

Data Schema for Technical Trust Framework for verifiable credentials



Contents

Document Control	4
Version History	4
1. Definition	5
2. Data schema	7
2.1 Core data vocabularies	7
2.2 Claim metadata	7
2.2.1 Provenance metadata	7
2.2.1.1 Origin	8
2.2.1.2 Provider	8
2.2.1.3 Pedigree	8
2.2.2 Accuracy metadata	9
2.2.2.1 Verifier	9
2.2.2.2 Verification method	9
2.2.3 Currency metadata	10
2.2.3.1 Last verification	11
2.2.3.2 Last refresh	11
2.2.3.3 Expiration date	11
2.2.4 Privacy Metadata	12
2.2.5 Classification metadata	12
2.2.6 Additional metadata	12
2.2.6.1 Assurance policy	13
2.2.6.2 Assurance outcome	13
2.2.7 JSON schema for claim metadata	13
2.3 Core credential types	14
2.3.1 PersonIdentity (identity credential)	15
2.3.1.1 JSON Schema for PersonIdentity	16

2.3.2 RightToWorkEvidenceCheck	17
2.3.2.1 JSON Schema for RtWEvidenceCheck	18
2.3.3 DBSStatus	18
2.3.3.1 JSON Schema for DBSStatus	19
2.3.4 ProfessionalRegistration	21
2.3.4.1 JSON Schema for ProfessionalRegistration	22
2.3.5 CoreSkills	24
2.3.5.1 JSON Schema for CoreSkills	26
2.3.6 EmploymentReference	27
2.3.6.1 JSON Schema for EmploymentReference	28
2.3.7 EnglishProficiencyTest	30
2.3.7.1 JSON Schema for EnglishProficiencyTest	30
2.3.8 Self-asserted or low trust credentials	31
2.4 Additional credential types	31
2.4.1 DBSEligibility Evidence	31
2.4.1.1 JSON Schema for DBSEligibilityEvidence	33
Appendix – NHS attribute mappings	35
Identity credential	35
Identity metadata	35
Verification outcome	36
DBSEligibility evidence	36
Right to work	37

Document Control

Key	Name	Role
Authors	ID Crowd	Subject matter experts
Approver	Phil Stradling	Architect, Transformation Directorate
Owner	Ian Townend	Chief Architect, Transformation Directorate
Reviewer	Marcus Appleton	Head of Future Workforce Solutions, Workforce, Training and Education Directorate

Version History

Version	Date	Description
1.0	22/01/2024	First final version
1.1	04/02/25	Amendment to right to work and DBS mandatory attributes

1. Definition

Alpha	A Digital Staff Passports technical alpha regarding the provisioning of access, user authentication and interoperability.
Authoritative Source	An entity that has access to, or verified copies of, accurate information from an issuing source (either itself as the issuer or another such entity). This enables other entities to confirm the validity of evidence supplied e.g., the validity of a credential.
Attribute Provider (AP)	Manages and provides assertions of attributes to other relying parties in the ecosystem.
Credential	A proof of achievement, identity, characteristic, etc.
Disintermediation	The act of bypassing the user/Holder and communication occurring directly between the Issuer and Verifier.
GPG45	Good Practice Guide 45 as published by the Cabinet Office and pertaining to the identity proofing and verification of an individual. This guidance is used as a key element of assurance to trust frameworks such as that proposed by DCMS for digital identity and is aligned with international standards such as NIST 800.63.3.
Holder	The Holder is an entity that holds and can securely share multiple credentials. The Holder may also be the Subject (see definition below).
Identity Provider (IDP)	An entity that can provide proof that an entity is who they claim to be at a recognised [by the relying parties] level of trust.
Information Security Management System (ISMS)	Information Security Management System as described in ISO/IEC 27001. An ISMS is a set of policies and procedures for the systematic management of sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.
Issuer	A participating entity in and compliant with the Trust Framework that is capable of issuing compliant credentials to a verified Subject.
Participating Entity	Any entity (e.g., an Issuer, Wallet Provider, Verifier, User or Relying Party) that operates a service or utilises credentials as part of the Trust Framework
Relying Party (RP)	An entity that relies upon credentials provided by a Holder (or other entity).
Scheme	The set of technical, operational, commercial, and compliance rules that define an identity system.
Selective Disclosure	The ability of a Holder to make fine-grained decisions about what information to share.
Service Provider (SP)	The Relying Party providing a digital service to the Subject through a user agent such as a browser or App (e.g., a Wallet).
Subject	The entity attempting to obtain and/or share credentials with other entities in the Trust Framework. Sometimes referred to as a Holder.

Data Schema for Technical Trust Framework for verifiable credentials

Trust Framework	A set of operational, business, and technical rules and associated governance to enable a group of entities (including schemes) to interoperate with an adequate level of trust.
(Trust Framework) Implementor	An organisation contracted under the Health Systems Support Framework (HSSF) to provide Digital Staff Passports or contracted specifically by an entity participating the trust framework (e.g., by an Issuer) to provide Issuer, Holder, or Verifier functionality.
Trust Framework Operator	An entity appointed by NHSX to manage the operation of the trust framework and to ensure that governance is adhered to by the participating entities.
User	In the context of this technical trust framework, User refers to the entity in control of a digital wallet acting as a Holder of verifiable credentials.
Verifiable Credential (VC)	A digital proof that can be verified independently of the issuer.
Verifier	A logical function of a Relying Party (or Service Provider) that seeks to verify the integrity of a Credential as presented by a Holder.
[Digital] Wallet	A means of holding multiple credentials from multiple Issuers in a secure digital format. Also provides the functionality to securely share credentials with Verifiers.

2. Data schema

Interoperability requires Issuers, Holders, and Verifiers to share a common set of descriptions for data types and credentials that are commonly required across the trust framework.

