सत्यमेव जयते
Ministry of
Skill Development
And Entrepreneurship

Adopting e-Credentialing in the Skilling Ecosystem

Version 1.0

June 2019

Table of Contents

Executive Summary

The jobs and skilling ecosystem is a complex arena with a number of frictions preventing an optimal supply and demand equilibrium, resulting in not only underemployment but also significant wage gaps. The Ministry of Skill Development and Entrepreneurship (MSDE) has been grappling with many of these issues in the Indian context. The established Directorate General for Training (DGT) runs approximately 10,000 Industrial Training Institutes (ITIs) across the country which seek to enhance the skill capabilities of youth in vocational trades such as welding, fitting, electrical, and computer operating & programming assistant - among a host of others.

In the context of a young, aspirational, and quickly growing labour force, MSDE's revamped Vision 2025 document articulates an **'ecosystem-enabling lens to transition India to a high skills equilibrium',** towards a vision of unlocking human capital. This new vision highlights the need for **technology-led change**, which can help the full network of actors across a complex, fragmented, and diverse ecosystem of skill training providers, employers, skill assessors, enablers (job or gig matchers), and individual aspirers to effectively interact to create productive learning and employment opportunities for individuals. Currently, many of these interactions are fraught with frictions - low trust, lack or asymmetry of information, low portability of skills gained and skills claimed, and low discovery of new opportunities to name a few. For instance, today individuals struggle to showcase their skill level in a manner which is comparable at scale for potential employers, and cannot easily exchange certificates or credentials[1] in a trusted manner with users of that information without being physically present.

In the ITI context, the National Trade Certificate (NTC) issued to candidates presents an opportunity to innovate: there are fraudulent NTCs in circulation which individuals are using to access jobs, but more importantly, the NTC could do more to provide further context to employers on the actual skill level of the candidate beyond just the degree attained in a manner that employers can trust is secure. In addition, currently prospective employers or job matching agents cannot easily digitally review a large batch of candidates' NTCs at scale without the physical presence of the candidates. This presents a bottleneck to the job application process for youths graduating from ITIs: in a world where most published job postings get applications in the hundreds, quickly discerning skill levels and suitability is critical to ensuring a higher wage reward to deserving candidates and reducing the cost of search and recruitment for firms.

To address this challenge, DGT proposes to issue digital 'eCredentials/eCertificates' which are freely portable for candidates and easily verifiable at scale by employers and job matching platforms, but continue to allow print and other visual forms for human

[1] In this document the terms *credential* and *credentials* are used to mean a *qualification or achievement of a person or entity used to indicate their suitability for something*. The National Trade Certificate is issued to award such a qualification attained through ITIs.

consumption. This would enable candidates to verifiably state their skill levels with a high degree of trust in authenticity to aggregators, matchers, and employers. This approach will be rolled out in the coming months, with an initial target of 2 million verifiable eCredentials issued by July 2019.

To accomplish this, DGT will leverage the open source e-Credentialing specification under Project inCredible[2], an extension to OpenBadges[3] specifications, which proposes a set of electronic standards for machine-readable data to represent various credentials in the skilling ecosystem across industry verticals. This electronic standard for data representing credentials allows certificates to be awarded in digital, machine-readable formats, which in turn makes it possible for an individual to freely transfer credentials in a trusted and consent-based manner and apply for jobs remotely. It combines existing technology elements (machine readable format, the use of digital signatures to ensure authenticity of a document, and the use of standards to clarify the detail behind an accomplishment, etc.) to create for the first time a standard for credentials to be machine readable and verifiably authentic in the skilling space. The standard is internationally compatible with blockchain based approaches to certification and is built on top of OpenBadges V2 specifications.

Moreover, in order to make the benefits of electronic credentialing a reality across the jobs and skilling ecosystem, the Ministry of Skill Development urges other institutions that upskill and train aspirers and workers (including employers) to adopt the open standard for digital credentialing. Skill and job experience data sharing at scale as per standards and user consent could have powerful network effects on the behaviour of skill data sharing and aggregation which ultimately serve both individuals' and employers/skill trainers' interests. For instance, employers could reliably ascertain the full set of contextualized previous training and work experience before interviewing a candidate. Existing job matching portals could better filter or automatically match recommended candidates for roles based on verified credentials. New companies could be built that automate aggregation of experience and training certificates of individuals without digital literacy themselves into competitive digital CVs - and create a trusted profile listing of aspiring individuals across various socioeconomic strata seeking employment. Finally, the new data might even shed light on the trends associated with demand flux for certain skills, better informing them on what skills to pursue at the outset of their careers.

In order to complement the effort to adopt the eCredential Standard, MSDE also proposes to build **Electronic Registries** with **trusted data** accessible to via **Open APIS** of training providers, assessment agents, and courses. This could enable a credential to refer to actors in a registry to verify the profile of an issuer, assessor, or awarding body. Other parallel efforts to support could include techniques to make available and share open data around skill supply and demand.

[2] Open source Project inCredible - https://github.com/sunbird-specs/inCredible

[3] OpenBadges V2 - https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/index.html

As a nation we have learnt a great deal over the last decade on how to use technology innovatively at scale in the Indian social sector. Though we cannot precisely predict the future, leveraging technology designed as digital infrastructure for the market allows us to quickly adapt to various needs and operate at India scale. Adopting this open specification for a skill credential could set us on a path to open up a strong ecosystem of players to competitively and interoperably inform, train, counsel, and certify aspirers and those in the job and skilling ecosystem, to help us truly realise India's demographic potential.

Introduction & Purpose

A specific and core issue in the jobs and skills arena that has been well-documented by jobs research is low trust in presented credentials - largely paper certificates - and a lack of specific, comparable, and micro-credentials robustly indicating past experience or skill training history (both informal and formal).

Paper certificates create a number of frictions:

1. For **aspirers**, there is a need to physically secure one 'original' and present it only in person;
2. For **employers**, there is a high risk of fake certificates and little common context to compare it to other job applicants.

The purpose of adopting the electronic credential specification is to provide certificate recipients at Industrial Training Institutes with a means for participating in a digital economy where:

- They can **digitally transfer skill credentials** as per training outcomes using trusted and verifiable means
- Skilled individuals can be **automatically matched** to jobs across regions
- ITIs can award certificates using their **preferred vocabulary for academic standards** without inhibiting exchange of information on skills supply and employment opportunity with other organisations

Some of the key benefits of an electronic skill credential over a traditional paper-based certificate are summarised in the table below.

