 5.1 of RFC 7519.

Key Identifier

The *Key Identifier* is the reference to the actual keys used by the issuer to sign the credential.

It is used for verification purposes of the signature, as index to identify the correct key from the registry that contains all the keys of all the issuers (see section 9). Signing the web token with a different key than the one defined in the *Key Identifier* will result in an error at verification stage, either by issuer, holder or verifier.

The X509 Serial number will not be used for defining a KID, as the serial number is only unique within the domain of the CA, making it possible that there is a collision of serial numbers if multiple CA's are used.

7.2 Payload

The Payload contains several “claims” grouped in three classes: *registered*, *public*, *private*. The claim is the name used for the attributes of the payload.

Registered claims

Please note that the attributes in the registered claims should refer to technical information and not to business data, i.e. the expiration time is a technical expiration time of the message itself and not the business expiration of the attestation.

This set-up would allow to differentiate between the business and technical data, e.g. the expiration of the entitlement and the technical expiration of the digital mean.

After shared reflections, the AHG established that, despite the technical validity, this distinction would bring little, if any, added value to the business case and create possible confusion among the end users, for instance in the case where the check on the technical validity would fail, while the entitlement would still be valid.

To enhance the user experience, the decision is to keep these claims for sake of completeness, and in case in the future the desired behaviour needs to be changed, but use the same values reflected in the business fields.

Our suggestion is to use just the small subset of “registered” claims listed here below:

- the ‘electronic EHC/entitlement document’ **Issuer** (“iss”) - the Issuer of the current JWT;
- the **expiration time** (“exp”) – under a technical point of view, it should indicate for how long this particular JWT message shall be considered valid. The purpose of this parameter is to force a limit of the technical validity period of this container.

Following the principle explained in the introduction of this paragraph, in our case this value shall be the same as the “Expiry date” defined in the business data;

- **not before time** (“nbf”) – under a technical point of view, it should be the time before which the current JWT shall not be accepted for processing. Following the principle explained in the introduction of this paragraph, in our case this value shall be the same as the “Start date of validity” defined in the business data;

- **issued at time** (“iat”) – under a technical point of view, it should be the time at which the current JWT was issued; it can be used to determine the age of the current JWT. The ‘Issued at time’ field shall not predate the validity period of the DSC that was used to sign the JWT. Following the principle explained in the introduction of this paragraph, this value shall be the same as the “Date of Issuance” defined in the business data.

Private claims

All the other needed business data will be encapsulated as “private” claims. This choice is made also to keep all the core business data together in the same group; in this way, if in the future new technical solutions will need to be adopted, all the data will be already packed in the same element and no adaptation/restructure will be needed to encapsulate them in a potential new container.

In order to use the JWT as a carrier for credentials, a body called the *Verifiable Credential (VC)* will be used to contain the missing business data defined in the JSON (see section 66).

Usage of “registered” claims can lead to inappropriate use with ambiguous outcomes. For example, it exists a “registered” claim named ‘given_name’, which is defined in context of authentication of a person using openID. The use of ‘given_name’ in the context of the eEHIC can lead to ambiguities, as it is not clear to whom the given name belongs, e.g. if the eEHIC is issued to a minor, whether it is the mother’s or the child’s name. Our idea is to avoid contextless information items, such as the “registered” claims, and to rely only on “private” claims, that are specifically defined for our use case and we know how they will be treated in our use case.

List of claims

In the following table we summarise the list of all claims to be included in the JWT, specifying where they are stored, the type of values allowed and cardinality.

Version 1

Label	Claim	Section	Group	Data type	Card.
Signing algorithm	<i>alg</i>	Header		String, pattern: “ES256” “ES256K” “Ed25519” “EdDSA”	1..1
Type of credential	<i>typ</i>	Header		String, pattern: "JWT"	1..1

Key Identifier	key	Header		String	1..1
Issued At	<i>iat</i>	Payload	Registered	Numeric date	1..1
Not before	<i>nbf</i>	Payload	Registered	Numeric date	1..1
Expiration	<i>exp</i>	Payload	Registered	Numeric date	1..1
Issuer	<i>iss</i>	Payload	Registered	String or URI	1..1
Name and given names	<i>hn</i>	Payload	Private	PersonName	1..1
Date of birth	<i>dob</i>	Payload	Private	String, pattern: "^((\\d\\d/){2}(19 20)\\d\\d\$)", format Date	1..1
Personal Identification number	<i>hi</i>	Payload	Private	String, maxLength=20	1..1
Identification number of the institution	<i>ii</i>	Payload	Private	String, minLength=4, maxLength=10	1..1
Name of the institution	<i>in</i>	Payload	Private	String, maxLength=21	1..1
Card Identification number	<i>ci</i>	Payload	Private	String, minLength=20, maxLength=20	1..1
Card Issuer Country	<i>ic</i>	Payload	Private	Possibles values ⁴ : ["AT", "BE", "BG", "CY", "CZ", "DE", "DK", "EE", "EL", "ES", "FI", "FR", "HR", "HU", "IE", "IS", "IT", "LI", "LT", "LU", "LV", "MT", "NL", "NO",	1..1

⁴ <https://publications.europa.eu/code/pdf/370000en.htm>

				"PL", "PT", "RO", "SE", "SK", "SI", "CH", "UK"]	
Start date of validity	<i>sd</i>	Payload	Private	String, pattern: "(\\d\\d/){2} (19 20)\\d\\d \$", format Date	1..1
Expiry date	<i>ed</i>	Payload	Private	String, pattern: "^((\\d\\d/){2} (19 20)\\d\\d \$", format Date	1..1
Date of issuance	<i>id</i>	Payload	Private	String, pattern: "^((\\d\\d/){2} (19 20)\\d\\d \$", format Date	1..1

PersonName type

Label	Claim	Section	Group	Data type	Card.
Surname	<i>fn</i>	Payload	Private	String, maxLength=40	1..1
Forename	<i>gn</i>	Payload	Private	String, maxLength=35	1..1

Version 2

In the table below we just spot the differences between the version 1 and version 2 of the claims, highlighting in yellow the still not defined aspects.

Label	Claim	Section	Group	Data type	Card.
Date of birth	<i>dob</i>	Payload	Private	String, pattern: "^(19 20)\\d\\d(- \\d\\d){2}\$", format Date	1..1
Start date of validity	<i>sd</i>	Payload	Private	String, pattern: "^(19 20)\\d\\d(-	1..1

				\\d\\d){2}\$", format Date	
Expiry date	<i>ed</i>	Payload	Private	String, pattern: "^(19 20)\\d\\d(-\\d\\d){2}\$", format Date	1..1
Date of issuance	<i>id</i>	Payload	Private	String, pattern: "^(19 20)\\d\\d(-\\d\\d){2}\$", format Date	1..1

PersonName type

Label	Claim	Section	Group	Data type	Card.
Surname	<i>fn</i>	Payload	Private	String, maxLength=XX	1..1
Standardised surname	<i>fnt</i>	Payload	Private	String, pattern: "[A-Z<]*\$", maxLength=XX	1..1
Forename	<i>gn</i>	Payload	Private	String, maxLength=XX	1..1
Standardised forename	<i>gnt</i>	Payload	Private	String, pattern: "[A-Z<]*\$", maxLength=XX	1..1

Serialisation and creation of the Virtual Credential payload

The following scheme represents the serialisation pattern.

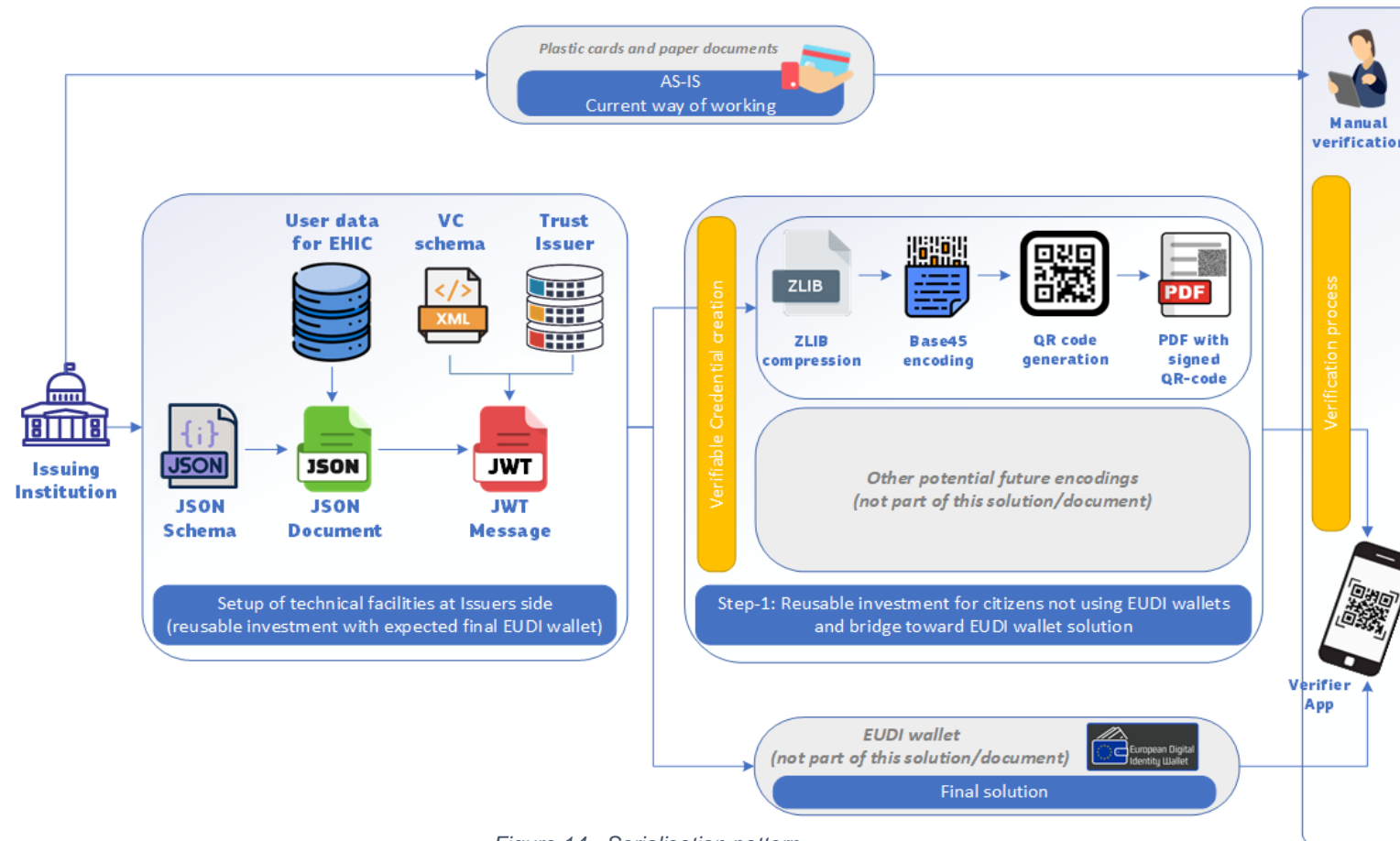


Figure 14 - Serialisation pattern

The process starts with extraction of data and its structuring according to the VC schemas defined in section 6. In this process the encoding in JSON format may take place before the serialisation to JWT starts.