2.1 Core data vocabularies

Existing Schema.org vocabularies should be adopted where applicable with extensions added only where a clear need is identified.

A linked data vocabulary for NHS Trust Framework (TF) credentials will be created and published as an addendum to this specification.

2.2 Claim metadata

Claim metadata is used to notify a consuming entity of the quality of data (claims) provided in the payload of credentials. ***These metadata should be applied per credential and not at the individual attribute level.***

NIST-IR-8112¹ describes five categories of metadata regarding claim data²: accuracy, currency, provenance, privacy, and classification. A profile of the proposed NIST-IR-8112 schema will be applied to credentials issued under the NHS Trust Framework observing a UK and NHS context where applicable.

The key elements of this metadata profile are described below.

2.2.1 Provenance metadata

NIST-IR-8112 Metadata Element	Description	Recommended Values	Use within NHS TF
Origin	The name of the entity that issues or creates the initial attribute value	<Origin name> or "None"	Asserted by Issuer
Provider	The name of the entity that is providing the attribute	N/A	Derived from VC <i>issuer</i> property
Pedigree	Description of the attribute value's relationship to the authoritative source of the value	One of: "Authoritative", "Sourced", "Self-Asserted", "Derived"	Asserted by Issuer

¹ NIST-IR-8112 - <https://csrc.nist.gov/publications/detail/nistir/8112/final>

² Claim data – referred to as Attribute data in NIST-IR-8112

2.2.1.1 Origin

The Origin element conveys the name of the entity that established the initial attribute value. This may or may not be an authoritative entity, or the provider; if, for example, an Attribute Provider generates the attribute value through a derivation process, then the Attribute Provider would be the origin.

The key distinction between the origin and the provider is the act of initially generating, capturing, or provisioning the attribute's value, rather than just asserting the attribute's value to a Relying Party.

2.2.1.2 Provider

Verifiable Credentials include an "issuer" element the value of which is a URI uniquely identifying the issuer of the credential. In this profile the "issuer" element will be used to satisfy the Provider metadata element.

2.2.1.3 Pedigree

Pedigree refers to the attribute value's relationship to an authoritative source.

Essentially, it allows the Relying Party to understand better the process by which an attribute's value is generated and to determine whether or not it is from an acceptable authoritative source.

Recommended values for this element include:

Value	Description
Authoritative	The attribute's value was acquired directly from the source of authority. For example, an AP has received a driver's license number directly from the state DMV which issued the license.
Sourced	The attribute's value has been acquired from one or more non-authoritative sources. For example, an AP purchases a driver's license number from a third-party data aggregator.
Self-Asserted	The value was provided to the AP directly by the individual with whom the attribute value is associated. For example, an AP receives a driver's license number directly from the individual who references ownership of the license through a web form or questionnaire. Self-asserted attributes may also be verified or unverified.
Derived	The attribute value was produced through the analysis and manipulation of related attribute values and data. For example, a GPS ride sharing application could determine a value for a home address based on analysis of pick-up and drop-off locations. Derived should not be confused with the concept of Probabilistic Verification (a recommended value for the Verification Method), which focuses on verifying the attribute's value rather than generating it.

Taken in conjunction with the accuracy metadata, this information can enable the Relying Party to better understand the origin of an attribute value, how it relates to its authoritative source, and how it has been verified — all of which help a Relying Party establish a more complete picture of the value’s usefulness and trustworthiness.

2.2.2 Accuracy metadata

NIST-IR-8112 Metadata Element	Description	Recommended Values	Use within NHS TF
Verifier	The type of entity that verified the attribute’s value	One of: “Origin”, “Provider”, “Not Verified”	Asserted by the Issuer
Verification Method	The method by which the attribute value was verified as true and belonging to the specific individual		Asserted by the Issuer

2.2.2.1 Verifier

Verified attributes help Relying Parties make informed decisions about whether to trust an attribute’s value during policy evaluation. In addition, understanding who verified an attribute value may influence the Relying Parties decision about whether or not to accept an attribute value as part of an access control decision.

The verifier metadata element is intended to answer this “who” question. Namely, did the organisation that established the attribute value perform the verification themselves or was the verification done at a later date by an attribute provider? Acceptable values for this metadata field include:

Value	Description
Origin	The attribute’s value was verified by the entity that issued or created it (e.g., a Social Security Number verified by the Social Security Administration).
Provider	The attribute’s value was verified by an attribute provider.
Not Verified	The value of the attribute was not verified.

2.2.2.2 Verification method

This metadata element contains information on the process used to confirm that an attribute value is both true and belongs to the specified individual. This is sometimes necessary to support an authorisation decision but may not always be required.

The acceptable values for Verification Method are intended to provide insight into the verification processes used by providers and enable greater confidence in a given attribute's value. This is particularly beneficial if there are multiple providers for instances of a single attribute. Recommended values for this element are:

Value	Description
Document Verification	The attribute value was verified by inspecting a document that is acceptable to the RP (e.g., driver's license, medical record, utility bill). Transactional participants may want to determine the types of acceptable documents for attribute value verification in advance.
Record Verification	The attribute value was verified against an authoritative record or database. For the purposes of this schema, the term "authoritative" is used consistently with its definition in the underlying policy e.g. (NIST 800-63-3, or GPG45).
Document Verification with Record Verification	The attribute value was verified against both an acceptable document and an authoritative record or database.
Proof of Possession	Confirmation of an individual's ability to demonstrate possession of a device or account is used to verify the attribute's value. Certain attributes and their values, such as phone numbers and email addresses, can be verified by direct communication (SMS, voice, or email) with the entity to which the value is attributed. This method of verification may not be applicable to all attribute values. However, to a certain set of attributes, this is a legitimate approach to determining that the attribute's value is both valid and associated with the appropriate individual.
Probabilistic Verification	The AP has compared the attribute's value to multiple non-authoritative data sources to increase the probability that the attribute value is true and belongs to the appropriate individual. For example, rather than verifying a user address with the post office, an AP may compare the shipping addresses from multiple e-commerce transactions to increase confidence in the attributes' value. There may be many reasons an AP leverages "probabilistic verification" including the lack of available authoritative sources or limited automated capabilities to leverage authoritative sources. Methods of 'probabilistic verification' should be defined in the provider's APS and should be carefully considered for potentially negative privacy impacts. Probabilistic Verification should not be confused with the concept of a Derived pedigree, which focuses on generating the attribute's value rather than verifying it.
Not Verified	The attribute's value has not been verified.