Table 1: Paper Certificate vs a Digital Skill Credential

	Paper Certificate	Digital Skill Credential
Verification + Trust	Difficult, low trust	Instant, permanent, online + offline verification. Non tamperable, so high **trust**
Review	Human evaluation	Machine readable, enabling comparisons across candidates at **scale.**

Detail & Context on Standards Achieved	Minimal or difficult to access universally	Always issued based on published standards which share required contextual standards & **information**
Presentation	Physical presence of an 'original' copy required	Replicable (no original) and electronically shareable: capacity for remote (presence-less) and automatic application to jobs. Highly **portable**.
Data & Analytics	No data exhaust or digital data trail	Anonymised verification data allows a better understanding of which skills are sought by the marketplace, reducing **information** asymmetry

Principles

In order to achieve its objectives, the electronic skill credential would need to enable:

Verifiability: Authenticity of the credential should be digitally verifiable by any application to which it is presented. This verification should not require the physical presence of the credential holder, or be contingent on any human action of the issuer.

Portability: The credentials should be digitally portable across systems participating in the ecosystem. Physical certificates are unrestricted -- the recipient can present the certificate to any party of her choice. The same property should be preserved. This includes easy digital storage in the control of the recipient of the credentials and easy consented transfer & sharing by the recipient for various purposes. These purposes could include job applications, loans or financial services applications or additional skill training amongst others.

Permanence: The credentials should continue to exist and be valid beyond the lifetime of the institution where it was awarded. That is, if an ITI which has awarded a credential subsequently ceases to exist, the credentials remain verifiable and portable across the ecosystem.

Self-Describing: The credential model should be self-describing in a manner that the consumer of the credential does not require private sources of information to validate or understand it. In practice, this means that any declaration of skill level or reference to DGT or ITIs as awarding institutions links to a publicly accessible and unencumbered source of further information with the institutional profile. This makes the credential truly portable across the ecosystem, since anyone to whom it is presented can make sense of the information contained within and have enough context to compare the accreditation with another certificate.

Consent-based: In view of the Supreme Court Judgment on privacy, as well as the upcoming Data Protection Bill, the privacy preservation and ensuring user's consent has been given primary significance in the proposal for adopting this manner of digital credentialing.

Current State

In the DGT context, issuing a single National Trade Certificate for a basket of skills is problematic in scenarios where the certificate does not include details of the contents of the 'basket'. It makes it difficult for employers to get a complete picture of the employee's capabilities. To ascertain the ability of an employee, employers must either conduct their own evaluations or have experience with the competencies of trainees graduating from a particular program. Both alternatives increases the cost and complexity of employer processes while lowering the value of the certificate issued.

Conversely, verifying multiple certificates can be challenging for employers when this practice is not consistently followed amongst different awarding bodies. Without intimate familiarity with the certification practices of the awarding body, employers will not know which certificates to expect from a trainee. This lowers the acceptability of a certificate reducing it to the set of employers who are familiar with the awarding body. Thus, this project.

Assessors

The role of the assessor is, in some instances, separate from the role of the certificate awarding body. Assessors may be private bodies which specialise in a specific skill (such as a Driving School) or may be awarding bodies like DGT or Sector Skill Councils which certify many skills within a specific industry.

Competency Standards

In the absence of competency standards maintained across awarding bodies, employers must be familiar with the awarding body's reputation in order to compare potential employees. Migrating certificates to an industry-led set of standards will allow portability across the ecosystem. *Ensuring that the standards are represented in digital, machine-readable formats will allow credential management, candidate evaluation and mobilisation at scale*.

There are a network of standards available within the skills domain. The National Skills Qualification Framework (NSQF) outlines a taxonomy of industry skills and competency levels which are broken down into Qualification Packs (QPs) comprising a collection of National Occupational Standards (NOS). However, *it is imperative that a mechanism is established for these standards to evolve led by industry demand for new skills* in existing domains as well as for entirely new domains. Utilising such an evolving framework of standards for issuing certificates across issuing institutions can dramatically increase the value of certificates for trainees and employers. Hence, skills certificates will be given out by awarding bodies which have been recognized by a regulator (such as NCVET) and mention the NSQF level and/or the NOS covered.

These standards may be used by all ecosystem participants including those who are purely private in nature. They may include employers, training providers , gig economy platforms (where competencies may include user ratings, GPS data showing services fulfilled, etc), job seeker platforms, and other participants.

Specifications Leveraged for Skill Certificates

Full technical specification and various utility libraries are available under the open source project inCredible on GitHub (https://github.com/sunbird-specs/inCredible).

Conceptual Model

The certificate will capture a relationship between the awarding body, the recipient, the domain, the standard(s) accomplished, the assessor, the evaluation, and the time. The **awarding body** certifies that the **recipient** has **accomplished** specified **standard(s)** in a **domain** based on an **evaluation** conducted by the **assessor** at a **particular time**. Note that a single certificate may be issued for the recipient's accomplishment of multiple standards.

For more details around the full object model (including structural mode of assertion, badge class, profile of awarding body, etc.), please view the open specification link available on GitHub.

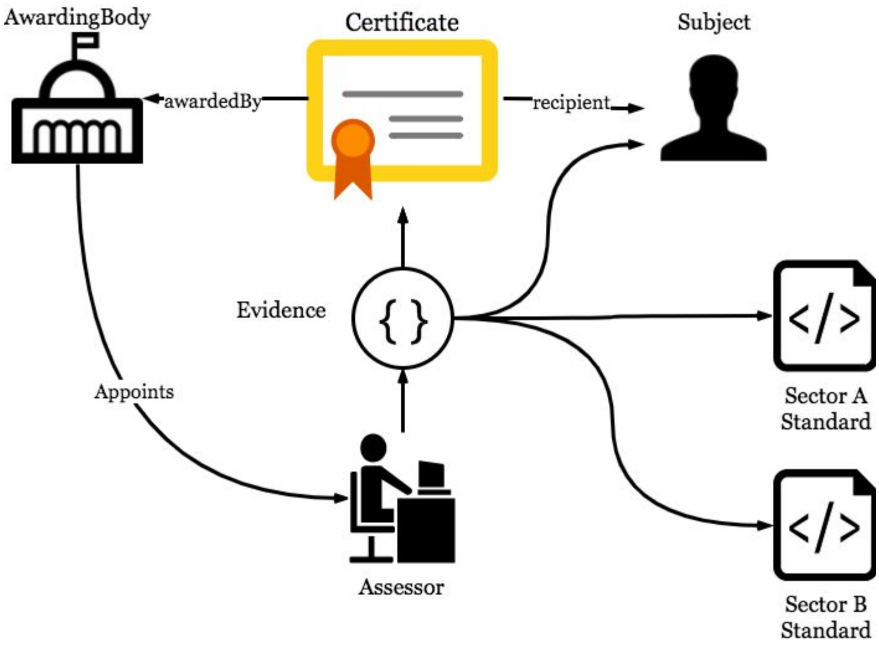


Fig 1 The actors in the certificate ecosystem

Data Modelling Principles

1. All entities in the certificate issuance transaction are represented using machine-readable objects
2. Each object in the data-model is a representation of an entity
3. Strong identifiers[4] will be assigned to all entities. The strong identifiers for the entities should never be altered.

Visual Representation

A visual representation of the credential (rendering) will be generated using data from the machine readable JSON-LD representation and subsequently embedded into the JSON-LD object.