Once the serialised JWT is available, the resulting data will be compressed using ZLIB (RFC 1950) and the *Deflate* compression mechanism, in the format defined in RFC 1951. After this process, the compressed data is encoded in Base 45 to be able to transform it in a 2-dimensional QR-code (see section 8 for further details).

7.3 Signature

This sub-section will include also references to supported algorithms for MAC (hash-code algorithms) and Signing (encoding algorithms) and signature validation requirements.

The integrity of payload data and the authenticity of the issuer is established by using cryptographic processes for signing and assuring the contents. The cryptographic processes and algorithms are defined in the JSON Web Signature (RFC 7915).

The *Signature Algorithm* (“alg”) claim in the Header indicates what algorithm is used for creating the signature. It must comply with the JWT requirements for algorithms, defined in JSON Web Algorithm (JWA) RFC 7518. The supported encryption methods are: ES256, ES256K, Ed25519 and EdDSA.

One primary and one secondary algorithm need to be defined. The secondary algorithm should only be used if the primary algorithm is not acceptable within the rules and regulations imposed on the issuer.

In order to ensure the security of the system, all implementations have to incorporate the secondary algorithm. For this reason, both the primary and the secondary algorithms must be implemented.

The proposed algorithms are ES256, as primary algorithm, due to the existing support of various open-source tools for validation and verification, and Ed25519, as secondary Algorithm.

8 QR code specifications

This section will describe the specifications of the QR code and the process to move from JWT to the QR code itself

8.1 QR codes as Verifiable Credentials

Verifiable Credentials (VC) are structured documents that are signed by Trusted Issuers. The VC contains information about a subject and about its Issuer, so that it can be verified without the Verifier knowing the Issuer directly.

The trust in the Issuer is established by means of verifying the Issuer encoded in the VC against trusted registries. A reference of the Issuer (the key identifier – kid) is used to retrieve information about the Issuer from the trusted registries for verification. The trusted registries contain the identity of all possible Issuers and their accreditation, i.e. whether they are entitled to issue this type of credentials. The authenticity of the VC can be verified, because it is cryptographically signed, and the signing key is cryptographically linked to the identity of the Issuer.

The signature assures authenticity of the issuance and the establishment of integrity of the document. The signature itself can prove whether the document has been tampered. The accreditation of the Issuer by other trusted entities is essential to create and establish trust in the identity.

8.2 Proposed QR code

The European Health Insurance Card data are encoded in JSON to conform to the defined JSON schema registered in the trusted registries (see section 6). This allows the encoding of the information printed on a physical EHIC card in a digitally verifiable format.

Usually, VCs are presented using a special wallet application on a smartphone. However, this solution can pose a barrier for adoption, since some users may lack the necessary hardware (device) or abilities to operate it. Therefore, in this section, we define a way of encoding the VC in a QR code that can be embedded in a digital document readable by commonly available standard software (e.g. browser or pdf reader) or even printed on a paper.

To make the size of the QR code manageable, steps are taken to minimise the data.

In Figure 15 below, the process is graphically depicted.

The data for the VC comes from the issuing institution, it is then transformed in the JSON format, which adheres to a schema for conformance purposes. The validated JSON document is then digitally signed, and the signature is stored in a compact JWS

format, using the (private) signing key of the institution. The resulting code is attached to a URN, which is used to identify the type of VC.

The resulting document is then compressed using ZLIB, and then encoded as a BASE-45 data-block, which is finally transformed into a QR code using Alphanumeric encoding.

This method of serialising JSON data into a QR code is similar to the one used in the [EU Digital COVID Certificate](#).

8.3 Creating the QR Code

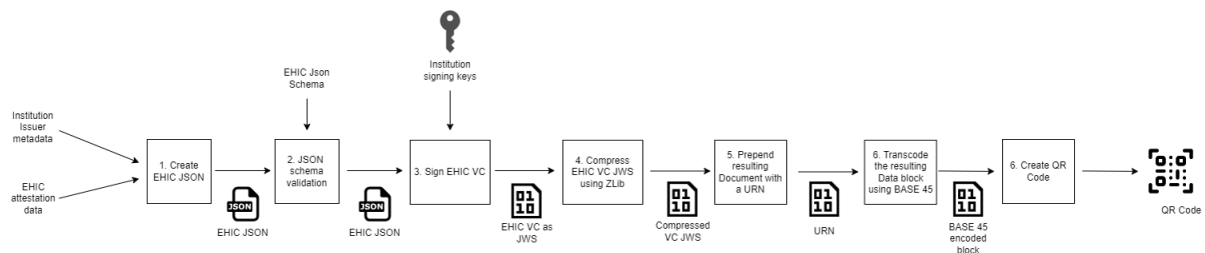


Figure 15 - Creating the QR code for the Verifiable Credential

Here is a summary of the steps depicted above:

1. create the VC JSON object with the data of the attestation and the issuer institution metadata;
2. validate the generated JSON based on the EHIC JSON schema;
3. sign the VC using the institution (private) signing key, creating a compact JWS signature;
4. compress the VC JWS using *ZLib*;
5. prepend the resulting compressed Document with a URN for identification purposes;
6. transcode the resulting data-block using *BASE-45*;
7. create a QR coding starting from the *BASE-45* transcoded data-block by using Alphanumeric encoding.

8.4 Decoding the VC QR code

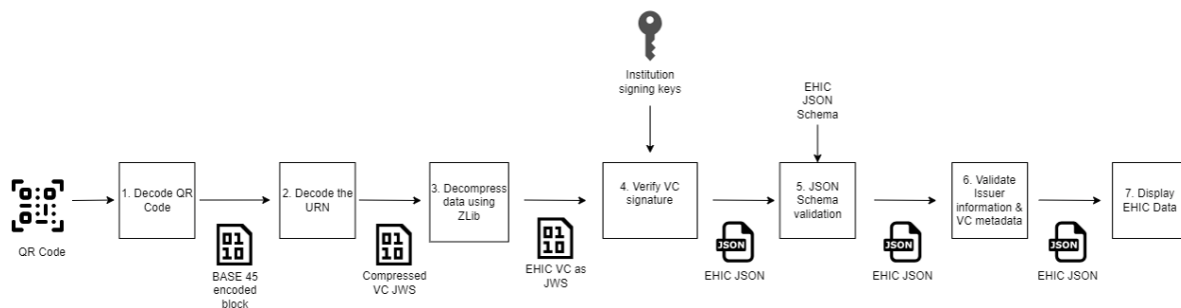


Figure 16 - Decoding the VC QR code

The process to decode the VC QR code is the reverse of the one described in the paragraph above and is summarised in the following step-by-step list, as depicted in Figure 16:

1. Decode the QR code using a reader, obtaining a BASE-45 encoded data-block;
2. Decode the URN from the data-block;
3. Decompress the resulting data using ZLib;
4. Verify the signature using the issuing institution (public) key;
5. Validate the obtained JSON using the VC JSON Schema, as defined in section6;
6. Validate Issuer information and VC metadata. This includes, but is not limited to, the Issuer identity and accreditations, and the attestation status, verifying the VC validity period;
7. Display VC data in an appropriate manner for the use case.

9 PKI (Public Key Infrastructure) - specifications of signatures used within the Verifiable Credential

Among the other considerations, this section will contain definition of PKI hierarchy, requirements, roles, responsibilities, policies, constraints, procedures, supported software/hardware, architecture for managing signatures of trusted institutions issuing eEHIC.

Main points to be addressed:

- how to establish the trust among stakeholders (you need to define the organisation that manages the trust and the processes to keep it)?
- Need to identify the entities in a common proper way.
- Definition of processes about how to register your keys in the public registry, what happens when a key expires, what is the validity of a document with an expired key... these are all questions we need to address clearly in the document. These questions are dealing with both business and technical aspects.

According to Article 88 of the *REGULATION (EC) No 987/2009* the Social Security Coordination domain already has an official database housing the needed information for Social Security institutions in Europe.

Such database is the EESSI-Institution Repository (IR) and stores the identities and keys that are used to sign digital messages in the context of EESSI.

Reusing the existing EESSI-IR seems the wisest choice under both a technical and cost-efficiency point of view. Having two different repositories would imply a doubling in costs, and maintenance.

It is important to stress that the defined PKI could be reused also when digitalising other Portable Documents (e.g. PDA1).

Assumptions:

- a) The reuse of EESSI-IR is enough for this intermediate digitalisation phase, as, relying on Article 88 of 987/2009, all the institutions issuing the EHIC are registered in this database.
 1. Currently, the certificate information is not exposed by the CAI/PAI applications that expose the EESSI-IR data on the internet. The solution we suggest is to create a service, called “bridge”, which would expose the needed (non-personal) data in a secure way on the internet.

2. The “bridge” should rely **on a robust production infrastructure**, capable to cope with an important amount of traffic.
 3. It is important to stress that, as described in section 12.60, the verification process should be possible also in offline mode, as internet connection cannot be always guaranteed. For this reason, the data exposed by the bridge should be also available for download. More details about this aspect will be defined in the dedicated section 10.30.
 - In case, in the future, an extension of such repository could be required, e.g. to include a different set of organisations, in function of their geographical location, their domain, or any other reasons, some sort of federation of repositories could be foreseen. The “bridge” solution could perfectly provide an answer to this need for generalisation, as it could hide the complexity of integrating multiple sources of information and simply providing the needed data from the federation in a seamless way for the caller, who will not need to adapt its interface.
- b) What are the data that EESSI-IR needs to expose, to allow the proper verification of the credentials, together with the public key? Is it needed to link the issuance of a type of attestation to the issuing organisation and do we need to keep the historical changes of these accreditations? If we need to control whether an organisation is entitled to issue the EHIC, we need to expose the current Boolean field called “Issue EHIC”. But what if an institution entitled to issue the EHIC loses this entitlement, i.e. its Boolean flag becomes ‘false’? The EHICs issued are still valid, but there is currently no way to know until when such organisation was entitled to issue EHIC. Either we will need to adapt the EESSI-IR and its interfaces to register also the dates when the entitlement of issuing the EHIC was changed, or we do not check the fact the institution is/was entitled to issue the EHIC, as it could bring to wrong results. The business and legal sub-group has decided that the entitlement of issuing the EHIC needs to be checked. So the EESSI-IR and its interfaces need to be adapted to be able to state when an institution was entitled to issue the EHIC. This need will be present also for other future entitlement documents.
 - c) In some Member States there could be a distinction between ‘Authentic source’/‘competent institution’, which is the organisation owning the data of the card holder and having the capability to establish whether a citizen is entitled to receive a EHIC (business decision), and the ‘Issuer’, which is the organisation actually issuing the (digital) attestation (processor/technical issuer). In case the “issuer” and the “authentic source” are different, should the link between them be recorded in the database, or its management is an internal matter of each Member State? We suggest that this situation needs to be managed internally by each Member State and shall not have an impact on the current solution, so this information will not be stored, at least for the version 1, in the EESSI-IR.
 - d) Should the same private/public keys-set be used by the EESSI-IR organisations to sign any kind of message/certificate in the domain of SSC (e.g. EHIC, PDA1, EESSI messages)? If this is not the case, we will need to change the IR to be able to store multiple keys for each organisation, specifying their specific use. The Ad-hoc group has not found a common agreement on the topic and the

same issue is being discussed in a dedicated thread in the Technical and Administrative Commission. A decision on the way forward needs to be taken.