2.2.3 Currency metadata

NIST-IR-8112 Metadata Element	Description	Recommended Values	Use within NHS TF
-------------------------------	-------------	--------------------	-------------------

Last Verification	The date and time when the attribute value was last verified as being true and belonging to the specified individual		VC <i>issuanceDate</i> property, or VC <i>proof:created</i> date whichever is the least recent.
Last Refresh	The date and time when the attribute was last refreshed.		VC property extension <i>lastRefresh</i>
Expiration Date	The date an attribute's value is no longer valid.		VC <i>expirationDate</i> property

2.2.3.1 Last verification

Relying Parties may not trust certain attribute values unless they have been verified within a certain time period.

Last Verification provides the most recent date and time at which the value was verified as true and belonging to the specified individual. This metadata provides only the last date that verification occurred and does not include any information about method of verification.

Where possible the value for this element should be sourced from the *Origin* although as an approximation the least recent of VC *issuanceDate* or VC *proof:created* may also be used.

2.2.3.2 Last refresh

The date and time of the last refresh for the attribute's value should be sourced from the entity that originally created the attribute (the Origin as described in 0).

2.2.3.3 Expiration date

Attribute values sent from an Attribute Provider to a Relying Party may only be valid for its defined use for a set amount of time, depending on requirements, policy, or legal factors. The date after which an attribute's value is considered no longer valid for its defined use is the Expiration Date.

Though Expiration Date and Last Refresh both allow an RP to determine if an attribute's value is current and sufficient, Expiration Date differs from Last Refresh in that there is a specified date or threshold after which the attribute's value becomes void for its defined use.

Relying Parties have the freedom to accept attributes after they have been considered expired for their original intended use, but this decision is made at their own discretion based upon the intended use of the attribute value, the type of interaction it is supporting, and the environment in which they operate.

2.2.4 Privacy Metadata

NIST-IR-8112 Metadata Element	Description	Recommended Values	Use within NHS TF
Date of Consent	The date on which subject consent for release of the attribute value was acquired		N/A
Consent Type	Indicates the type of consent		N/A
Acceptable Uses	Allowed use conditions for entities that receive attributes		N/A
Cache time to live	The length of time for which an attribute value may be cached		N/A
Data Deletion Date	Indicates the date the attribute is to be deleted from records		N/A

Privacy metadata under NIST-IR-8112 often relies on advance agreement between Relying Party and Attribute Providers which are not compatible with the decentralised wallet model adopted for the Technical Trust Framework. As such Privacy Metadata elements are not supported for the alpha.

2.2.5 Classification metadata

Classification metadata under NIST-IR-8112 is concerned with the national security classification of data and scope of sharing said data with other entities. ***This is not applicable under the NHS Trust Framework.***

2.2.6 Additional metadata

Additional Metadata Element	Description	Recommended Values	Use within NHS TF
Trust Framework		DIATF	Yes
Assurance Policy		GPG45, NIST-800-63-3, eIDAS	Yes
Scheme		DBS, RtW, NDIS	Yes
Assurance Outcome	Value associated with the "Assurance Policy"	e.g., H1A, M1C etc as defined by the underlying identity assurance scheme.	Yes
SubjectID	Unique identifier		Yes

2.2.6.1 Assurance policy

The entity that performs identity verification should state the assurance policy applied such as GPG45. The Issuer should retain this metadata in any issued credentials even if the Issuer did not itself perform the identity verification.

2.2.6.2 Assurance outcome

The level of trust or scoring as denoted by the corresponding Assurance Policy. For example, in the case of GPG45 a level of assurance such as LOA3.

2.2.7 JSON schema for claim metadata

The following JSON schema defines the metadata that should accompany each core credential shared under the trust framework. Subsequent JSON schema in this document defining credentials such as PersonIdentity will reference the claimMetadata schema as shown below.

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "claimMetadata",
  "description": "Additional metadata regarding the quality and provenance of the claims",
  "type": "object",
  "properties": {
    "Origin": {
      "description": "The creator of the credential e.g., GMC, NHS TrustName, etc",
      "type": "string"
    },
    "TrustFramework": {
      "description": "e.g., DIATF",
      "type": "string"
    },
    "AssurancePolicy": {
      "description": "e.g., GPG45",
      "type": "string"
    },
    "Scheme": {
      "description": "e.g., DBS, NDIS, RtW",
      "type": "string"
    },
    "SubjectID": {
      "description": "e.g., unique identifier",
      "type": "string"
    },
    "AssuranceOutcome": {
```

```

        "description": "As defined by the AssurancePolicy specifications
e.g., H1A",
        "type": "string"
    },
    "Verifier": {
        "description": "e.g., Origin, Provider [i.e., attribute
provider]",
        "type": "string"
    },
    "VerificationMethod": {
        "description": "e.g., Record Verification",
        "type": "string"
    },
    "pedigree": {
        "description": "e.g., Authoritative, Derived etc",
        "type": "string"
    },
    "lastRefresh": {
        "description": "the most recent date and time at which the value
was verified in ISO 8601 format i.e., YYYY-MM-DDThh:mm:ssTZD (e.g., 1997-07-
16T19:20:30+01:00)",
        "type": "string",
        "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-
9]|12)[0-9])T(2[0-3]|0[0-9]):?(?:[0-5][0-9]):?(?:[0-5][0-9])(Z|[-+](?:2[0-
3]|0[0-9])(?:?:[0-5][0-9]))?"
    }
},