The eCredential specification states that applications are open to using format of choice when embedding the rendered certificate. DGT proposes to adopt PDF documents since they are well-suited for long-term survivability and compatibility, and may also carry metadata inside them. If metadata is added to PDF documents, it must follow or be compatible with the metadata standards defined at egovstandards.gov.in.

QR Codes

Printable representations of the credential will also carry QR codes as an offline-to-online bridge. The QR code will contain credential metadata in its payload which aids in the verification of the credential. There are two broad means of verifying a credential, either by verifying the digital signature of a hosted representation or by verifying the digital signature offline.

1. Where the credential is cloud-hosted,
   a. The QR code should contain the HTTP URI from where the signed JSON-LD document describing the credential can be retrieved.
   b. Once retrieved, this JSON-LD data may be passed to downstream digital systems for signature verification.
   c. It may also be stored offline for further sharing or for other needs including visual comparison against the printed credential.
2. Where the credential cannot be accessed in the cloud,
   a. If the credential JSON document is small enough, the JSON payload may be encoded as a string and embedded into the QR code. To reduce the size of JSON, the payload may be compressed using the GZIP compression algorithm.
   b. If the credential JSON document is larger than 2900 bytes, the QR code should contain essential information to verify the digital signature offline. The

[4] An identifier is any alphanumeric string which has a denotational property of representing the identity of an entity

following items required for signature verification should be inserted into a JSON object and encoded as a string then embedded into the QR code.

i. `@id`: @id of the document
ii. `hash`: hash of the document without the `ocd:signature` element
iii. `key_id`: HTTP URI of the key used to sign the credential
iv. `signatureValue`: bytes of the digital signature generated using (a) and (b)

Entity Identity

As stated in the eCredential specification, an important part of issuing credentials is to identify the entities involved in the process. To issue the credential a few different types of entities participate: institutions, individuals, documents and standards. Since a credential is a permanent document by nature which may be used and remain valid over a long period of time, two broad principles apply for all identifiers:

- **Singularity**: An identifier should resolve to a single entity, for example a person or an institution are single entities.
- **Permanence**: An identifier should not be reassigned to a different entity at a future point.

For example, a phone number is not a good means of identifying a person for the purpose of issuing a credential. A credential must be valid for many years, it may be presented for validation 10, 20 or even 50 years later. A person's phone number may change in the intervening time-period and the number given up by that person may be re-allocated to another different person. Hence an ID, such as a phone number, which does not provide the guarantee of resolving to the same person for the duration of use of the credential is not well-suited for identifying the recipient.

Conversely, a document such as a passport, a ration card or a voter identity card (which will eventually expire) is a better candidate for identifying a person since the passport number or voter id number is not reused and will always continue to represent the same person over time.

DGT Adoption & Usage

Issuing Credentials

Credentials are issued by creating an assertion using the items of data described below. They reference the structure of the assertions in the examples described above

1. **Assertion ID**: Each assertion must be given a unique id.

2. **Awarding body ID**: The awarding body's identity may either be represented using a tag URI or using an HTTP URI to a JSON-LD object containing the awarding body's profile.
3. **Awarding body Public Key**: The awarding body's public key from the cryptographic key pair is embedded into the certificate for verifiability.
4. **Recipient ID**: The recipient may be identified by other strong identifiers. Where the information in the identifier is sensitive, the identifier can be salted and hashed for security.
5. **Evidence**: The awarding body collects evidence from the assessors of the trainee. The evidence may optionally be signed. The awarding body must ensure that
    a. The subject of the evaluation conducted is the same person to whom the credentials are being issued. The awarding body can do this by comparing the id of the evidence object's subject with the id of the recipient.
    b. If the evidence is signed by the assessors, each evidence's signature can be verified by using the assessor's publicKey embedded in the evidence.
6. **Signature**: Finally, the awarding body uses their own private key to generate a signature for the assertion data and inserts that signature to the assertion. In the event that there is a signatory to the certificate who is also applying a digital signature, the unsigned assertion is signed using the signatory's private key as well. Both signatures are then included in the list of signatures for the certificate. See full specifications for details on the signing algorithm.

Signing and Security of Private Key

Signing a certificate is a process by which a one-way digest of the assertion object is computed and is then cryptographically signed (encryption) using the awarding body's private key. The signature suite used will specify the digest and the cryptographic functions which are to be applied (suggestion is to use LinkedDataSignature2015[5]).

The private key used for signing must be maintained in a highly secure repository and should be transferred only via secure channels. This is to ensure that duplicate/fake certificates cannot be issued by anyone else. During application usage the keys should be maintained in the secure area such as an HSM. The data to be signed using the private key should be sent for signing and the signed value returned.

Delivery and Storage of Credentials

Delivery mechanisms for credential documents can vary based on the context where they are awarded. A certificate for an online course may be awarded immediately in the browser, while an offline ITI course with written exams may have an alternate method to deliver certificates. Furthermore, these mechanisms are dynamic and change over time.

[5] https://w3c-dvcg.github.io/lds-rsa2018/

New modes of delivery may be developed and present methods may become obsolete. Similar considerations apply to the means of storing the certificate; the recipient may choose from multiple options available for securely storing the digital document.

To empower recipients with a choice of delivery and storage mechanisms and to ensure compatibility with future methods, delivery and storage is independent of the data in the credential. Thus we may use any means to identify the recipient of the credential and independently choose the way it is delivered and stored. Below we consider some well-established delivery and storage options as well as a few emerging technology options such as Blockcerts and uPort.

Email

One mode of delivery may be email. If the recipient's email address is known, and the recipient elects for email delivery, the certificate can be sent to the recipient's email address as an attachment. The recipient is then free to store using any solution available such as a cloud drive, offline storage etc.

Web

An alternate mode of delivery can be via a private URL which allows the recipient to download the JSON-LD credential. The recipient is then free to store using any solution available such as a cloud drive, thumb drive, offline storage etc. The private URL can be sent to the recipient via an SMS message to a mobile device, an email or any other communication channel available to the awarding body and the recipient.

DigiLocker

Certificates can be stored in the cloud using services such as **DigiLocker**. The machine-readable format has a printable representation embedded in it which can be used by client applications to render previews of the credential.

Blockchain

Blockchain applications may also be used to deliver the certificate to the recipient. The awarding body can use a blockchain certificate publishing protocol such as **Blockcerts**[6] which is also compatible with OpenBadges to store certificates on a blockchain as part of transaction metadata. Recipients can then retrieve the certificate from the blockchain and store as per their choice.

Wallet

Application developers can create mobile wallets for storing credentials. The JSON-LD document containing the certificate can be imported into any number of such applications to manage accomplishments and credentials. The embedded printable representation may be used by wallet applications to render previews of the credential.