9.1 PKI introduction

Digital certificates are electronic credentials that bind the identity of the certificate owner to a pair of electronic encryption keys (one public and one private) that can be used to encrypt and sign information digitally. The primary purpose of the digital certificate is to ensure that the public key in the certificate belongs to the entity to which the certificate was issued. In other words, to verify that a person sending a message is whom they claim to be and then provide the message receiver with the means to encode a reply to the sender.

Public key cryptography depends on key pairs: one is the private key to be held by the owner and used for signing and decrypting, and one is the public key that can be used to encrypt data sent to the public key owner or authentication of the certificate holder's signed data.

The digital certificates play a crucial role in helping our solution to achieve its most critical information security goals: this includes ensuring integrity and non-repudiation (by signing digital data) and confidentiality (by encrypting data).

Public Key Infrastructure (PKI) is another essential element of digital encryption and cryptography. PKI governs the management and deployment of digital certificates and public key encryption by establishing the required roles, policies, and procedures.

9.2 The EESSI Institution Repository (IR)

The Institution Repository contains all information on the institutions exchanging messages within EESSI. This information is managed and maintained at the Central Service Node (CSN) and synchronised towards Access Points (AP) and, optionally, National Applications (NA). The Institution Repository was defined based on decision E8 that implements the Regulation (EC) No 987/2009 and Regulation (EC) No 883/2004.

Since the Institution Repository data integrity and quality is essential for the EESSI environment, the European Commission requires participating Countries to follow the process below before populating the Institution Repository. The following process is used when EESSI Central Service Desk provides access credentials for IR SPOCS (IR Business SPOC and IR Technical SPOC) for the CSN environment:

1. EESSI SPOC together with IR SPOCs completes the access request form;
2. EESSI SPOC sends the request form to EESSI Central Service Desk;
3. EESSI Central Service Desk provides access credentials;
4. IR SPOCs (IR Business SPOC and IR Technical SPOC) start populating the IR in the PRODUCTION environment.

More information can be found in the document EESSI Institution Repository - Criteria for Production Environment (document available in the AHG team or in the EESSI internal documents repository).

As described in the EESSI Terms of Collaboration (AC 682/17REV), each EESSI participating Country designated their Institution Repository Business Data Contributor (IR Business SPOC) and Institution Repository Technical Data Contributor (IR Technical SPOC), responsible for maintaining the accuracy of the Institution Repository information for the institutions covered by the APs in that country. The IR Technical SPOC must populate the institution's technical data (Endpoints and Certificates) in the Institution Repository (IR). This activity can be performed manually, using the IR Institutions Management Console (IMC).

The IR Technical SPOC is responsible for issuing and managing the institution's ebMS (e-business Messaging Service) and business certificates abiding by the specification in the EESSI Certificate Profiles in the National Domain document (document available in the AHG team or in the EESSI internal documents repository).

The Data Model for the Institution data provided for the Institution Repository has been defined in the EESSI - CSN Repository Structure and Management document which is part of the Architecture Pack v1.0 (document available in the AHG team or in the EESSI internal documents repository). Details on the structure of the Institution data have been defined in the EESSI CSN IR Front End Use Cases and Specifications document.

9.3 Trust List format

In this section the specification of the EESSI-IR certificate and its requirement should be defined.

The EESSI IR's Certificate Repository contains certificate information used by the Institutions and Access Points to secure the message transfer from the originating to the destination institution. The information is always updated at the repository in the CSN and is then published to the repositories at the AP's.

The institution certificates are stored in the CSN database in a binary format. Several Certificate attributes like Certificate Thumbprint, Serial Number, Subject, Issuer, Public key, ValidFrom, ValidTo are synchronised with the Access Points.

9.4 Security considerations

In this section any security considerations concerning the identity, certificates, trusts the process should be described according to current practice using the EESSI-IR. For instance , any policy on who can access the EESSI-IR to update it. Any audit functionality to ensure the correctness of

registered data. Any particular form of facility use to create/request certificates.

Digital Certificates and Public Key Infrastructure (PKI) are at the core of the existing EESSI Security model. The Social Security Institution's certificates in the IR represent the sending/receiving competent institution or liaison body, as defined in the EESSI Terms of Collaboration. These keys could be used also to digitally sign entitlement documents in the social security coordination domain, e.g. EHIC and PDA1.

The existing EESSI security architecture was conceived using a hybrid trust model based on mutual exchange and the domain trusted list. The EESSI model relies on digital certificates from various trust anchors. Without a single trust anchor, countries are usually free to choose their preferred one and mutually exchange the trusted root certificates with each other. Since the exchanged digital certificates represent the trust anchor, the validation and verification of trust are reflected by the existence of the digital certificate in the local trust store.

The existing security model also uses a domain trusted list containing the trusted certificates. This list is maintained centrally on the Central Service Node (CSN) and is synchronized with Access Points (AP). This list can be used for authorising institutions to send business messages and, in the EHIC case, to sign the digital credential. The signing certificate thumbprint is verified against this list.

The countries are responsible for acquiring and managing certificates within the national domain. In the current architecture, national domain certificates are issued exclusively by a Certification Authority (CA) from the EU trusted list, following guidelines provided by the EESSI project team in the "EESSI - Certificate Profiles National Domain" document (document available in the AHG team or in the EESSI internal documents repository). Countries have the freedom to choose a CA based on the ECSD recommendation for Social Security Institution's ebMS and business certificates.

The CSN's Institution Repository (IR) serves as the authoritative and trusted data source for Social Security Institutions to exchange information within the EESSI ecosystem.

The CSN stores data about all institutions participating in EESSI, and synchronises this data with EESSI components. For a Social Security Institution (SSI) to issue an EHIC, it must be added to CSN's IR and follow a process defined in the relevant legislation to prove its identity and competencies for message exchange with other SSIs.

The certificates for the Social Security Institutions are used in the current architecture as described below:

- **NA Business Signature Certificate** - this certificate is used for signing Structured Electronic Documents (SEDs) generated by the National Application.
 - The business digital certificate represents the sending/receiving Competent Institution or Liaison Body.
 - The certificate is issued under the national domain name.
 - The private key is installed on the NA.
 - The public key is added to the Institution Repository.
- **NA ebMS Certificate** - this certificate is used for signing ebMS (electronic business Messaging Service) messages created by the National Application.
 - The ebMS digital certificate represents the sending/receiving Competent Institution or Liaison Body.
 - The certificate is issued under the national domain name.
 - The private key is installed on the NA.
 - The public key is added to the Institution Repository.

For signing the electronic EHIC/Entitlement document, we suggest to use the EESSI Business Signature Certificate, since it is the one officially representing the Social Security institution.

Currently, some institutions share the same certificate in the EESSI-IR and this could bring to trust issues. Details on the use of digital certificates should be further discussed.

The CSN infrastructure is hosted by the European Commission at the DIGIT Data Centre and is securely deployed in accordance with both the EESSI Security Policy and the European Commission's security policy controls. This system is not accessible from the internet; it is available to participating countries exclusively through the secure S-TESTA network. Access to the IMC (Information Management Component) is authenticated and authorised via two-factor authentication, using the EC corporate identity service, EU Login. Furthermore, the system is integrated into the Commission's Governance, Risk Management, and Compliance (GRC) framework and has a comprehensive Security Plan in place.

9.5 Key management

In this section we should describe the process about how institutions create/change/rotate/delete registrations in the EESSI-IR (this will be relevant for issuing the EHIC entitlement documents) and which steps they need to do to acquire a valid certificate to register in the EESSI-IR.

The EESSI participating countries are responsible for key management, including creating/changing/rotating and deleting their keys. To do so, they have in place key management processes and they are issuing the business and technical certificates to be added to IR following the specification below.

New institution business data are added to the Institution Repository (IR) from Central Service Node (CSN) to be used within the EESSI environment. The addition of an institution goes through a data publication and activation process. Before the publication of an Institution, all defined mandatory data must be filled in. After successful validation of the data that were entered by the Institution Repository Business Data Contributor (the system checks all business validation rules), the data are published and an activation date is set (the IR Business Data Contributor informs his country's Administrative Commission delegate who informs the Secretariat of the Commission, and the Secretariat informs the stakeholders on the publication of this new Institution).

The process of creating a new institution and adding the business and technical certificates is described in chapter 5.1.1 Use Case IR_IMC_01 - Add New Institution (Business Data) of the IMC end user manuals and guides document (document available in the AHG team or in the EESSI internal documents repository).

The Institution Repository allows for multiple entries in the "Certificates" field for an institution, for both certificate types "Business Signature" and "ebMS Signature." Having at least one "Business Signature" and one "ebMS Signature" certificate is mandatory for an institution to be active in EESSI.

Every line in the Certificates section of the technical information block of fields represents one and only one institution (the institution ID is added in the line). Since the Institution Repository allows setting of multiple entries for the Certificates for an Institution, then there may be multiple lines with the same Institution ID.

The certificates (*.cer files) must not include the whole chain of certificate data up to the Root Certificate Authority.

Certificate Issuing Authorities

All certificates used for EESSI National Domain must be issued by a trust service provider.

EESSI Certificate Profiles

EESSI-compliant X.509 certificates used for electronic seals (the National Institution ebMS certificate and National Institution Business Signing certificate) should comply with ETSI EN 319 412-3 in line with the QCP-I profile in ETSI EN 319 411-1, with amendments specified in the next Certificate Profiles.

Certificate Profiles

The following specifications establish a minimal set of requirements for requesting certificates within the National Domain. These certificates must be issued by Trusted Service Providers from the eIDAS EU Trusted List. Participating countries can request

digital certificates from any Certification Authority of a Trusted Service Provider listed in the EU Trusted List, not limited to those CA listed in the EU Trusted List.

It is highly recommended that the chosen provider is listed within the Microsoft Trusted Root Certificate Program and CA/Browser Forum trusted root store for ease of usage during the operational phase.

EESSI only requires advanced signatures. However, participating countries have the option to use qualified digital certificates for EESSI business signatures. It is the responsibility of these countries to test the proper functionality of the application within the EESSI context when using qualified certificates.

Note: when not further specified, the minimum requirements specified in the description of an element listed in the table below apply to all types of EESSI certificates for the National Domain identified in Certificate Profiles. When preceded by [TLS], the minimum requirements specified in the description of an element are only applicable to EESSI-compliant X.509 TLS/SSL certificates. Elements whose description is preceded by [Seal - ebMS] are only applicable to ebMS certificates, and elements whose description is preceded by [Seal – Business Signature] are Business Signature X.509 certificates used for the establishment of electronic seals.

Element		Description
Serial number		According to the TSP requirements.
Validity from/to		Certificates used by EESSI National domain services SHOULD be valid for a maximum of 3 years.
IssuerUniqueID		The field "IssuerUniqueID" MUST NOT be used.
SubjectUniqueID		The field "SubjectUniqueID" MUST NOT be used.
Subject		According to the TSP requirements.
Issuer		The DName MUST be identical to the subject DName of the Issuer certificate.
Extensions		
Authority Key Identifier		(a) "Authority KeyIdentifier" MUST be included as an extension in the certificate. (b) The "SubjectKeyIdentifier" of the issuing CA MUST be used. (c) AuthorityCertIssuer and AuthorityCertSerialNumber SHOULD NOT be used as AuthorityKeyIdentifier.
Subject Key Identifier		(a) "SubjectKeyIdentifier" MUST be included as an extension in the certificate. (b) One of the methods described in clause 4.2.1.2 of [RFC 5280] MUST be used.