"required": ["Origin", "AssurancePolicy", "Verifier", "pedigree"]
}

```

2.3 Core credential types

This section is non-normative.

The core credential types describe the baseline set of credentials required to satisfy the requirements of Relying Party Trusts.

Credential Type (name)	Overview / use
PersonIdentity	Core identity data related to a single person.
RightToWork	Status of right to work in the UK checks.
DBSStatus	DBS status of the individual.
ProfessionalRegistration	Zero or more professional registrations e.g., GMC, GDC, NMC, HCPC etc.
CoreSkills	CSTF training completed and the method of attainment.
EmploymentReference	An employment reference provided by an employer.

EnglishProficiencyTest	Proof of attainment for IETLS English for study, migration, or work.
-------------------------------	--

Note: additional credential types such as HR Records may be added as agreed by the governing body of the technical trust framework.

2.3.1 PersonIdentity (identity credential)

Credentials describing the verified identity of an individual Subject should include the following attribute data items.

Term	Description
givenName	The first and any middle names of the individual
familyName	The family or surname of the individual
birthDate	Date of Birth
gender	Gender of the individual
address	Current address of the individual
nationality	As verified during onboarding
image	Image of the individual in ICAO format captured during onboarding “IDSPs are required to verify that the image supplied with the IDSP check matches the identity document.” (optional)

Data items should be presented in the following formats in a verifiable credential.

Term	givenName
Format	http://schema.org/givenName
Mandatory	Y
Usage	One or more names verified as belonging to the claimant.

Term	familyName
Format	http://schema.org/familyName
Mandatory	Y
Usage	One or more names verified as belonging to the claimant.

Term	birthDate
Format	Date of birth specified in ISO 8601 format i.e., YYYY-MM-DD: YYYY indicates a four-digit year, 0000 through 9999. MM indicates a two-digit month of the year, 01 through 12. DD indicates a two-digit day of that month, 01 through 31.
Mandatory	Y
Usage	Birth date of the claimant.

Term	gender
-------------	--------

Format	http://schema.org/Text Values for gender MUST be one of the following: Male Female Not Specified
Mandatory	Y
Usage	The gender of the claimant.

Term	address
Format	http://schema.org/PostalAddress
Mandatory	Y
Usage	The current correspondence address of the claimant.

Term	nationality
Format	http://schema.org/nationality
Mandatory	Y
Usage	The nationality of the claimant as verified during onboarding.

Term	image
Format	http://schema.org/image
Mandatory	Y
Usage	A valid image of the claimant in ICAO format captured during onboarding.

2.3.1.1 JSON Schema for PersonIdentity

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "PersonIdentity",
  "description": "Core identity data related to a single person.",
  "type": "object",
  "properties": {
    "givenName": {
      "description": "The first and any middle names of the individual",
      "type": "string"
    },
    "familyName": {
      "description": "The family or surname of the individual",
      "type": "string"
    }
  }
}
```

```

    "birthDate": {
      "description": "Date of Birth",
      "type": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-9]|12)[0-9]"
    },
    "gender": {
      "description": "Gender of the individual",
      "type": "string",
      "pattern": "Male|Female|Unspecified"
    },
    "address": {
      "description": "Current address of the individual",
      "$ref": "PostalAddress.jschema"
    },
    "nationality": {
      "description": "Nationality of the individual",
      "type": "string"
    },
    "image": {
      "description": "Image of the individual",
      "type": "string"
    },
    "claimMetadata": {
      "description": "metadata related to the verification of the claims in this entity / credential",
      "$ref": "claimMetadata.jschema"
    }
  },

  "required": ["givenName", "familyName", "birthDate", "claimMetadata"]
}

```

2.3.2 RightToWorkEvidenceCheck

Term	Description
vizPage	Image of the biometric page of the identity document

Data items should be presented in the following formats in a verifiable credential.

Term	vizPage
Format	http://schema.org/image
Mandatory	Y
Usage	An image of the viz page from the passport.