[6] https://www.blockcerts.org

uPort

uPort is a toolkit for building distributed applications on top of the Ethereum blockchain. uPort applications can issue credentials to a user which are then attached to the user's profile. The certificate spec described above can be linked into a uPort message which is transported a JSON Web Token (JWT). The JWT contains signed-data as a `claim` which can be the assertion JSON object.

Verifying Authenticity of a Certificate

A certificate will be authenticated along three dimensions.

First, verify that the certificate has been awarded by the awarding body.

1. The certificate contains one or more signatures in the signature field. The signature should be encrypted using the awarding body's private key.
2. Decrypt the signature using the awarding body's public key which returns the digest of the message.
3. The digest of the message is computed and compared with the decrypted digest.
4. If the two digests match, the signature is verified.

Second, verify that the certificate is optionally digitally signed by the signatory.

1. The certificate may also contain the signatory's digital signature in the signature field. The signature is encrypted using the signatory's private key.

Finally, if the certificate contains signed evidence, verify the assessor's signature in each item of evidence in certificate.

1. The credential contains one or more items of evidence which contain signatures using the assessor's private key.
2. The signature can be verified as above using the assessor's public key.
3. The subject of the evidence must be the same as the recipient of the certificate.

Note that when authenticating the physical certificate, downloading the machine readable version from the URL contained in its QR code is a first step. If the URL resolution fails, it cannot be assumed that the certificate is invalid, the URL may be unavailable for many reasons. In this scenario, the authenticity of the physical certificate must be verified via other means.

Portability of Certificates

The accomplishments in the certificate identify standards, levels and criteria which are evaluated by an assessor. This allows the consumer of the certificate to compare competencies against desired skills using the same standard, level and criteria as a reference.

Permanence

To ensure that the authenticity of a certificate is verifiable without needing external data, the certificate payload carries the public keys required to verify signatures.

Key Management

Public keys for the awarding bodies could be cloud-hosted by each signing body. For instance, each Sector Skill Council (SSC) could maintain its own public keys in the cloud where they can be accessed by anyone trying to verify a certificate awarded by the SSC. However, if signing keys are cloud-hosted and the cloud location is embedded inside the certificate then any change in the location of the key will invalidate certificates. Awarding bodies may or may not be able to maintain a permanent location for their keys metadata. This could be worked around by either employing a key broker service which enables keys to be discovered after an awarding body has changed its location or alternatively by a capable entity providing a secure repository of public keys for all awarding bodies as an ecosystem service.

Sample Certificates

For reference, a sample certificate indicating how the open eCredential specification could be leveraged for degree completion and a marksheet are shown below. Further examples are in the annex.

Degree Completion

A university degree certificate is awarded after completion of the requirements for a degree. Such a certificate may reference other credentials as evidence. When a certificate references another certificate, the reference is encoded as a JSON reference object. The certificate below references each semester in the curriculum as evidence towards completing a degree. Other degree certificates may choose alternate evidence which is accumulated towards a degree. A certificate may freely mix **`AssessedEvidence`** and **`Evidence`** which references other certificates in its **`evidence`** array.

Attributes

1. Evidence links to other certificates which are referenced by **`urn:uuid`** URIs. The referenced certificates are not embedded into the document. However, **`AlignmentObjects`** provide consumers with information about the content of the referenced certificate.
2. The **`genre`** field of the Evidence is the string certificate.

Sample

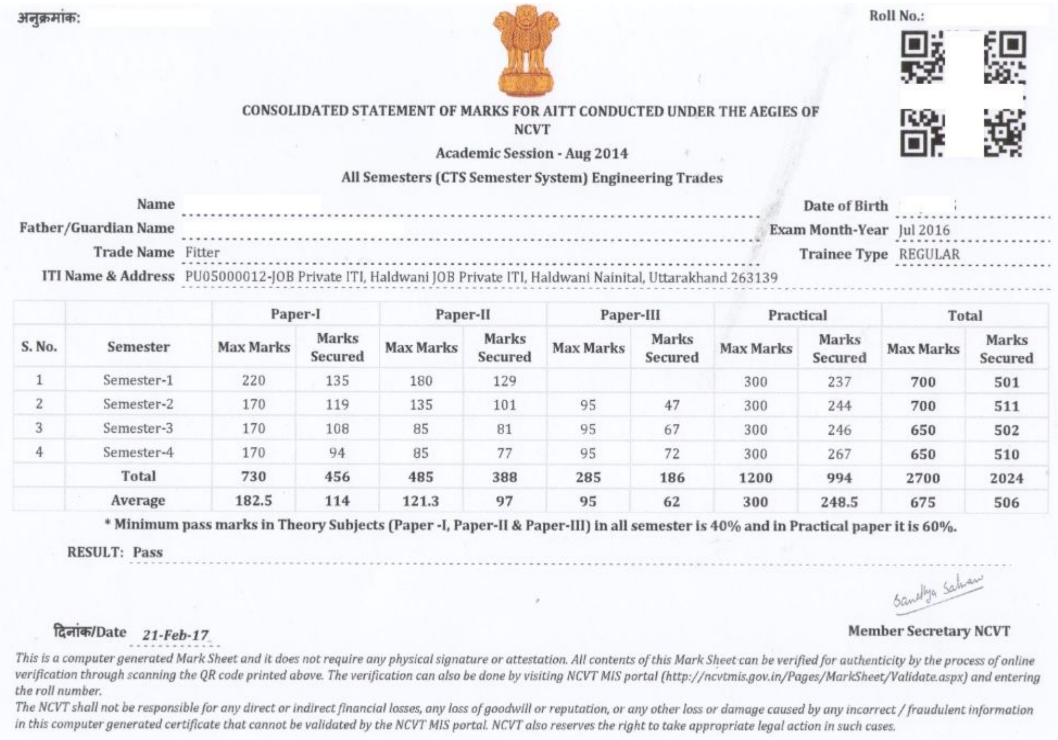
```
{
  "id": "urn:uuid:1c0af19b-df85-42f3-9441-8a390b6c1589",
  "type": ["Assertion", "Extension", "CertificateExtension"],
  "recipient": {
    "type": "composite",
    "components": [{
      "annotation": "urn",
      "identity": "urn:in.gov.eci.voterid:<Recipient voter id>",
    }, {
      "type": "photo",
      "identity": "data:image/jpg;base64,<... base64 encoded image ...>",
    }],
    "name": "<Name of recipient>",
  },
  "badge": "https://example.university.org/certs/degree/bvoc.json",
  "awardedOn": "2019-05-21T10:21:43.087UTC",
  "image": "https://example.university.org/certs/1c0af19b8a390b6c1589.png",
  "narrative": "<Recipient name> has successfully completed 6 (six) semesters
of B. Voc curriculum"
  "evidence": [{                    <<<<<     1. Evidence links to certificates
    "type": "Evidence",
    "id": "urn:uuid:8db760b1-1348-4edd-8dfe-2c29799de4b2",
    "name": "Semester 1",
    "genre": "certificate",         <<<<<            2. Genre is a certificate
    "alignment": {
      "targetName": "Semester 1",
      "targetURL": "https://example.university.org/certs/bvoc/semesters/1",
      "targetDescription": " ... ",
      "targetFramework": "B. Voc Semster Curriculum",
      "targetCode": "BVOC/S/1"
    }
  }, ... {
    "type": "Evidence",
    "id": "urn:uuid:0b3b0c30-c4f0-4075-b663-970cf9768cf0",
    "name": "Semester 6 ",
    "genre": "certificate",
    "alignment": {
      "targetName": "Semester 6",
      "targetURL": "https://example.university.org/certs/bvoc/semsesters/6",
      "targetDescription": " ... ",
      "targetFramework": "B. Voc Semester Curriculum",
      "targetCode": "BVOC/S/6"
    },
  }],
  "verification": {
    "type": "LinkedDataSignatures"
  },
  "signatory": ["https://example.ncvet.org/p/secretary/1"],
  "printUri": "data:image/png;base64,<png-data>",
  "signature": [{
    ... signature of the awarding body ...
  }]
}
```

```
https://example.ncvet.org/p/secretary/1
  {
    "type": ["urn", "Extension", "SignatoryExtension"],
    "identity": "urn:in-dl-dl:<Delhi DL #>",
    "name": "<Name of signatory>",
    "image": "https://example.ncvet.org/p/secretary-sign-image.jpg",
    "designation": "Member Secretary, NCVT"
}
```