KeyUsage (critical)	<p>(a) "KeyUsage" MUST be included as an extension in the certificate.</p> <p>(b) The extension MUST be designated as critical.</p> <p>(c) [TLS]: The digitalSignature and keyEncipherment bits MUST both be set to true to the exclusion of all other Key Usage bits that MUST be set to false [Seal -ebMS] [Seal –Business Signature]: The Non-Repudiation bits MUST be set to true to the exclusion of all other Key Usage bits that MUST be set to false.</p>
IssuerAltNames (non-critical)	(a) "IssuerAltNames" SHOULD NOT be included as an extension in the certificate.
SubjectAltNames (non-critical)	(a) "SubjectAltNames" SHALL only be included as an extension in the certificate if the value is identical to the Subject-DName/CN of the Certificate.
BasicConstraints	(a) "BasicConstraints" MUST be included as an extension in the certificate.
Extended Key Usage (non-critical)	(a) [Seal –Business Signature][Seal -ebMS] "ExtendedKeyUsage" MUST be included as an extension in the certificate according to eIDAS (and CA/B) requirements in accordance with RFC5280. Note that this extension value is not validated by the EESSI software thus following the TSP provider recommendation will suffice. [TLS] Both values id-kp-serverAuth [RFC5280] and id-kp-clientAuth [RFC5280] MUST be present.
CRL Distribution Points (non-critical)	<p>(a) "CRLDistributionPoints" MUST be included as an extension in the certificate.</p> <p>(b) The certificate MUST include a CRL distribution point extension.</p> <p>(c) When present, the CRL distribution point extension MUST include at least one reference to a publicly accessible CRL distribution point. available CRL.</p> <p>(d) At least one of the present references MUST use http (http://) [RFC 7230 -7235]</p> <p>(e) The extension shall not be marked critical</p>

Authority Info Access (non -critical)	<p>(a) "AuthorityInfoAccess" MUST be included as an extension in the certificate.</p> <p>(b) When OCSP is supported by the issuing CA, the Authority Information Access extension MUST include an accessMethod OID, id-ad-ocsp, with an accessLocation value specifying at least one access location of an OCSP [RFC 6960] responder authoritative to provide certificate status information for the present certificate.</p> <p>(c) When present, at least one access location MUST specify either the http (http://) [RFC 7230-7235] or https (https://) [RFC 2818] scheme to reference a publicly available OCSP responder, which accepts unsigned and unauthenticated status requests.</p> <p>(d) When the issuing CA is not represented by a self-signed root certificate, the Authority Information Access extension MUST include an accessMethod OID, id-ad-caIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA. At least one access location shall use the http (http://) IETF RFC 7230-7235 scheme or https (https://) IETF RFC 2818 scheme. This requirement MAY be ignored altogether when the issuing CA is represented by a self-signed root certificate.</p>
--	--

(Maximum) validity of a certificate

The maximum validity of a certificate in EESSI is two years. Expired certificates are not permitted to be added to the IR. However, the IR can include and synchronise expired certificates up to 5.000 days past their expiration date, based on the current configuration. For tracking-changes purpose, a change history is maintained, which keeps track of all certificate changes for each institution.

9.6 The Key Identifier (KIDs) of the Issuer

In this section the specification of the Key Identifier used to detect the correct Issuer on the EESSI-IR should be described.

The purpose of the KID is to easily identify the Issuer and retrieve its public keys for verification purposes. The KID will be created with the private key of the Issuer, which is used to create the public key in the X509 certificate. The Algorithm to derive the KID will be described in Annex V - Key Identifier algorithm.

The Issuer needs this algorithm to determine the KID at signing time via the algorithm. The KID will be used to find the appropriate public key in the federated trust-store.

10 Federated trust landscape

10.1 The future vision

The trust landscape, from which the information about the trust registries is retrieved by verifiers of attestations for validation and verification purposes, needs to be extensible and domain independent.

It can be postulated that once EUDI wallets will be a *de facto* standard, several other systems at EU level will have the same needs of our EHIC case and should be able to reuse the infrastructure we are defining, reducing the complexity of the future EU systems landscape and reducing the cost for Member States that won't need to re-develop components providing the same functionalities.

To achieve this goal, the final proposal is to have a federated trust landscape where systems from different domains can *transparently* expose the trust for their individual issuers, without the need to be concerned about the process and status of the established trusts of other domains.

The Federated Trust allows the decoupling of network enclaves (such as TESTA where EESSI-IR is connected) from the internet. Furthermore, the Federated Trust is modelled independently from the Domain Trusted Registries with regard to the availability, security and resilience of services (e.g. the need to increase the capability of EESSI-IR to support a higher usage from the healthcare providers). If the Federated Trust Store would be compromised, this shall not affect the specific domain registries, as these are decoupled via an interface (Bridge) and the flow of information is one way from the domain registries to the Federated Trust Store.

The federated trust landscape will allow Issuers from other domains, such as education, to be accessible to the same stakeholders in the same manner, without the need to add non Social Security entities to the EESSI-IR. The EESSI-IR will remain managed under the current governance and regulation.

To achieve this concept, the EESSI-IR must be coupled to the federated trust through the implementation of a service, which we refer to as the "Bridge". The responsibility of the bridge is to make available all the changes in the domain of EESSI-IR to the federated trust by translating and mapping the trust among domains, and keeping the entries aligned.

10.2 Version 1

The implementing acts foreseen in the European Digital Identity framework Regulation (eIDAS 2.0) laying down more details on the trust framework are still in drafting phase.

One of the aspects that has not been defined yet is how this trust framework will integrate/liaise with already existing trust repositories, like the EESSI-IR. For this reason, defining a solution in this direction could lead to the need to re-engineer it in

the short-period when the framework will be completely defined. Moreover, the consortia are already designing the complex final trust model to be applied to the social security domain and it would have no sense to define anything different.

For the above explained reasons and to stick to the principles that the version 1 of this solution shall be delivered as soon as possible and with as less new implementations as possible, the first release will be based just on the trust framework established by the EESSI-IR and the Bridge service will expose to the internet just the relevant data needed to verify the digital attestation, without the definition of a federated trust.

In a second moment, when the consortia will have defined the eIDAS 2.0-compliant trust framework, the back-end of this solution will be modified to adapt to it, when the same changes will be needed to use the EUDI wallets, so not duplicating the needed costs at MS level.

These changes will be transparent for the end users, as the user journeys will be exactly the same, as what is going to change are the mechanisms behind the scenes.

10.3 Bridge definition

This paragraph describes the functionalities and details of the Bridge service that will expose the needed (non-personal) data from the EESSI-IR to the Internet.

The Bridge implementation falls under the responsibility of the European Commission and further details of its implementation will be defined at a later stage.

Some details on the way the Bridge will be working and what data it will expose are mentioned in the introduction to section 9.

11 Format of the digital credential document

This section will describe the final look of the digital credential, as downloaded by the citizens.

TARJETA SANITARIA EUROPEA
EUROPEAN HEALTH INSURANCE CARD

ES

3. Apellido(s)
LOPEZ POTES

4. Nombre(s)
MONICA

5. Fecha de nacimiento
04 / 03 / 1993

6. Numero de identificacion personal
1234567890

7. Numero de identificacion de la institucion
2800 - INSS MADRID

8. Numero de identificacion de la tarjeta
9865789656DGGTRSAG4T

9. Fecha de expiracion
15 / 06 / 2025

10. Fecha de emisión
29 / 05 / 2024

11. Fecha de inicio
15 / 06 / 2020

[ISSUER'S LOGO]
[ISSUER'S NAME]
[Issuer's information]

La autenticidad, integridad y fecha de vencimiento de este documento se pueden verificar escaneando el código QR con la aplicación de verificación específica.

European Union

Figure 17 - Possible layout of the PDF in A4 format (Spanish version)

The fields are numbered from 1 to 11 to allow an easy recognition of every field, as the numbers will be identical from country to country, despite the fact labels will be in the issuing Member State official language.

The plastic card does not have fields 10 and 11, but the numbering appeared to be logical, as last field was marked as "9".

To overcome the possibility that a clerk of a foreign HCP has issues identifying the correct human-readable data in the PDF, as not understanding the language used for the entitlement document labels, we could foresee to have a second page of the document containing the translation of all the fields in the 27+5 languages of the countries using the EHIC.

12 Verification APP

This section will describe the functional specifications of the verification application, following its business requirements defined by the business working-group.

The verification app will be released as mobile app and as web application.

12.1 Business requirements

The table hereafter lists the business requirements of the future application for the verification of the electronic EHIC/entitlement document, as described in section 3 of the document.

Business requirement	Description
Validity, integrity and authenticity	The verification app must provide the possibility to check the validity (i.e. document has not expired), integrity and authenticity of the electronic EHIC/entitlement document online and in real-time to relevant actors, like healthcare providers, competent institution.
Offline usage	The verification app must be able to work offline when verifying the validity and authenticity of the electronic EHIC/entitlement document by authorised users.
electronic EHIC/entitlement document verification	The verification app must clearly provide the result of the verification of the electronic EHIC/entitlement document of the insured person to relevant actors, like healthcare providers and competent institution.
Export of information from the electronic EHIC/entitlement document	The verification app must provide the possibility to authorised users to extract the electronic EHIC/entitlement document dataset, and possibility to prove the fact that the digital EHIC dataset has been read when the document was presented, in order to prove the entitlement to access health care (i.e. print the information, send the information as attachment to an email with the information about time (date) when information was stored, reuse the digital information for future proof in reimbursement).

Internationalisation	The verification app must provide to the user the possibility to switch language when displaying the electronic EHIC/entitlement document data.
-----------------------------	---

12.2 Validity of the VC

A verification of the VC will result positive if all the following checks will result positive:

- the VC has been issued by a recognised/valid institution;
- the Issuer was entitled to issue the EHIC **at issuance date**;
- at issuance date**, the Issuer certificate was valid, i.e. the signature was valid compared to the digital certificate at issuance date and the certificate was not revoked. This means that the verifier shall be able to verify attestations having an expired Digital Signature Certificate;
- the data has not been tampered with, i.e. the hash of the decrypted payload is equal to the encrypted hash;
- the expiration date is not before **the treatment date**;
- all the dates respect the checks defined in paragraph “**Error! Reference source not found.**Business rules for dates”;
- all the other fields respect the constraint specified in section 0;
- the VC conforms to the specific predefined schema (i.e. the one specified in section 66).

Here below, the timeline defines an easy example of valid verification of the VC.