2.3.2.1 JSON Schema for RtWEvidenceCheck

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "RtWSupplementaryEvidence",
  "description": "Attributes required to complete a RtW check .",
  "type": "object",
  "properties": {
    "vizPage": {
      "description": "Image of the viz page of the passport",
      "type": "string"
    },
    "claimMetadata": {
      "description": "metadata related to the verification of the claims in this entity / credential",
      "$ref": "claimMetadata.jschema"
    }
  },
  "required": ["vizPage", "identityVerified", "DateofIDCheck", "GPG45Profile", "claimMetadata"]
}
```

2.3.3 DBSStatus

Term	Description
disclosureType	The type of DBS check recorded on the certificate.
disclosureNumber	The disclosure number recorded on the certificate
issueDateIR	Issue date of the indicative result.
resultIR	The indicative result code e.g., clear.
certificateNumber	The certificate number as would be on a printed certificate.
surname	The surname as recorded on the certificate.
birthDate	Date of birth as recorded on the certificate.
organisation	Organisation name from the certificate data.

These data items should be presented in the following formats in a verifiable credential.

Term	disclosureType
Format	http://schema.org/Text
Mandatory	Y
Usage	The type of DBS check recorded on the certificate.

Term	disclosureNumber
Format	http://schema.org/Text
Mandatory	Y

Usage	The disclosure number as provided for an interim result.
--------------	--

Term	issueDateIR
Format	Date specified in ISO 8601 format i.e., YYYY-MM-DD
Mandatory	Y
Usage	e.g., 2022-04-01

Term	resultIR
Format	http://schema.org/Text
Mandatory	Y
Usage	The indicative result code e.g., Clear

Term	certificateNumber
Format	http://schema.org/Text
Mandatory	Y
Usage	The certificate number as would be on a printed certificate.

Term	surname
Format	http://schema.org/Text
Mandatory	Y
Usage	The surname as recorded on the certificate e.g., Smith

Term	birthDate
Format	Date specified in ISO 8601 format i.e., YYYY-MM-DD
Mandatory	Y
Usage	e.g., 1980-05-17

Term	organisation
Format	http://schema.org/Text
Mandatory	N
Usage	Organisation name from the certificate data e.g., "Exton Primary School"

2.3.3.1 JSON Schema for DBSStatus

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "DBSStatus",
  "description": "DBS status of the individual. May be indicative result or full certificate data.",
  "type": "object",
```

```

    "properties": {
      "disclosureNumber": {
        "description": "The disclosure number",
        "type": "string"
      },
      "issueDateIR": {
        "description": "issue date of the indicative result in ISO 8601 format (YYYY-MM-DD)",
        "type": "string",
        "pattern": "([0-9]{4})(-?)(1[0-2]|0[1-9])\\2(3[01]|0[1-9])|([12][0-9])"
      },
      "resultIR": {
        "description": "The indicative result code e.g., clear",
        "type": "string"
      },
      "certificateNumber": {
        "description": "certificate number as would be on a printed certificate",
        "type": "string"
      },
      "surname": {
        "description": "surname as recorded on the certificate",
        "type": "string"
      },
      "birthDate": {
        "description": "date of birth as recorded on the certificate",
        "type": "string",
        "pattern": "([0-9]{4})(-?)(1[0-2]|0[1-9])\\2(3[01]|0[1-9])|([12][0-9])"
      },
      "organisation": {
        "description": "organisation name from the certificate data",
        "type": "string"
      },
      "claimMetadata": {
        "description": "metadata related to the verification of the claims in this entity / credential",
        "$ref": "claimMetadata.jschema"
      }
    },
    "required": ["disclosureNumber", "issueDateIR", "resultIR", "claimMetadata"]
  }

```

2.3.4 ProfessionalRegistration

Term	Description
referenceNo	A unique reference number identifying the individual as registered with the professional body e.g., GMC Number
registrationBody	Legal name of the registration body e.g., General Medical Council
status	Status of the professional registration.
practiceStatus	The individual's licenced or otherwise regulated ability to practice.
registrationDate	Date of registration
primaryQualification	Primary (relevant) qualification as a professional.
yearQualified	Date the primaryQualification was achieved.
periodStart	Optional date the registration became valid
periodEnd	Optional date the registration lapsed
specialistRegisters	Optional – one or more specialist registers

Data items should be presented in the following formats in a verifiable credential.

Term	referenceNo
Format	http://schema.org/Text
Mandatory	Y
Usage	A unique reference number identifying the individual as registered with the professional body e.g., GMC Number

Term	registrationBody
Format	http://schema.org/Text
Mandatory	Y
Usage	Legal name of the registration body e.g., General Medical Council

Term	status
Format	http://schema.org/Text
Mandatory	Y
Usage	The status of the professional registration e.g., pending / registered / disqualified / suspended.

Term	practiceStatus
Format	http://schema.org/Text
Mandatory	Y
Usage	Licenced / Not Licenced / Not Applicable

Term	registrationDate
Format	Date specified in ISO 8601 format i.e., YYYY-MM-DD

Data Schema for Technical Trust Framework for verifiable credentials

Mandatory	Y
Usage	e.g., 1997-04-01

Term	primaryQualification
Format	http://schema.org/Text
Mandatory	Y
Usage	Primary (relevant) qualification as a professional.

Term	yearQualified
Format	Year described as YYYY
Mandatory	Y
Usage	e.g., 1997
Term	periodStart
Format	Date specified in ISO 8601 format i.e., YYYY-MM-DD
Mandatory	N
Usage	e.g., 1997-03-21

Term	periodEnd
Format	Date specified in ISO 8601 format i.e., YYYY-MM-DD
Mandatory	N
Usage	e.g., 2017-03-20

Term	specialistRegisters
Format	http://schema.org/Text
Mandatory	N
Usage	Free text list of one or more specialist registers

2.3.4.1 JSON Schema for ProfessionalRegistration

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "ProfessionalRegistration",
  "description": "Professional registration for an individual",
  "type": "object",
  "properties": {
    "referenceNo": {
      "description": "A unique reference number identifying the individual as registered with the professional body e.g., GMC Number",
      "type": "string"
    },
    "registrationBody": {
```

```

      "description": "Legal name of the registration body e.g., General
Medical Council",
      "type": "string"
    },
    "status": {
      "description": "Status of the professional registration.",
      "type": "string"
    },
    "practiceStatus": {
      "description": "The individual's licenced or otherwise regulated
ability to practice.",
      "type": "string"
    },
    "registrationDate": {
      "description": "Date of registration",
      "type": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-
9]|12)[0-9])"
    },
    "primaryQualification": {
      "description": "Primary (relevant) qualification as a
professional.",
      "type": "string"
    },
    "yearQualified": {
      "description": "Year the primaryQualification was achieved.",
      "type": "string",
      "pattern": "([0-9]{4})"
    },
    "periodStart": {
      "description": "Optional date the registration became valid",
      "type": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-
9]|12)[0-9])"
    },
    "periodEnd": {
      "description": "Optional date the registration lapsed",
      "type": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-
9]|12)[0-9])"
    },
    "specialistRegisters": {
      "description": "Optional - one or more specialist registers",
      "type": "string"
    },
    "claimMetadata": {
      "description": "metadata related to the verification of the
claims in this entity / credential",

```