Table 5: JSON-LD representation of a University degree certificates

Graduation Marks Certificate

In this sample we show a sample graduation marks certificate which describes a student's performance in multiple subjects as part of a larger achievement.



अनुक्रमांक:

Roll No.:

CONSOLIDATED STATEMENT OF MARKS FOR AITT CONDUCTED UNDER THE AEGIES OF NCVT

Academic Session - Aug 2014

All Semesters (CTS Semester System) Engineering Trades

Name		Date of Birth	
Father/Guardian Name		Exam Month-Year	Jul 2016
Trade Name	Fitter	Trainee Type	REGULAR
ITI Name & Address	PU05000012-JOB Private ITI, Haldwani JOB Private ITI, Haldwani Nainital, Uttarakhand 263139		

		Paper-I		Paper-II		Paper-III		Practical		Total	
S. No.	Semester	Max Marks	Marks Secured	Max Marks	Marks Secured	Max Marks	Marks Secured	Max Marks	Marks Secured	Max Marks	Marks Secured
1	Semester-1	220	135	180	129			300	237	700	501
2	Semester-2	170	119	135	101	95	47	300	244	700	511
3	Semester-3	170	108	85	81	95	67	300	246	650	502
4	Semester-4	170	94	85	77	95	72	300	267	650	510
	Total	730	456	485	388	285	186	1200	994	2700	2024
	Average	182.5	114	121.3	97	95	62	300	248.5	675	506

* Minimum pass marks in Theory Subjects (Paper -I, Paper-II & Paper-III) in all semester is 40% and in Practical paper it is 60%.

RESULT: Pass

दिनांक/Date 21-Feb-17

Member Secretary NCVT

This is a computer generated Mark Sheet and it does not require any physical signature or attestation. All contents of this Mark Sheet can be verified for authenticity by the process of online verification through scanning the QR code printed above. The verification can also be done by visiting NCVT MIS portal (http://ncvtmis.gov.in/Pages/MarkSheet/Validate.aspx) and entering the roll number.

The NCVT shall not be responsible for any direct or indirect financial losses, any loss of goodwill or reputation, or any other loss or damage caused by any incorrect / fraudulent information in this computer generated certificate that cannot be validated by the NCVT MIS portal. NCVT also reserves the right to take appropriate legal action in such cases.

Fig 5: Sample Consolidated Marksheet

For brevity, previously described objects (**`BadgeClass`** and **`Assessor`**) have been represented via their URIs, and repetitive elements have been truncated. For maximum portability and permanence, the assertion should have all these entity URIs dereferenced and their JSON-LD representations embedded into the credential.

Attributes

1. Multiple items of evidence per subject are linked into a single certificate
2. Evidence is described using **`alignmentObject`** which link to specific items in the curriculum.
3. PrintURI embeds a printable document for the assertion into the JSON-LD object.

Sample

```
{
  "id": "urn:uuid:1c0af19b-df85-42f3-9441-8a390b6c1589",
  "type": ["Assertion", "Extension", "CertificateExtension"],
  "recipient": {
    "type": ["Identity","Extension","extensions:CompositeIdentity"]
    "components": [{
      "type": ["Identity","Extension","extensions:CompositeIdentity"]
      "annotation": "FATHER NAME",
      "identity": "<Name of father>",
    }, {
      "type": ["Identity","Extension","extensions:CompositeIdentity"],
      "annotation": "dob”,
      "identity": "<DOB of recipient>",
    }, {
      "type": ["Identity","Extension","extensions:CompositeIdentity"],
      "annotation": "urn",
      "identity": "urn:in.gov.msde.dgt-rollno:<Roll # of the recipient>",
    }],
    "name": "<Name of recipient>",
  },
  "badge": "https://example.examboard.org/certs/csma.json",
  "awardedOn": "2017-02-21T10:21:43.087UTC",
  "image": "https://example.examboard.org/certs/1c0af19b8a390b6c1589.png",
  "narrative": "Passed",
  "evidence": [{                      <<<<<             1. Multiple evidence
    "type": ["Evidence", "Extension", "extensions:AssessedEvidence"],
    "id": "urn:uuid:02644c88-d2b7-41ef-a78c-6adf7fbdb268",
    "name": "Semester 1 Mathematics",
    "assessment": {
      "type": ["Assessment","Extension","extensions:MarksAssessment"]
      "value": "135",
      "maxValue": "220",
      "minValue": "0",
      "passValue": "88",
    },
    "assessedBy": "https://example.examboard.org/assessor.json",
    "assessedOn": "2015-12-22T6:30:00Z",
    "alignment": [{                   <<<<<           2. Evidence descriptors
      "targetName": "Semester 1 Mathematics",
      "targetURL": "https://example.examboard.org/fitter/maths/s1",
      "targetDescription": " ... ",
      "targetFramework": "Examboard Semester Curriculum",
      "targetCode": "MATHS/S1"
    }],
    "signature": {
      ... optional signature of the assessor ...
    }
  }, ..., {
    "type": ["Evidence", "Extension", "extensions:AssessedEvidence"],
    "id": "urn:uuid:4ccc8f7b-30a4-466f-a50a-aef08378ae65",
    "name": "Semester 4 Practical",
    "assessment": {
      "type": ["Assessment","Extension","extensions:MarksAssessment"]
      "value": "267",
      "maxValue": "300",
      "minValue": "0",
      "passValue": "180",
    },
    "assessedBy": "https://example.schoolboard.org/assessor.json",
    "assessedOn": "2017-02-19T06:30:00Z",
    "alignment": {
      "targetName": "Semester 4 Practical",
      "targetURL": "https://example.examboard.org/fitter/practical/s4",
      "targetDescription": " ... ",
      "targetFramework": "Examboard Semester Curriculum",
      "targetCode": "PRAC/S4"
    },
  }, {
    "type": ["Evidence", "Extension", "extensions:AssessedEvidence"],
    "id": "urn:uuid:4ccc8f7b-30a4-466f-a50a-aef08378ae65",
    "name": "Semester 4 Total",
    "assessment": {
      "type": ["Assessment","Extension","extensions:MarksAssessment"]
      "value": "510",
      "maxValue": "650",
      "minValue": "0"
    },
    "assessedBy": "https://example.schoolboard.org/assessor.json",
    "assessedOn": "2017-02-19T06:30:00Z",
    "alignment": {
      "targetName": "Semester 4 Total",
      "targetURL": "https://example.examboard.org/fitter/total/s4",
      "targetDescription": " ... ",
      "targetFramework": "Examboard Semester Curriculum",
      "targetCode": "TOT/S4"
    },
  }],
  "verification": {
    "type": "LinkedDataSignatures"
  },
  "signatory": "https://example.ncvet.org/p/secretary/1", <<<<<  4. Official
signatory
  "printUri": "data:application/pdf;base64,<pdf-data>", <<<<<  3. Printable
representation
  "signature": [{
    ... signature of the awarding body ...
  }],
}
```

```
https://example.ncvet.org/p/secretary/1
{
    "type": ["urn", "Extension", "SignatoryExtension"],
    "name": "<Name of signatory>",
    "image": "https://example.ncvet.org/p/secretary-sign-image.jpg",
    "identity": "urn:in-dl-dl:<DL DL #>",
    "designation": "Member Secretary, NCVT"
}
```