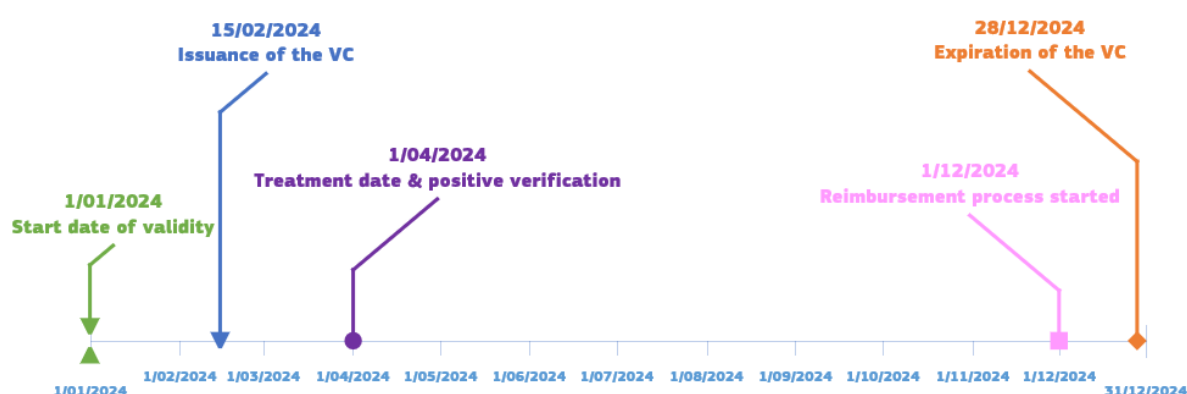


Figure 18 - Simple positive verification check of the electronic EHIC/entitlement document

Just to depict a complex example, taking in consideration different potential exceptional situations, the timeline below represents a positive result of the check, whenever it is performed, even when the VC has expired, the Issuer certificate has changed and the Issuer is not entitled to issue an EHIC anymore, as **the reference date for the control will always be the date of treatment**. For this reason, the verification app will require the Verifier to fill in the only information that is missing to

perform these checks, i.e. the treatment date, which is not obviously part of the data available in the QR-code.

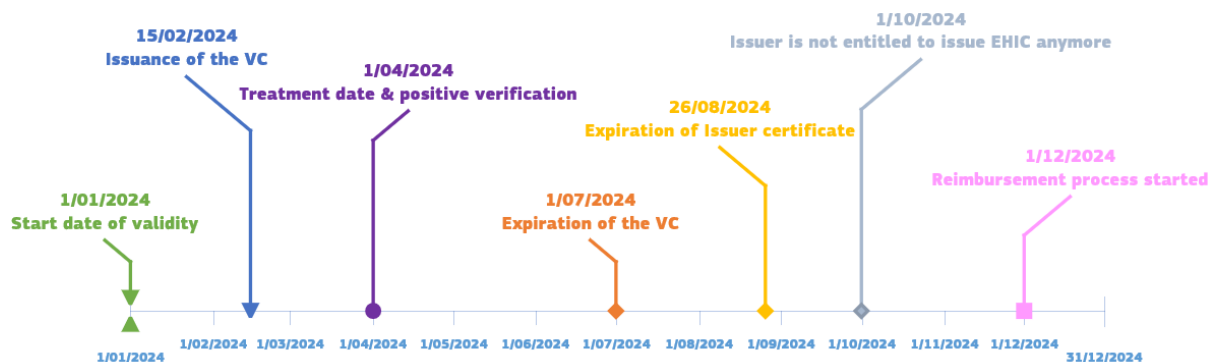


Figure 19 - Complex positive verification check of the electronic EHIC/entitlement document

The ecosystem needs to provide sufficient information concerning the validity of the electronic EHIC/entitlement document at the treatment date during the whole period that the reimbursement process from the HCP is still possible. One way to achieve this is to provide access to the historical context of all the digital credentials of the Issuers.

12.3 Verification of the QR-code

This paragraph describes how the verification of the QR code can guarantee that the electronic EHIC/entitlement document has not been tampered with

After having scanned the QR-code, the verification app unpacks the read content to retrieve the electronic message and the digital signature it contains.

Afterwards, it calculates the hash of the read 'electronic EHIC/entitlement document' data and compares it against the decrypted hash of the digital signature: if these two are the same, the document has not been tampered with.

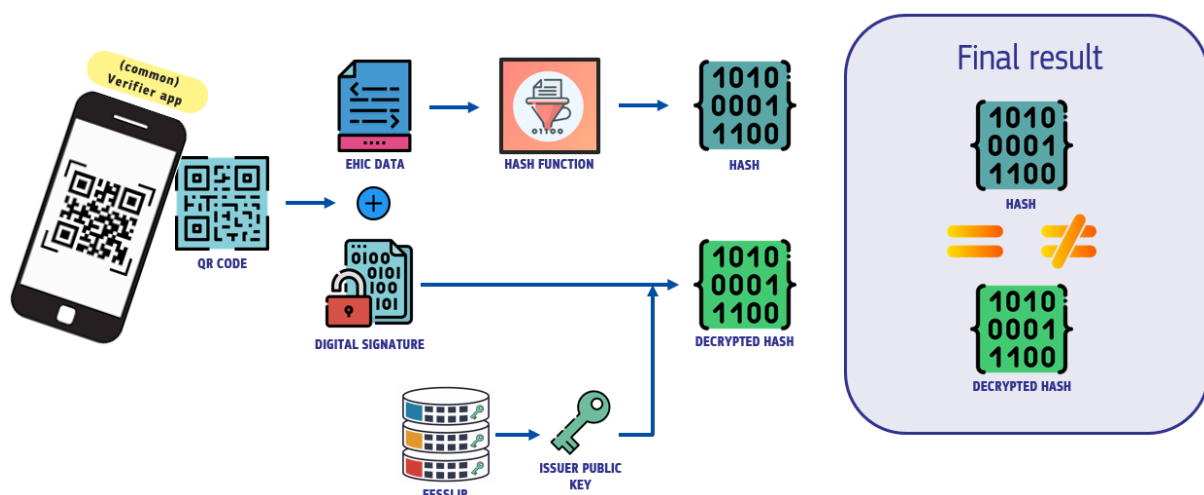


Figure 20 - Exemplification of the integrity verification of the QR code

12.4 Export data interface

This section will describe the data and the data format of the export interface of the verification app, which will allow HCPs to automatically retrieve data from the scanned QR code and get a proof of the fact the VC has been checked.

Even for the verification app, we are suggesting a 2-step approach, where version 1 will not change the way the Verifier (Health Care Provider) is used to see the data, while version 2 provides a change also in the visibility of information for this stakeholder.

Version-1

The first version of the verifier app will allow the Verifier to:

- export the read data in a human-readable format, i.e. export the PDF, as presented by the citizen, housing both the human readable data and the QR code;
- export the entitlement data in machine-readable format, i.e. JSON, in the same format defined in section 6, or CSV (Comma Separated Values);
- export a human-readable proof of the performed check of the VC with verification date and its result in PDF format. This PDF can be kept in the HCP dossier for future reference during the reimbursement process.

Some practical examples

This paragraph will provide a couple of hypothetical examples about how the read data can be exported from the verification app and imported into the HCP system. Obviously, there are thousands of different systems in the real world, each one with their own peculiarities, so these examples do not represent a comprehensive set of suggestions, but have just the aim of explaining the basic concepts described above.

We stress the importance to **take into account data protection implications when copying and moving exported data** from a device to its final storage destination. This section does not go into details for this aspect, as the various scenarios will depend on the set-up of each HCP.

Use of the verification app through a browser installed on a desktop computer

- 1) The citizen, Mario, reaches the HCP desk to register for unforeseen healthcare and provides his ID card and shows the pdf from his smartphone;
- 2) The clerk, Daisy, has a browser open on her desktop computer and easily browses to the verification app URL, which is bookmarked in her favourites;
- 3) Daisy scans the QR code in the pdf with a webcam or any other reading device connected to her desktop computer;
- 4) Daisy fills in the current date as “treatment date” and clicks on the “Verify” button in the verification app;
- 5) Daisy can see on the screen whether the checks returned a green status, i.e. everything is OK with the verified credentials, or a red one, i.e. there is an issue with the presented credentials;

In case of green status

- a) Daisy checks that name and surname on the provided ID document match with the ones verified and that are displayed **on the screen** (coming from the QR code and not the ones on the pdf itself, which could have been modified);

If name and surname do not match, the document is refused, as Mario is not the person covered by the EHIC.

If name and surname match, the document is accepted, as all the checks provided positive results.

- b) Daisy downloads a proof of the verification and stores it in the HCP folder related to Mario’s dossier;

- c) Mario, if he wants, will be able to download its own proof that its EHIC was checked positive by the validation app that specific day. It is important to underline that this proof certifies that the entitlement document is valid at the moment of treatment and not that was checked by the HCP. This would not be possible, as we do not have a verifier list for the moment, but it will be added in the version 2 of this solution;
- d) Daisy downloads the EHIC data in the form of CSV or JSON and stores it in the HCP dedicated folder for import/export. If needed, she can rename the CSV file, as needed by her organisation, in case any match needs to be done with the treatment;
- e) Mario can proceed with his needed treatment;
- f) The HCP has different ways to inject the data into their internal system:
 - Daisy goes into her HCP system, reaches Mario's dossier, clicks on the import button and selects the export data she saved at step d). The data is read, parsed and injected into the system;
 - the HCP set up a routine job, which every night automatically scans the dedicated folder for import/export, it finds the new file related to Mario's EHIC, and manages it, reading the data in the file, parsing them and storing them in the HCP internal system.

In case of red status

- A. Daisy sees the errors at screen and communicate them to Mario;
- B. The document is refused, as some of the checks did not pass the verification.

Use of the verification app through a smart device

1. The citizen, Rosalinda, reaches the HCP desk to register for unplanned necessary healthcare treatment and provides her passport and shows a printout of the pdf;
2. The clerk, Luigi, opens the verification app on his smartphone;
3. Luigi scans the QR code on the piece of paper with the verification app, fills in the current date as "treatment date" and clicks on the "Verify" button;
4. Luigi can see on the device whether the checks returned a green status, i.e. everything is OK with the verified credentials, or a red one, i.e. there is an issue with the presented credentials.

The rest of the example is exactly the same as the one described before, the only difference is that the import/export folder where to store the exported data needs to be reachable from the mobile phone where the verification app was executed, e.g. it could be a safe place on the HCP intranet or website, or the file can be stored on the device itself and downloaded on the local computer at the end of the day, or as soon as the Luigi has completed the management of Rosalinda's acceptance.

Version-2

The second version of the verifier app will potentially not allow the Verifier to download the personal data of the holder of the VC. It could allow the Verifier to:

- export a human-readable proof of the performed check of the VC with verification date and its result in PDF format, simply mentioning the VC ID and not all the data contained in the digital document. This PDF needs to be digitally signed too by the Verifier. Such proof can be useful for both the citizen and the HCP for the reimbursement phase;
- export the digital document ID in a machine-readable format, i.e. JSON (format to be defined), or CSV.

Further details on this version 2 of the verification app can still be defined/refined at a later stage, following the evolvement of the digital EHIC pilots using EUDI wallets.

12.5 The verification process

The process for the verification of the EHIC by healthcare providers (Verifiers) is explained hereafter:

1. the Verifier requests the electronic EHIC/entitlement document and an identification document (e.g. ID card, passport) to the citizen;
2. the Holder provides the PDF containing the QR-Code to the Verifier;
3. the Holder provides an identification document to the verifier;

Manual verification (in case HCP does not want to use the verification app).

This process is the same as today.

We do not recommend at all this approach, as a pdf can be easily forged, so verification is fundamental to avoid frauds.

4. the Verifier checks the identity information on the PDF and whether it matches against the information on the Holder's identity document;
5. the Verifier checks the content of the PDF to ensure that the Holder can benefit from the healthcare treatment;
6. the Verifier persists the content of the PDF (through photocopying, picture or email) for later use (i.e. reimbursement process).

Automatic verification with the verification app.