```

    "$ref": "claimMetadata.jschema"
  },
  "required": [
    "referenceNo",
    "registrationBody",
    "status",
    "practiceStatus",
    "registrationDate",
    "primaryQualification",
    "yearQualified",
    "claimMetadata"
  ]
}

```

2.3.5 CoreSkills

Term	Description
statMandSubject	Statutory/Mandatory subject name e.g., Infection prevention and control
level	Subject level (if applicable) e.g., Level 1
attainmentStatus	Indication of attainment e.g., Attained / Incomplete / Failed / Lapsed
dateGiven	Date training was given specified in ISO 8601 format i.e., YYYY-MM-DD
refreshRate	The frequency at which the training should be refreshed e.g., 2 Years
employer	The employer at the time of attainment.
employerAlignment	Boolean: employer aligned to the CSTF framework (self-asserted currently)

For naming conventions and rules (e.g. for statMandSubject names) see:

<https://www.skillsforhealth.org.uk/images/services/cstf/CSTF%20Naming%20Conventions%20%20Competencies%20on%20ESR%20June%202019.pdf>

Data items should be presented in the following formats in a verifiable credential.

Term	statMandSubject
Format	http://schema.org/Text Values for statMandSubject MUST be one of those described in the document: "UK Core Skills Training Framework Naming conventions and the use of CSTF competencies on the NHS Electronic Staff Record (ESR)" ³ .
Mandatory	Y
Usage	The name of the Statutory/ Mandatory training subject.

Term	level
Format	http://schema.org/Text One of the following levels as described in the CSTF Naming Conventions, for example: Level 1

³ CSTF Naming Conventions –

<https://www.skillsforhealth.org.uk/images/services/cstf/CSTF%20Naming%20Conventions%20%20Competencies%20on%20ESR%20June%202019.pdf>

Data Schema for Technical Trust Framework for verifiable credentials

	Level 2 Level 3 Module A Module B Module C
Mandatory	Y
Usage	Subject level (if applicable) in regard to the statMandSubject, e.g., Level 1

Term	attainmentStatus
Format	http://schema.org/Text
Mandatory	Y
Usage	Indication of attainment e.g., Attained / Failed / Lapsed

Term	dateGiven
Format	Date in ISO 8601 format i.e., YYYY-MM-DD
Mandatory	Y
Usage	Date training was given

Term	refreshRate
Format	http://schema.org/Text A refresh rate as specified in the CSTF Naming Conventions: No Specified Renewal 1 Year 2 Years 3 Years
Mandatory	Y
Usage	The frequency at which the training should be refreshed e.g., 2 Years

Term	employer
Format	http://schema.org/Text
Mandatory	Y
Usage	The employer at the time of attainment.

Term	employerAlignment
Format	Boolean
Mandatory	N
Usage	The employer at the time of attainment.

2.3.5.1 JSON Schema for CoreSkills

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "CSTF Core Skills",
  "description": "CSTF training completed and the method of attainment.",
  "type": "object",
  "properties": {
    "statMandSubject": {
      "description": "Statutory/Mandatory subject name e.g., Infection prevention and control",
      "type": "string"
    },
    "level": {
      "description": "Subject level (if applicable) e.g., Level 1",
      "type": "string"
    },
    "attainmentStatus": {
      "description": "Indication of attainment e.g., Attained / Failed / Lapsed",
      "type": "string"
    },
    "dateGiven": {
      "description": "Date training was given specified in ISO 8601 format i.e., YYYY-MM-DD",
      "type": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-9]|12)[0-9]"
    },
    "refreshRate": {
      "description": "The frequency at which the training should be refreshed e.g., 2 Years",
      "type": "string"
    },
    "employer": {
      "description": "The employer at the time of attainment",
      "type": "string"
    },
    "employerAlignment": {
      "description": "Employer aligned to the CSTF framework (self-asserted currently)",
      "type": "boolean"
    },
    "claimMetadata": {
      "description": "metadata related to the verification of the claims in this entity / credential",
      "$ref": "claimMetadata.jschema"
    }
  }
}
```

```

    "required": ["statMandSubject", "attainmentStatus", "dateGiven",
"refreshRate", "employer", "claimMetadata"]
}

```

2.3.6 EmploymentReference

Term	Description
referee	Full name of the referee
employer	The employers legal name
startDate	Start date for the employment period
endDate	End date for the employment period
referenceText	The actual written reference as free text.
dateOfReference	Date reference was written
positionHeld	Position held by the employee
disciplinaryAction	Any recent or ongoing disciplinary action or referrals
contactEmail	Email address that can be used to make enquires if needed.

These data items should be presented in the following formats in a verifiable credential.

Term	referee
Format	http://schema.org/Text
Mandatory	Y
Usage	Full name of the referee

Term	employer
Format	http://schema.org/Text
Mandatory	Y
Usage	The employers legal name

Term	startDate
Format	Date in ISO 8601 format i.e., YYYY-MM-DD
Mandatory	Y
Usage	e.g., 2012-07-21

Term	endDate
Format	Date in ISO 8601 format i.e., YYYY-MM-DD
Mandatory	Y
Usage	e.g., 2017-05-28

Term	referenceText
Format	http://schema.org/Text
Mandatory	Y
Usage	

Term	dateOfReference
Format	Date in ISO 8601 format i.e., YYYY-MM-DD
Mandatory	Y
Usage	e.g., 2022-02-13

Term	positionHeld
Format	http://schema.org/Text
Mandatory	Y
Usage	The actual written reference as free text.

Term	disciplinaryAction
Format	http://schema.org/Text
Mandatory	N
Usage	Any recent or ongoing disciplinary action or referrals

Term	contactEmail
Format	Constrained by regular expression to conform with standard email address format.
Mandatory	N
Usage	Email address that can be used to make further enquires if needed.