Table 4: JSON-LD representation of a graduation marks certificate

Benefits of Ecosystem-Wide Adoption

In order to make the benefits of electronic credentialing a reality across the jobs and skilling ecosystem, the Ministry of Skill Development urges other institutions that upskill and train aspirers and workers (including employers) to adopt the open standard for digital credentialing. This could have powerful network effects on the behaviour of skill data sharing and aggregation which ultimately serve both individuals' and employers/skill trainers' interests. For instance, employers could reliably ascertain the full set of contextualized previous training and work experience before interviewing a candidate. Existing job matching portals could better filter or automatically match recommended candidates for roles based on verified credentials. New companies could be built that automate aggregation of experience and training certificates of individuals without digital literacy themselves into competitive digital CVs. Finally, the new data might even shed light on the trends associated with demand flux for certain skills, better informing them on what skills to pursue at the outset of their careers.

The first phase of adoption could be incorporating this certificate specification into the existing certificate issuance systems of training providers and universities. Following this, independent assessment agencies could start evaluating individuals against these standards (or publish their own to be more competitive) and begin issuing electronic credentials in this form for employers to evaluate. To enable scale of access and use of the credential, it is critical to have a multiplicity of standards across and within industries which evolve quickly based on emerging market needs, and can be created to meet hyper local requirements. Finally, employers could adopt the credential standard for learning on the job, if the right policy incentives are put in place. In parallel, the ecosystem could also design CV Markup Language, which enables verifiable job history experience records be to digitally attested and shared with future employers.

Conclusion

This document describes DGT's proposed adoption of an electronic schema-based standard for describing credentials data in a machine-readable format along with its printable human-friendly version to make credential exchange between digital agents open and reliable. Credentials issued according to this specification are secured using digital signatures for severless certificate verification. Having an ecosystem shift towards a data-driven approach through the use of micro e-Credentials could enhance the level of information, trust, and resource efficiencies of the skill ecosystem, ultimately serving both aspirers' and employers or skill trainers' interests to transition India into a high skills equilibrium.

Annex

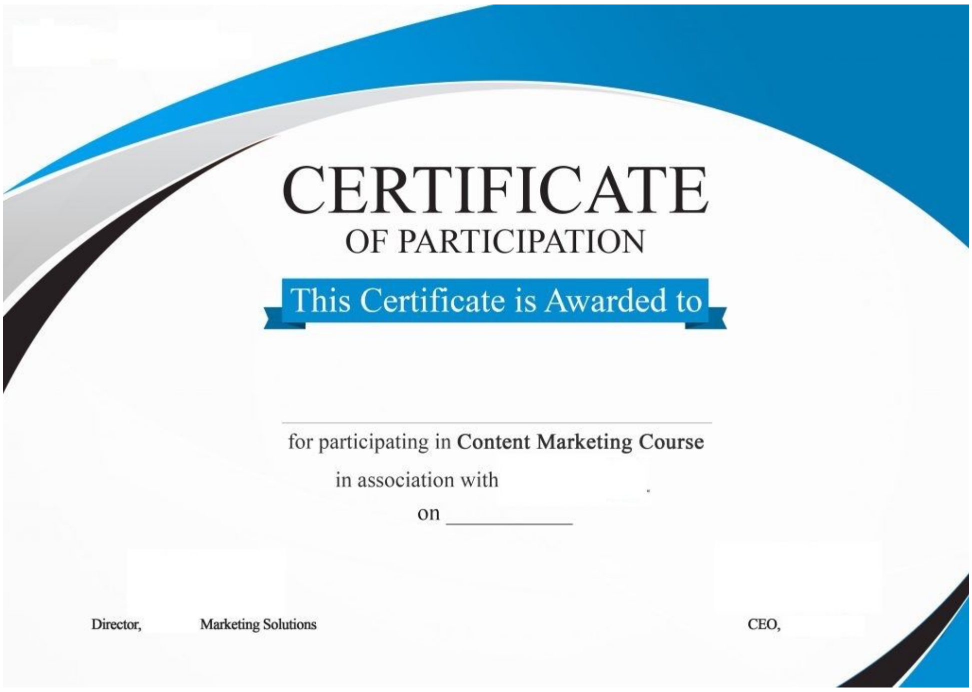
References

1. Project inCredible - https://github.com/sunbird-specs/inCredible
2. OpenBadges v2: https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/
    a. examples: https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/examples/
3. JSON-LD Syntax: https://w3c.github.io/json-ld-syntax/#introduction
4. JSON-LD: https://www.w3.org/TR/json-ld/
5. RDF: https://www.w3.org/RDF/
6. RDF Schema: https://www.w3.org/TR/rdf-schema
7. RDFa: https://www.w3.org/TR/rdfa-primer/
8. Turtle: https://www.w3.org/TR/turtle/
9. Uniform Resource Names: https://tools.ietf.org/html/rfc8141
10. The Tag URI scheme: https://tools.ietf.org/html/rfc4151
11. Schema.org Full Vocabulary: https://schema.org/docs/full.html
12. Use of '@id' vs 'identifier': https://schema.org/docs/datamodel.html#identifierBg
13. Linked Data Signatures: https://w3c-dvcg.github.io/ld-signatures/
14. Rsa Signature Suite 2018: https://w3c-dvcg.github.io/lds-rsa2018/
15. Digilocker: https://digilocker.gov.in/
16. National Academic Depository: http://nad.gov.in/
17. Blockcerts: https://www.blockcerts.org
18. uPort application development kit: https://www.uport.me/
19. Linked Data Platform: https://www.w3.org/TR/ldp/
20. Architecture of the Web: https://www.w3.org/TR/webarch
21. Web Payments Vocabulary: https://web-payments.org/vocabs/security

Sample Certificates

1. Ad-Hoc Certificate

A simple example of an assertion which certifies that a person has participated in an event.