4. the Verifier uses the verification app to scan the QR-code on the PDF;
5. the Verifier checks the feedback and result provided by the verification app (i.e. valid or not valid and, in the latter case, for what reasons);

6. the Verifier checks the identity information on the PDF and matches it (manually) against the information on the Holder's identity document;
7. the Verifier persists the content of the PDF/QR-code for later use (reimbursement process) either downloading a copy, or exporting the data into its updated system, capable to read the format exposed by the verification app;
8. the Verifier downloads the proof of verification and keeps it in its digital or physical archive and shares it by email with the Holder for future reference, if needed.

12.6 Offline verification

The offline verification is the process of verification of the entitlement document by means of the verification app without the availability of an active internet connection.

The verification process is explained in paragraph 12.2.

It is worth highlighting that the business information about the electronic EHIC/entitlement document, e.g. holder's name, issuance date, expiration date, are stored directly in the QR-code. As such, the electronic attestation data can be retrieved simply by scanning the QR-code, without the need of any internet connection. As a result, the steps d), e), f) g) and h) of the verification process can be easily automated in full offline mode.

Nevertheless, steps a), b) and c) require that the verification app retrieves the cryptographic material from the EESSI Institution Repository, in order to check that the digital certificate used to sign the entitlement document (1) belongs to a trusted Issuer, (2) the Issuer is authorised to issue EHIC documents, and (3) the Issuer's certificate was valid at issuance time. Ideally, the verification app should download the cryptographic material from the Institution Repository upon every verification made. However, this approach would require an active internet connection to carry out the verification process. To overcome this problem, the verification app may download the necessary cryptographic material (snapshot) at regular intervals, e.g. every night, and store it locally. This would allow the verification app to work completely in offline mode, including when checking the trustworthiness of the issuer's digital certificate.

Nevertheless, it must be highlighted that caching the cryptographic material locally in the verification app may generate a situation whereby the certificates stored locally are not synchronised with the ones stored in the Institution Repository. Please check the examples below. We need to underline that the Exceptional situation depicted below is really rare to happen, as we do not expect long time of internet unavailability and certificates in EESSI-IR have a lifespan of years.

By the way, it is fundamental to stress that the "Exceptional situation" can cause **just false negatives** and **never false positives**, so there are no risks for the reimbursement process.

Normal situation <i>Local cache and Institution repository synchronised</i>	Exceptional situation <i>Local cache and Institution Repository out-of-synch</i>
<ol style="list-style-type: none"> 1. The verification app downloads the latest snapshot of the certificates on day X 2. The internet is not available on day X+1 and X+2 (latest synchronisation done on day X) 3. A patient shows the electronic EHIC/entitlement document on day X+2 for a EHIC issued a week earlier 4. The (offline) verification of the EHIC is successful, as the certificate in the cache is the one that was used to issue the shown electronic EHIC/entitlement document 	<ol style="list-style-type: none"> 1. The verification app downloads the latest snapshot of the certificates on day X 2. The internet is not available on day X+1 and X+2 (latest synchronisation done on day X) 3. An issuer changes its certificate on day X+1 and issues an electronic EHIC/entitlement document to a patient (this certificate is not in the verification app cache, as it has no internet connection since day X) 4. The patient shows the electronic EHIC/entitlement document on day X+2 5. The (offline) verification of the EHIC fails, as the app does not recognise the certificate of the issuer

To be complete, and to avoid risks of fraud, further **business** discussions need to take place to understand how to behave in situations where there is a prolonged internet disconnection.

To overcome the situation where the data downloaded by the verification app becomes probably obsolete, the verification app should connect to the internet to download the latest version of the necessary cryptographic material as often as possible, e.g. every night.

There is a need to define in a later stage for how many days the verification app can be disconnected from the internet and, consequently, the digital certificates in the cache not being synchronised.

12.7 Evolution towards the final EUDI solution

The first release of the verification application will deal exclusively with the use of electronic attestations (e.g. the electronic EHIC/entitlement documents) and will not

foresee any interactions with digital wallets. A electronic attestation represents, in a digital format, the same information that a physical credential (e.g. the plastic EHIC) represents. The addition of digital features, such as digital signatures, makes the proposed solution more tamper-evident and more trustworthy than its physical counterparts. In its first release, the verification application will be able to scan a QR-code containing the electronic attestation in its entirety, representing the EHIC.

With the evolution towards the EUDI solution, the verification application may rely on the use of Verifiable Presentations. A Verifiable Presentation is similar to a Verifiable Credential, but it contains data derived from one or more Verifiable Credentials, issued by one or more Issuers, that is shared with a specific Verifier. As an example, the EHIC Verifiable Presentation may contain information about the EHIC itself combined with the information about the identity of the Holder issued by another trusted party, e.g. population register. By relying on Verifiable Presentation, the final solution of the EHIC verification app may be able to also verify the identity of the Holder of the EHIC.

12.8 Authentication and access

Version 1

In terms of authentication and authorisation of the users, in its first release the verification app may be developed so that no registration is required, like it was happening for the COVID-19 verification app.

Nevertheless, the lack of registration and, consequently, of authentication would not allow the verification app to store audit logs, e.g. which verifier performed a verification and when. As the verification process provides a proof of the happened verification, we so not consider this is as a needed feature.

In case there should be the need to overcome this limitation, the first release of the verification app may include a basic identity and access management module to guarantee that only authenticated verifiers can use the verification app, and to store the audit logs about operations that may be used later, e.g. during the reimbursement process.

It is important to stress, for clarity reasons, that, in case this latter choice is undertaken, anybody could be able to create an account to use the verification app and use it, so the application would not provide any sort of regulation of the accesses.

HCPs will be able to choose between creating one single account for their institution, or one account for each clerk who will need to use the app for verification tasks.

Version 2

When moving towards the EUDI Wallet ecosystem, the access to the verification app may be managed through the use of trusted list of verifiers. In this case, the verifiers allowed to use the verification app will be stored in a trusted list, and the use of the verification app will be granted just based on the identity binding of the verifier.

12.9 How the verification app will be deployed/released?

During previous discussions in the AC, several Member States underlined the inefficiency to implement twenty-seven (plus five) different verification applications performing the same tasks.

Starting from this position, the EC is in favour of providing a support in the definition and implementation of the verification app.

Different models can be foreseen, but the EC strongly suggest the release of the verification app as open-source code:

- the EC to provide a reference architecture and then each MS to implement, maintain and run its own verification app;
- the EC to provide a reference architecture and then to find a common third party to implement it in open-source form and run and maintain it;
- the EC to provide a reference architecture and the initial open-source code and find a common third party to maintain and run it.

The Ad hoc group suggests the third option, to be sure to have a reliable and working starting point and then to delegate to a third party the maintenance, evolution and operative tasks. In this case, a clear service level agreement (SLA) shall be defined.

Providing the code in open-source fashion will imply yearly review cycles to decide which improvements to apply to the code, in function of feedback received. There is the need to decide who will be responsible for that task.

12.10 Verification app visuals

Some exemplificatory mock-ups of the screens of the Verification app (mobile app version) have been added in a dedicated Annex VI – Possible screens of the Verification app.

13 Data protection and other legal considerations/requirements

This section provides a first high-level assessment of data protection aspects. Further analysis will need to be carried out also depending on different implementation choices

The solution and all relevant data processing operations need to comply with the EU data protection legal framework ([Regulation \(EU\) 2016/679](#) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, General Data Protection Regulation, GDPR and – if applicable - Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies).

The **legal basis for the data processing** is Article 6(1) c of the GDPR which provides that processing is “necessary for compliance with a legal obligation to which the controller is subject”.

The **purpose of the data processing** is to ensure compliance with EU social security coordination regulations, and in particular with the obligation of a Member State to provide insured persons temporarily staying outside their competent Member State with the benefits in kind which become necessary on medical grounds during their stay. These benefits shall be provided as if the persons were insured in the Member State of stay. The solution would allow:

- insured persons seeking necessary healthcare abroad to easily prove their entitlement to receive such benefits;
- healthcare providers in the country of stay to verify online and offline the authenticity and validity of the entitlement document of the persons seeking necessary healthcare abroad;
- healthcare providers and competent institutions in the involved Member States to exchange the relevant information for the reimbursement process.

In the context of the digitalisation of the EHIC, the dataset present on the electronic entitlement document will be almost the same as the one available on the physical EHIC card. Personal data will not be stored at central level and will be made accessible only to authorised users (e.g. healthcare providers, social security institutions etc). Trusted parties will not be allowed to use the data for other purposes (**purpose limitation**).

Only a limited amount of data is processed, and it is only used for the specific purpose for which they are processed, in line with Articles 5(1) (c) of the GDPR (**data minimisation**).

To check online and offline the authenticity of the document (i.e. whether the document was issued by an authorised institution) no personal data will be processed. Only

information related to the institution/ the attestation itself will be checked. Personal data will be transferred by healthcare providers to the social security institution for reimbursement purposes in cases covered by the social security coordination regulations.

The solution meets the requirements of the principles of **necessity and proportionality**. Only information is processed that is reasonably and strictly necessary for the proper functioning of the solution and in a manner that is proportionate and does not impact the rights and freedoms of the relevant data subjects more than necessary.

The **data subjects** (i.e. persons whose personal data are collected, held or processed) are insure people temporarily staying outside the competent Member State requiring unplanned necessary healthcare treatment.

Special categories of data (sensitive) under Article 9 of the GDPR, e.g. data concerning health, are not involved in the processing activity. Additional information, including sensitive data may be requested at a later stage during the reimbursement process, but this falls under the 'EESSI data protection agreement'.

Personal data held is kept accurate and up to date (**accuracy**).

Security measures for the protection of personal data should be adopted for each processing operations.

The roles and responsibilities of the various actors (i.e. controllers and processors) should be clearly defined.

14 Annex I – example of creation and validation of a JWT for electronic EHIC/entitlement document

This annex will show an example of how to transform some EHIC data into JWT.

14.1 Digital credential data

Name and given names: Jean-Pierre, Frédéric Clément-Lafarge

Date of birth: 2000-02-29

Personal Identification number: 0001019999

Identification number of the institution: 0216X

Name of the institution: LAMUTUALITENEUTRE

Card identification number: 021XXXXXXXX2023035407

Card issuer Country: BE

Entitlement start date: 08-02-2023

Expiry date: 29-02-2024

Date of issuance: 31-01-2024

14.2 CREATION OF THE JSON

Version 1

```
{
  "ic": "BE",
  "hn": {
    "fn": "Clément-Lafarge",
    "gn": "Jean-Pierre, Frédéric",
  },
  "dob": "29-02-2000",
  "hi": "0001019999",
  "ii": "0216X",
  "in": "LAMUTUALITENEUTRE",
  "ci": "021XXXXXXXX2023035407",
  "sd": "28-02-2023",
  "ed": "29-02-2024",
  "id": "31-01-2024"
}
```


Version 2

```
{
  "ic": "BE",
  "hn": {
    "fn": "Clément-Lafarge",
    "fnt": "CLEMENT<LAFARGE",
    "gn": "Jean-Pierre, Frédéric",
    "gnt": "JEAN<PIERRE<FREDERIC"
  },
  "dob": "2000-02-29",
  "hi": "0001019999",
  "ii": "0216X",
  "in": "LAMUTUALITENEUTRE",
  "ci": "021XXXXXXXX2023035407",
  "sd": "2023-02-28",
  "ed": "2024-02-29",
  "id": "2024-01-31"
}
```