2.3.6.1 JSON Schema for EmploymentReference

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "EmploymentReference",
  "description": "An employment reference provided by an employer.",
  "type": "object",
  "properties": {
    "referee": {
      "description": "Full name of the referee",
      "type": "string"
    },
    "employer": {
      "description": "The employers legal name",

```

```

        "type": "string"
      },
      "startDate": {
        "description": "Start date for the employment period",
        "type": "string",
        "pattern": "([0-9]{4})(-?)(1[0-2]|0[1-9])\\2(3[01]|0[1-9]|12)[0-9]"
      },
      "endDate": {
        "description": "End date for the employment period.",
        "type": "string",
        "pattern": "([0-9]{4})(-?)(1[0-2]|0[1-9])\\2(3[01]|0[1-9]|12)[0-9]"
      },
      "referenceText": {
        "description": "The actual written reference as free text.",
        "type": "string"
      },
      "dateOfReference": {
        "description": "Date reference was written",
        "type": "string",
        "pattern": "([0-9]{4})(-?)(1[0-2]|0[1-9])\\2(3[01]|0[1-9]|12)[0-9]"
      },
      "positionHeld": {
        "description": "Position held by the employee",
        "type": "string"
      },
      "disciplinaryAction": {
        "description": "Any recent or ongoing disciplinary action or referrals",
        "type": "string"
      },
      "contactEmail": {
        "description": "Email address that can be used to make further enquires if needed.",
        "type": "string",
        "pattern": "([a-zA-Z0-9_\\-\\.]+)@([a-zA-Z0-9_\\-\\.]+)\\.([a-zA-Z]{2,5})"
      },
      "claimMetadata": {
        "description": "metadata related to the verification of the claims in this entity / credential",
        "$ref": "claimMetadata.jschema"
      }
    },
  },

```

```

    "required": ["referee", "employer", "startDate", "endDate",
"referenceText", "dateOfReference", "positionHeld", "claimMetadata"]
  }

```

2.3.7 EnglishProficiencyTest

Term	Description
trainingProvider	Name of the training provider for the IELTS test
dateAttained	Date the test was taken, and score attributed
scoreAttained	IELTS score scale attained (ranging from 0 to 9). See: https://www.ielts.org/about-ielts/what-is-ielts

Data items should be presented in the following formats in a verifiable credential.

Term	trainingProvider
Format	http://schema.org/Text
Mandatory	Y
Usage	The name of the competent training provider used by the claimant.

Term	dateAttained
Format	Date of attainment specified in ISO 8601 format i.e., YYYY-MM-DD.
Mandatory	Y
Usage	Date the score was attained from a competent training provider.

Term	scoreAttained
Format	http://schema.org/Text scoreAttained = bandScore skillLevel Where: bandScore (numeric 0 to 9 e.g., 6) skillLevel (text e.g., "Competent user") For example: 6 Competent user
Mandatory	Y
Usage	IELTS score scale attained (ranging from 0 to 9 with explanatory skill level). See: https://www.ielts.org/about-ielts/what-is-ielts

2.3.7.1 JSON Schema for EnglishProficiencyTest

```

{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "EnglishProficiencyTest",

```

```

    "description": "Proof of attainment for IELTS English for study,
migration, or work.",
    "type": "object",
    "properties": {
      "trainingProvider": {
        "description": "Name of the training provider for the IELTS
test",
        "type": "string"
      },
      "dateAttained": {
        "description": "Date the test was taken, and score attributed",
        "type": "string",
        "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-
9]|1[12][0-9])"
      },
      "scoreAttained": {
        "description": "IELTS score scale attained (ranging from 0 to
9). See: https://www.ielts.org/about-ielts/what-is-ielts",
        "type": "string"
      },
      "claimMetadata": {
        "description": "metadata related to the verification of the
claims in this entity / credential",
        "$ref": "claimMetadata.jschema"
      }
    },
    "required": ["trainingProvider", "dateAttained", "scoreAttained",
"claimMetadata"]
  }

```

2.3.8 Self-asserted or low trust credentials

Self-asserted credentials may be requested by a Verifier and/or provided by the Holder but MUST be accompanied by metadata describing their provenance and quality i.e., in *claimMetadata* the value of *Verifier* should be set to “Not Verified”.

2.4 Additional credential types

This section is non-normative.

The supplemental credential types describe the credentials required to satisfy the requirements of external Relying Parties such as the Disclosure and Barring Service and the UK Home Office.

2.4.1 DBSEligibility Evidence

Term	Description
------	-------------

Data Schema for Technical Trust Framework for verifiable credentials

PassportNumber	Unique number in the passport
PassportDob	Date of birth in the passport
PassportNationality	Nationality in the passport
PassportIssueDate	Issue date in the passport
DrivingLicenceNumber	Unique number in the driver's licence
DrivingLicenceDOB	Date of birth in the driver's licence
DrivingLicenceType	Full or Provisional
DrivingLicenceValidFrom	Valid from in the driver's licence
DrivingLicenceIssueCountry	Issuing country in the driver's licence

Data items should be presented in the following formats in a verifiable credential.

Term	PassportNumber
Format	http://schema.org/Text
Mandatory	Y
Usage	Unique number in the passport

Term	PassportDob
Format	Date specified in ISO 8601 format i.e., YYYY-MM-DD.
Mandatory	Y
Usage	e.g., 2012-07-21

Term	PassportNationality
Format	http://schema.org/Text
Mandatory	Y
Usage	Nationality in the passport

Term	PassportIssueDate
Format	Date passport issued specified in ISO 8601 format i.e., YYYY-MM-DD.
Mandatory	Y
Usage	e.g., 2012-07-21

Term	DrivingLicenceNumber
Format	http://schema.org/Text
Mandatory	Y
Usage	Unique number in the driver's licence

Term	DrivingLicenceDOB
Format	Date of attainment specified in ISO 8601 format i.e., YYYY-MM-DD.

Data Schema for Technical Trust Framework for verifiable credentials

Mandatory	Y
Usage	e.g., 2012-07-21

Term	DrivingLicenceType
Format	http://schema.org/Text
Mandatory	Y
Usage	E.g. Full or Provisional

Term	DrivingLicenceValidFrom
Format	Date licence valid from specified in ISO 8601 format i.e., YYYY-MM-DD.
Mandatory	Y
Usage	e.g., 2012-07-21

Term	DrivingLicenceIssueCountry
Format	http://schema.org/Text
Mandatory	Y
Usage	Country of issue

2.4.1.1 JSON Schema for DBSEligibilityEvidence

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "SupplementaryEvidence",
  "description": "Attributes required to complete a RtW and/or DBS check.",
  "type": "object",
  "properties": {
    "PassportNumber": {
      "description": "unique number in the passport",
      "type": "string"
    },
    "PassportDob": {
      "description": "Date of birth": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-9])|12[0-9])"
    },
    "PassportNationality": {
      "description": "nationality in the passport",
      "type": "string"
    },
    "DrivingLicenceNumber": {
      "description": "unique number in the passport",
      "type": "string"
    }
  }
}
```

```

    "PassportIssueDate": {
      "description": "Issue date": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-9])|12[0-9])"
    },
    "DrivingLicenceDOB": {
      "description": "Date of birth": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-9])|12[0-9])"
    },
    "DrivingLicenceType": {
      "description": "Type": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-9])|12[0-9])"
    },
    "DrivingLicenceValidFrom": {
      "description": "Date of birth": "string",
      "pattern": "([0-9]{4})(-?) (1[0-2]|0[1-9])\\2(3[01]|0[1-9])|12[0-9])"
    },
    "DrivingLicenceIssueCountry": {
      "description": "Country of issue": "string",
      "type": "string"
    },
    "claimMetadata": {
      "description": "metadata related to the verification of the claims in this entity / credential",
      "$ref": "claimMetadata.jschema"
    }
  },

  "required": ["PassportNumber", "PassportDob", "PassportNationality", "PassportIssueDate", "DrivingLicenceDOB", "DrivingLicenceType", "DrivingLicenceValidFrom", "DrivingLicenceIssueCountry", "claimMetadata"]