CERTIFICATE

OF PARTICIPATION

This Certificate is Awarded to

for participating in **Content Marketing Course**

in association with

on ____________

Director, Marketing Solutions

CEO,

Fig 3: Ad-hoc Participation Certificate

Attributes

1. The **`@id`** of the assertion is a URL where this credential can be downloaded for verification.
2. Awarded to a recipient identified by a hashed email.
3. Since the participation credential is an ad-hoc certificate which may not be issued multiple times, the badge class is identified by a **`urn:uuid`** class URI ([see note on BadgeClass `@id`]). The BadgeClass document is embedded into the assertion.
4. The badge image is embedded into the certificate as a data URI representing a base64-encoded PNG image.
5. Issuer is identified by an **`@id`** which is a tag URI which uses the issuer's domain name.
6. The assertion employs hosted verification and is thus not signed.

Sample

```
{
  "id": "https://www.example.com/certs/2018/9900001234.json",
  "type": ["Assertion", “Extension”, “extensions:CertificateExtension”],
  "recipient": {                           <<<<<          Recipient identity
    "type": "email",
    "hashed": "true",
    "identity": "sha256$bdeffdadbd28657adcead3825fdb23875dab8e928ad8d68f6",
    "salt": "bluewater",
    "name": "<Name of the recipient>"
  },
  "badge": {                                  <<<<<       BadgeClass inline
    "id": "urn:uuid:ec58b28e-a6ab-49c2-a24d-ebefa02476cd",
    "type": ["BadgeClass"],
    "name": "Certificate of Participation",
    "description": "Content Marketing Course",
    "issuer": "http://example.come/awardingBody/1"
  },
  "issuedOn": "2018-08-11T09:27:30.613UTC",
  "narrative": "Awarded for participating in Content Marketing Course in
association with Partner Marketing Solutions",
  "verification": {                           <<<<<       Hosted verification
    "type": "HostedBadge",
    "allowedOrigins": "*"
  },
  "signatory": [                         <<<<<            Official signatory
      “http://example.com/signatories/ceoSignature/1”,
      “http://example2.com/directors/mktDirectorSignature/1”
  ]
}
```

```
http://example.come/awardingBody/1
    {
      "type": "Profile",
      "id": "tag:example.com,2009-11-28:#profile.json"  << Issuer identity
      "name": "Example Training Corp",
      "image": "https://www.example.com/images/logo.png",
      "email": "certificates@example.com",
    }
```

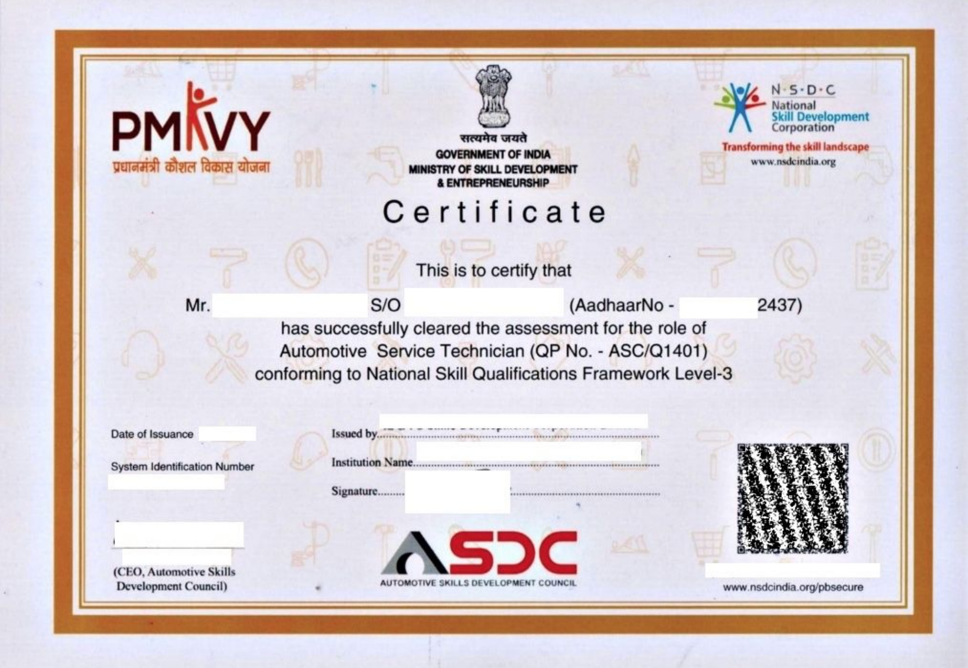
```
http://example.com/signatories/ceoSignature/1
{
    "type": ["Profile", "Extension", "extensions:SignatoryExtension"],
    "components": [{
      "type": "name",
      "annotation": "FATHER",
      "identity": "<signatory’s father’s name>"
    }, {
      "type": "photo",
      "identity": "data:image/jpeg;base64,<base64 jpg image>"
    }],
    "name": "<Name of signatory>",
    "image": "https://example.com/p/ceo/sign-image.jpg",
    "designation": "CEO, Example Training Corp"
}
```

```
http://example2.com/directors/mktDirectorSignature/1
{
    "type": ["Profile", "Extension", "extensions:SignatoryExtension"],
    "name": "<Name of signatory>",
    "image": "https://example2.com/edb/l:dir/mkt/sign-image.jpg",
    "identity": "urn:in.gov.eci.voter:<Voter #>",
    "designation": "Director, Partner Marketing Solutions",
}
```

Table 2: JSON representation of an ad-hoc certificate

2. Course Completion

This example details the data added to a certificate for completion of a course which aligns to more than one academic standard. The BadgeClass contains details of the alignments to the target standards. The evidence for the certificate is represented in the form of the grade received for the course. While this example includes evidence aligned to one QP of the NSQF framework, the issuer is free to include multiple such items which detail the recipient's performance across multiple QPs if such granularity is so desired.