14.3 Creation of the JWT

Version 1

```
{
  "iat": 1706194800,
  "nbf": 1706194800,
  "exp": 1737817200,
  "sub": <identity of issuer>,
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://w3id.org/vc/status-list/2021/v1"
    ],
    "type": [
      "VerifiableCredential",
      "VerifiableAttestation"
    ],
    "credentialSubject": {
      "ic": "BE",
      "hn": {
        "fn": "Clément-Lafarge",
        "gn": "Jean-Pierre, Frédéric"
      },
      "dob": "29-02-2000",
      "hi": "0001019999",
      "ii": "0216X",
      "in": "LAMUTUALITENEUTRE",
      "ci": "021XXXXXXXX2023035407",
      "sd": "28-02-2023",
      "ed": "29-02-2024",
      "id": "31-01-2024"
    },
    "credentialSchema": {
```

```

        "id": "https://api-pilot.ebsi.eu/trusted-schemas-
            registry/v3/schemas/0xfa899fd2bc2a5a66ad51f9881813401ebe02f7dd40
            b0926c3e49c9514a77cb6a",
        "type": "FullJsonSchemaValidator2021"
    }
},
"iss": <identity of issuer>
}

```

Version 2

```

{
  "iat": 1706194800,
  "nbf": 1706194800,
  "exp": 1737817200,
  "sub": <identity of issuer>,
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://w3id.org/vc/status-list/2021/v1"
    ],
    "type": [
      "VerifiableCredential",
      "VerifiableAttestation"
    ],
    "credentialSubject": {
      "ic": "BE",
      "hn": {
        "fn": "Clément-Lafarge",
        "fnt": "CLEMENT<LAFARGE",
        "gn": "Jean-Pierre, Frédéric",
        "gnt": "JEAN<PIERRE<FREDERIC"
      },
      "dob": "2000-02-29",
      "hi": "0001019999",
      "ii": "0216X",
      "in": "LAMUTUALITENEUTRE",
      "ci": "021XXXXXXXX2023035407",
      "sd": "2023-02-28",
      "ed": "2024-02-29",
      "id": "2024-01-31"
    },
    "credentialSchema": {
      "id": "https://api-pilot.ebsi.eu/trusted-schemas-
          registry/v3/schemas/0xfa899fd2bc2a5a66ad51f9881813401ebe02f7dd40
          b0926c3e49c9514a77cb6a",
      "type": "FullJsonSchemaValidator2021"
    }
  },
  "iss": <identity of issuer>
}

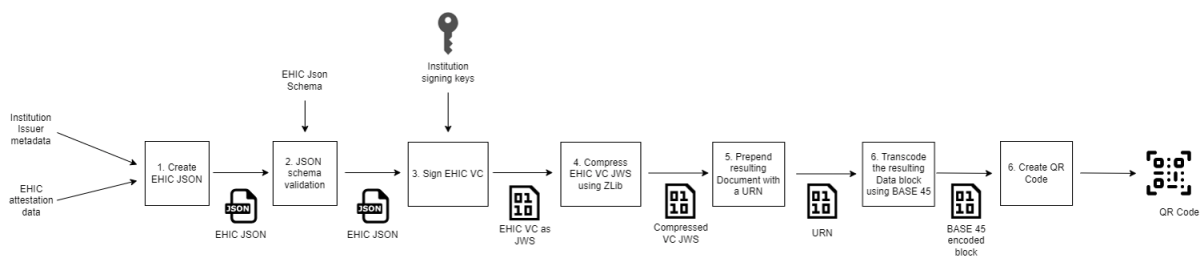
```

15 Annex II – example of creation and validation of a PDF with QR code from JWT

This annex will show an example of how to transform the JWT into a QR code and then append it to a PDF.

In this annex just version 1 is exemplified. The only differences linked to version 2 are related to the new introduced fields and changes of data formats (see paragraph 3.6).

Process overview:



Note: in version 1 we will skip the URN.

15.1 Step 1 and Step 2 (a schema compliant EHIC JSON payload.)

For the first step, we assume that the issuer will be able to create a compliant JSON containing the Institution Issuer metadata and the electronic EHIC/digital entitlement attestation data.

As example we will use the following JSON data for a non-existing artificial person:

```
{
  "ic": "BE",
  "hn": {
    "fn": "Clément-Lafarge",
    "gn": "Jean-Pierre, Frédéric"
  },
  "dob": "28/02/1900",
  "hi": "0001019999",
  "ii": "0216X",
  "in": "LAMUTUALITENEUTRE",
  "ci": "021XXXXXXXXX2023035407",
  "sd": "28/02/2023",
  "ed": "29/02/2024",
  "id": "31/12/2099"
}
```

15.2 Step 3: A Signed JSON Webtoken (JWS).

The resulting JWS (1562 Bytes):

A resulting translation from JWT.io

```
{
  "iat": 1706194800,
  "jti": "did:ebssi:zzmXyldyg4o8RJNEM5zgZRK",
  "nbf": 1706194800,
  "exp": 1737817200,
  "sub": "did:ebssi:zZGoWffutnqpELZA17Voofh",
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1"
    ],
    "id": "did:ebssi:zzmXyldyg4o8RJNEM5zgZRK",
    "type": [
      "VerifiableCredential",
      "VerifiableAttestation"
    ],
    "issuer": "did:ebssi:zZGoWffutnqpELZA17Voofh",
    "issuanceDate": "2024-01-16T08:10:52.500Z",
    "issued": "2024-01-16T08:10:52.500Z",
    "validFrom": "2024-01-16T08:10:52.500Z",
    "expirationDate": "2024-01-16T08:10:52.500Z"
  }
}
```

```

"credentialSubject": {
  "ic": "BE",
  "hn": {
    "fn": "Clément-Lafarge",
    "gn": "Jean-Pierre, Frédéric"
  },
  "dob": "28/02/1900",
  "hi": "0001019999",
  "ii": "0216X",
  "in": "LAMUTUALITENEUTRE",
  "ci": "021XXXXXXXXX2023035407",
  "sd": "28/02/2023",
  "ed": "29/02/2024",
  "id": "did:ebssi:zZGoWFfutnqpELZA17Voofh"
},
"credentialSchema": {
  "id": "https://api-conformance.ebssi.eu/trusted-schemas-registry/v2/schemas/z6HkKUAhWgMQqGQEcc1kewTWJrY4nrtadncmid7hsfGV8",
  "type": "FullJsonSchemaValidator2021"
},
"iss": "did:ebssi:zZGoWFfutnqpELZA17Voofh"
}

```

15.3 Step 4: the ZLIB compressed Payload

The JWS will then be compressed using ZLIB (rfc1950),

(<https://datatracker.ietf.org/doc/html/rfc1950>).

Note: this rendering of a ZLIBBED file is not correct, as the ZLIB file is a binary which will result in dataloss when putting it in a document. Input file: 1562 bytes, Resulting output file : 936 Bytes.



zlibbed.zlib

The Zlibbed intermittend data.

15.4 Step 5: The Identification URN added to the Payload.

Not in version 1.

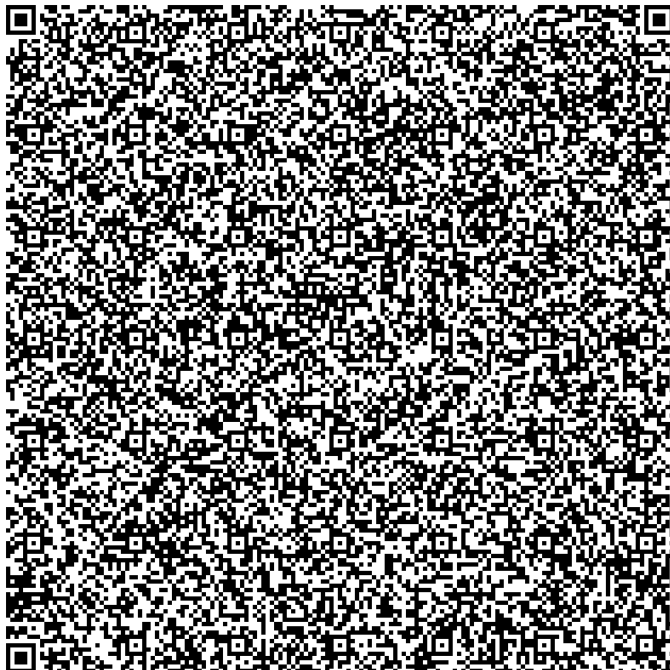
15.5 Step 6: The BASE 45 transcoded Payload.

IN order to make the binary file of the compression usable for QR Code transformation - ALPHA the character space should be alphanumeric, as with the healthcard and recommendatin for creating QR codes we use base-45 encoding, this will increase the document size again a bit.

Input file: 936 bytes, Resulting output file : 1404 Bytes.

6BFN*IXMR1SJIT2FNK680R-RY39DS5I+8132658X85FCPJ-
A2WJUWTVIT2V9/TUG0GY25NVE6NEJ:Q/8V0+PGVL5TUWQMYH50+RTVRJX7*PNK6N5A6YQPM2FMW
FQ3F09ESZM*-1HGQ5Q2O3HT\$ESV5R+FAV5\$7B\$Y9B:SW4LRVLPLR
ACNB2W4N2ZALZS*S71PKU80LEDUOTYXI3*2QNT4.T 99KE48S3UR519UWW1%3O15C8TM\$LIH
L1UR\$60KFJUP3YL03BI8YG2-8.9A/4D3 QKM835C\$52O3SU-D*YG GTJ\$T/-DA-
AXBTF/D6/J\$JCA105I9OG3-7GQUR6LP29P0TUQDGVHFIIT/MJ\$7KWK5HKHETAD6GSF8S
1X5IP*DZAOX%A571XLV9/TKPVBM57PV+9B:N4PHFUAOHN4Y4J8MRTX5KIT0CEYF6KHGQEL4H5F2
PQ*CNSRK.8SDV1FFKOH*9W+KL4C3S:PI:SU3NNFA1GT:3PM9QB82:XUNWTSRM\$RQ\$2Q6WSYGCP\$
H667E:G6KPD4MFI9D2DP4VMEUSJ6P0LUYH%POOBL796*KJY-VV04
+KBXEZ2O+%RFUJ8TK21MLZVGL5:HJGJGFWAZLF3T8LH9UYDD9D943/3F
QDDVFBY7RNF6713THN4AKI9K%BMBPC*SDP9W4L4S5C:3SPJN/FQUC54MC7QO%936CH6M TDQ-R-
RE3B5DQFP9VS%A0.JA%KYGUU1INGUK3A5*T-Y39GGC.RO3T3DJD 732P0NCS90WC6Q
E4SNMZ7KBE\$*N-XJP:O /O+YR:3V3NAFWSSC6.JJ28IABE 503*0%-
B7:JMA3IX7\$ML0GCV*PUNKLO6K/K2RM.4E\$JRY8KWG1UTI/39+X026WB%N./P
%59TDJOHB39%2J/RR:4VUSCN.2W6JQ2SZ3N*DL8GAJ7JKNDA10EUJ.141XMZZIQ8F9
RV58NTAT+D-NH2:ILQKPZI221FSJ6MMQAIC/9/*5G:TI2BKCOY%2610U5CP-
5.+E8UHB7V*\$UEPC6DWD38JAFZWVAJR.9W7BUMO5JXH:XRT+FJ5P777*A6Z2MHAMZNC1JLO4LS-
JY:LO2JP99%GMR1ID5W8:PR*PD+P 7SHS7O6\$\$PE%AR:538TQXFAZ12BL7VPN1H0KVDSL-
B7.4KPYVX*MHPI4%7VK8\$WC\$7GLCNBSALO62IT+DVA+S2.B-
ZL6CK*+59A5YCEIZDAO52D50XEXLF*05:CMVW3E0A/5JT0EYEP:N3TX5V:A4X5\$2V2N9F7G46LF
:0STP*4EAL5.*A8HHGIADV781AQCWM/1QJ0G28Y6N0QRDNLENBLFC01*9K
JP5TEJUOXRUAQ066CM5Q3NL0.NH26V8RF2AGOK63GO2GM14CU2

15.6Step 6: The encoded QR Code.