```

Appendix – NHS attribute mappings

Identity credential

DSIT data schema	Attribute	NHS TTF data schema
<i>Given name</i>	givenName	personIdentity (Core credential types)
<i>Middle name</i>		The first and any middle names of the individual include in givenName
<i>Family name</i>	familyName	personIdentity (Core credential types)
<i>Address</i>	address	personIdentity (Core credential types)
<i>Date of birth</i>	birthDate	personIdentity (Core credential types)
<i>Gender*</i>	gender	personIdentity (Core credential types)
<i>Nationality</i>	nationality	personIdentity (Core credential types)
<i>Image</i>	Image	personIdentity (Core credential types)
NOTES		
*Gender is not part of the DSIT schema but can be obtained and is required by the NHS		

Identity metadata

DSIT	Attribute	NHS TTF data schema
<i>Trust Framework</i>	TrustFramework	Additional metadata (Claim metadata)
<i>Scheme</i>	Scheme	Additional metadata (Claim metadata)
<i>Assurance Policy</i>	AssurancePolicy	Additional metadata (Claim metadata)
<i>Confidence Level</i>		Derived from assurance outcome i.e. H1A equals High
<i>Identity Evidence Profile</i>	AssuranceOutcome	Additional metadata (Claim metadata)
<i>Verification</i>	VerificationMethod	Additional metadata (Claim metadata)
<i>Organisation</i>	Origin	Provenance Metadata (Claim metadata)
<i>Subject ID</i>	Subjectid	Additional metadata (Claim metadata)

Verification outcome

DSIT Attribute	Attribute	NHS TTF data schema
<i>Confidence Level</i>		Derived from assurance outcome i.e. H1A equals High
<i>Identity Evidence Profile</i>	AssuranceOutcome	Additional metadata (Claim metadata)
<i>Strength</i>		not required as it can be derived from the GPG45
<i>Validity</i>		not required as it can be derived from the GPG45
<i>Activity history</i>		not required as it can be derived from the GPG45
<i>ID Fraud</i>		not required as it can be derived from the GPG45
<i>Verification</i>	VerificationMethod	Accuracy Metadata (Claim metadata)

DBSEligibility evidence

DBS requirement*	Attribute	NHS TTF data schema
<i>Passport Details</i>	PassportNumber, PassportDob, PassportNationality, PassportIssueDate	DBSEligibilityEvidence (Additional credential types)
<i>Driving Licence Details</i>	DriverLicenceDOB, DriverLicenceType, DriverLicenceValidFrom, DriverLicenceIssueCountry	DBSEligibilityEvidence (Additional credential types)
NOTES		
* https://www.gov.uk/government/publications/dbs-identity-checking-guidelines/dbs-digital-identity-verification-guidance		

Right to work

DSIT Attribute	Attribute	NHS TTF data schema
<i>Given name</i>	givenName	personIdentity (Core credential types)
<i>Middle name</i>		The first and any middle names of the individual include in givenName
<i>Family name</i>	familyName	personIdentity (Core credential types)
<i>Date of birth</i>	birthDate	personIdentity (Core credential types)
<i>Image of the biometric page of the identity document</i>	Image of the biometric page of the identity document	RtWSupplementaryEvidence (Additional credential types)
<i>Image</i>	Image	personIdentity (Core credential types)
<i>Identity verified (Y/N)</i>		Not required
<i>Evidence checked by</i>	Origin	Provenance Metadata (Claim metadata)
<i>Date of ID check</i>		Identity profile and date verified in the metadata
<i>GPG45 profile</i>	AssuranceOutcome	Additional metadata (Claim metadata)
Annex C: Digital identity verification – Guidance for employers and Identity Service Providers (IDSPs)		