16 Annex III – example(s) of processes to manage the PKI

If needed, this annex will be populated with some examples on the way PKI is managed

17 Annex IV – Governance of Identities using EESSI-IR

This annex will describe the journey of becoming a trusted issuer from the moment that a new institution which is not in EESSI-IR to the moment it can issue credentials

18 Annex V - Key Identifier algorithm

This annex will clearly describe the algorithm used to generate the KID from the X509 certificate used by the Issuer, and which contains the public key used to decipher the signature of the electronic EHIC/entitlement document. This KID will be registered in the Federated Trust Store as part of the identity of the Issuer

19 Annex VI – Possible screens of the Verification app

The screenshot shows a mobile application interface for document verification. At the top, the status bar displays the time 9:41, signal strength, Wi-Fi, and battery icons. Below this, the URL 'organisation-webapp.com' is visible. A purple header bar contains the text 'Sample application for verification purposes in the context of the ESSPASS pilot project'. The main header area includes a back arrow, a 'VERIFY' button with a checkmark icon, and a user profile icon labeled 'JD'. The main content area has a large heading 'Select verifiable document' followed by a paragraph: 'Please select from the dropdown list below the type of document that you would like to verify.' There are two input fields: a dropdown menu currently showing 'EHIC' with a downward arrow, and a date selection field labeled 'Select treatment date' with a calendar icon.


Figure 21 - Verifier selects the treatment date


9:41

organisation-webapp.com

Sample application for verification purposes in the context of the ESSPASS pilot project

←

 VERIFY

 JD


Select verifiable document

Please select from the dropdown list below the type of document that you would like to verify.

EHIC

▼

29-10-2024



Scan QR code

Figure 22 - Once treatment date is filled in, <Scan QR code> button appears



Figure 23 - The verifier scans the QR code using a webcam or the smart device

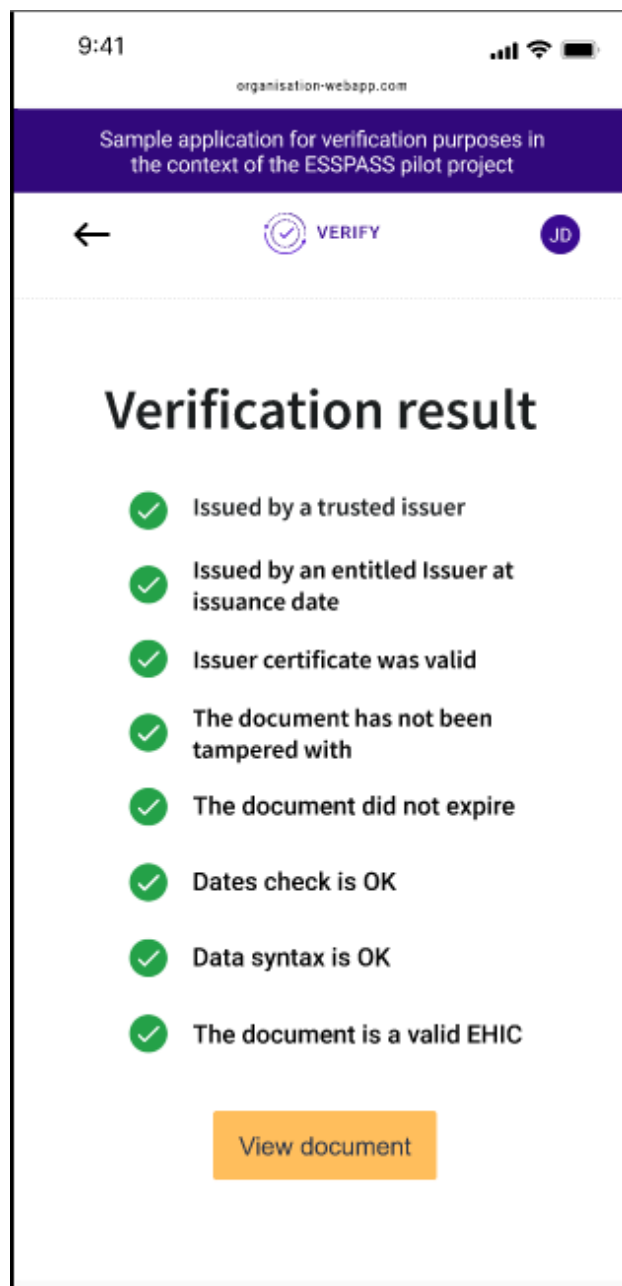


Figure 24 - The result of all the performed checks is displayed with a clear colour-code indication

9:41organisation-webapp.com

Sample application for verification purposes in the context of the ESSPASS pilot project

←

EUROPEAN HEALTH INSURANCE CARD

VERIFY

JD

Status **VALID**

Issuer 2800 - INSS MADRID

ES

EHIC

3. Names

LOPEZ POTES

4. Given names

Monica

5. Date of birth

4 / 03 /1993

6. Personal identification number

1234567890

7. Identification number of the institution

2800 - INSS MADRID

8. Identification number of the card

9865789656DGGTRSAG4T

9. Expiry date

15 / 06 / 2025

Issue date 29 / 05 / 2024

Starting date 15 / 06 / 2020

[Download in PDF](#)

[Download in CSV](#)

[Download in JSON](#)

Finish verification

Figure 25 - Verifier can see all the data on the screen and download in three different formats

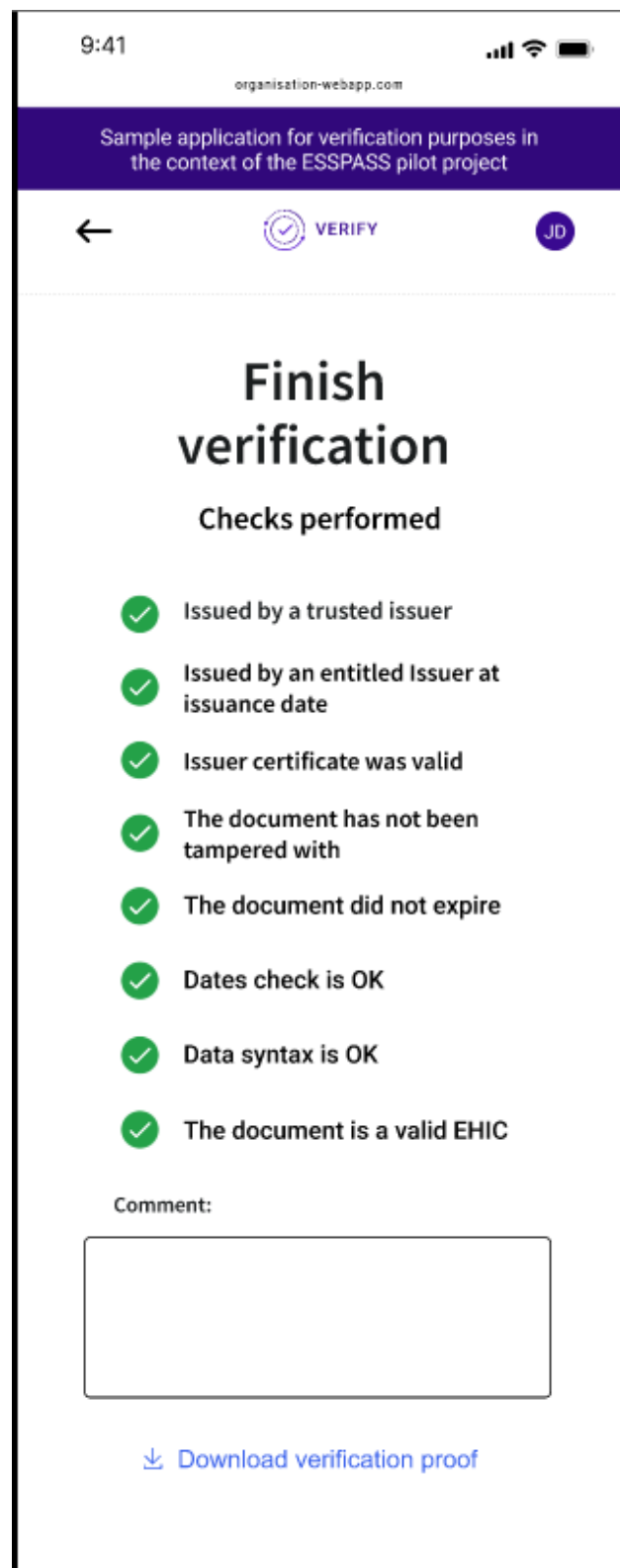


Figure 26 - Clicking on <Finish verification>, the verifier can download a digitally signed proof of verification with additional personal comments

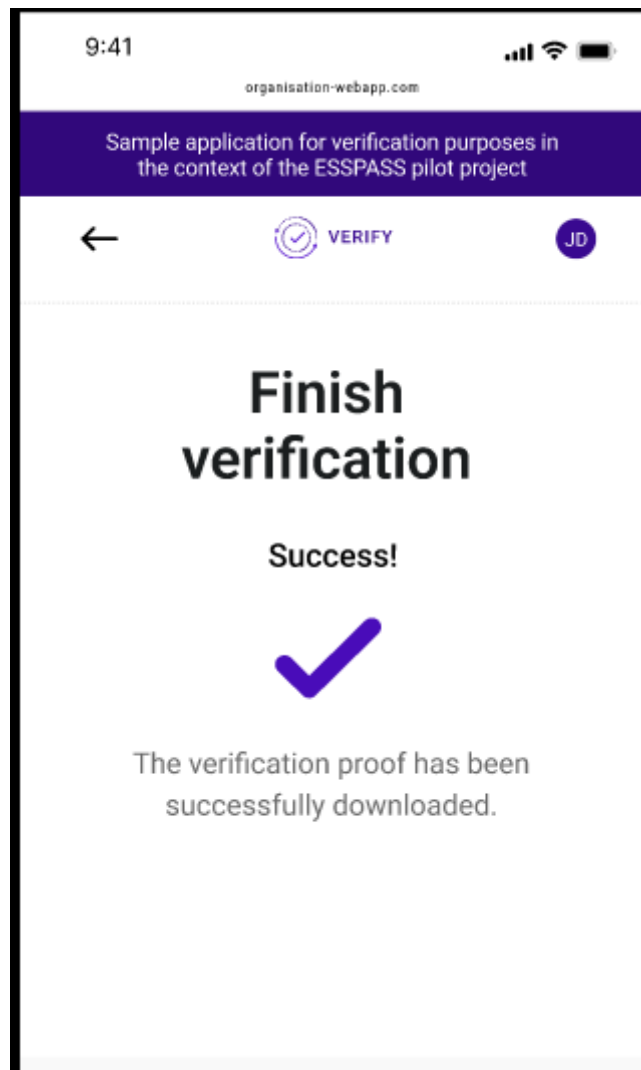


Figure 27 - End of the verification screen, after the proof of verification has been downloaded