PMKVY
प्रधानमंत्री कौशल विकास योजना

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape
www.nsdcindia.org

Certificate

This is to certify that

Mr. [redacted] S/O [redacted] (AadhaarNo - [redacted] 2437)
has successfully cleared the assessment for the role of
Automotive Service Technician (QP No. - ASC/Q1401)
conforming to National Skill Qualifications Framework Level-3

Date of Issuance [redacted]

System Identification Number [redacted]

Issued by [redacted]

Institution Name [redacted]

Signature [redacted]

[redacted]

(CEO, Automotive Skills Development Council)

ASDC
AUTOMOTIVE SKILLS DEVELOPMENT COUNCIL

[redacted]

www.nsdcindia.org/pbsecure

Fig 4: Sample Course Completion Certificate

Attributes

1. In the illustration, the recipient is a reference to the subject of the evidence collected. The subject is identified by a composite identity of name, father's name and the last digits of an Aadhaar number.
2. The certificate has an issuer, assessor and trainer institution profiles embedded. The issuer and assessor provide signed documents, hence are represented using the SignatorExtension class. These objects contain **`publicKey`** properties to enable validation of the signatures.
3. The course is aligned to a NSQF qualification which in turn comprises of multiple NOS standards
4. Though the illustration above does not contain this, the evidence below encodes the grade received for the course based on an assessment
5. The assessment evidence is signed by the assessor (using their private key). The **`Signature`** class contains a **`creator`** property which references the **`@id`** of the assessor's **`publicKey`**

6. The signatory of the certificate is the CEO of the Automotive Skills Development Council
7. The certificate is signed by the awarding body (using their private key). The **`Signature`** class contains a **`creator`** property which references the **`@id`** of the awarding body's **`publicKey`**

Sample

```
{
  "id": "urn:uuid:1c0af19b-df85-42f3-9441-8a390b6c1589",
  "type": ["Assertion", "Extension", "extensions:CertificateExtension"],
  "recipient": {                          <<<<<     1. Reference to evidence subject
    "type": ["Identity","Extension","extensions:CompositeIdentity"]
    "name": "<Name of recipient>",
    "components": [{
        "type": ["Identity","Extension","extensions:CompositeIdentity"]
        "annotation": "FATHER",
        "identity": "<Name of father>"
      }, {
        "type": ["Identity","Extension","extensions:CompositeIdentity"]
        "annotation": "MASKED",
        "identity": "urn:in.gov.uidai.aadhaar:XXXX-XXXXXXXX-2437"
      }]
  },
  "badge": {
    "id": "https://example.pasdc.org/certs/courses/ASCL3",
    "type": "BadgeClass",
    "name": "Automotive Service Technician Course",
    "description": " ... ",
    "image": "data:image/png;base64,<base64-encoded-png-data>",
    "criteria": {
      "type": "Criteria",
      "narrative": "Successfully cleared course for Automotive Service
Technician"
    },
    "issuer":  "https://certs.example.gov/o/pasdc/0781ABCDEAC191", <<<<< 2.
URL to an Awarding body profile
    "alignment": [{                       <<<<<          3. Alignment to standards
      "targetName": "Automotive Service Technician - Level 3",
      "targetURL": "https://www.nqr.gov.in/ASC/Q1401",
      "targetDescription": " ... ",
      "targetFramework": "NSQF",
      "targetCode": "ASC/Q1401"
    }, {
      "targetName": " Assist in vehicle service and maintenance",
      "targetURL": "https://www.nqr.gov.in/ASC/N1401",
      "targetDescription": " ... ",
      "targetFramework": "NOS",
      "targetCode": "ASC/N1401"
    }, {
      "targetName": "Plan and organise work to meet expected outcomes",
      "targetURL": "https://www.nqr.gov.in/ASC/N0001",
      "targetDescription": " ... ",
      "targetFramework": "NOS",
      "targetCode": "ASC/N0001"
    }]
  },
  "awardedOn": "2018-10-29T10:21:43.087UTC",
  "image": "https://example.pasdc.org/certs/1c0af19b8a390b6c1589.png",
  "evidence": [{
    "id": "urn:uuid:f4e30fc7-fd1f-4afb-9d34-26b92e0078c3",
    "type": ["Evidence", "Extension", "extensions:TrainingEvidence"],
    "name": "Training Course",
    "trainedBy": https://trainer.example.edu/PTE/profile, <<<<< 2. Training
institution profile
    "duration": {
      "startDate": "2018-07-25",
      "endDate": "2018-10-22"
    },
    "session": "2018 Aug-Oct Batch #3"
  },{
    "id": "urn:uuid:02644c88-d2b7-41ef-a78c-6adf7fbdb268",
    "type": ["Evidence", "Extension", "AssessedEvidence"],
    "name": "Course Grade",
    "assessment": {                    <<<<<          4. Representing the grade
      "type": ["Assessment","Extension","extensions:GradeAssessment"],
      "value": "B+",
      "maxValue": "A+",
      "related": {
        "type": ["equivalent", "percentage"],
        "value": "72"
      }
    },
    "assessedBy":"https://certs.example.gov/o/acmeauto/0781ABCDEAC191",<<<<<
                                       2.. Embedded assessor profile
    "assessedOn": "2018-10-19T6:30:00Z",
    "signature": {                     <<<<<       5. Assessor’s digital signature
      "type": "LinkedDataSignature2015",
      "creator": "https://example.assessor.org/keys/1",
      "created": "2018-10-23T20:21:34Z",
      "signatureValue": "LTQzNTVVmMm3ODM3QzNmtlYzIZD34GIyZGk="
    }
  }],
  "verification": {
    "type": "LinkedDataSignature2015"
  },
  "signatory": ["http://example.com/gov/ka/dot/ceo/1"],     <<<<< 6. Official
signatory
  "printUri": "data:image/jpeg;base64,<jpg-data>",
  "signature": [{                      <<<<<7. Awarding body’s digital signature
    "type": "LinkedDataSignature2015",
    "created": "2018-10-23T10:21:40.817UTC",
    "creator": "https://example.pasdc.org/keys/1",
    "signatureValue": "OGQzNGVkMzVmMmQ3ODIyYzI4ZDY3NjI4NTIyZTk="
  }]
}
```

```
"https://certs.example.gov/o/pasdc/0781ABCDEAC191"
{
      "type": ["AwardingBody", "Extension", "SignatoryExtension"],
      "id": "https://certs.example.gov/o/pasdc/0781ABCDEAC191",
      "name": "Partner & Associate Skills Development Corporation",
      "image": "https://example.pasdc.org/images/logo.png",
      "publicKey": {                <<<<<      2. Awarding body publicKey
        "id": "https://example.pasdc.org/keys/1",
        "type": "CryptographicKey",
        "owner": "https://certs.example.gov/o/pasdc/0781ABCDEAC191",
        "publicKeyPem": "-----BEGIN PUBLIC KEY-----\n... <<INSERT KEY>>
...\n-----END PUBLIC KEY-----\n"
}
```

```
https://trainer.example.edu/PTE/profile
   {
      "type": "Profile",
      "id": "https://trainer.example.edu/about.json",
      "name": "Partner Training Institute",
      "image": "https://trainer.example.edu/logo.jpg"
   }
```

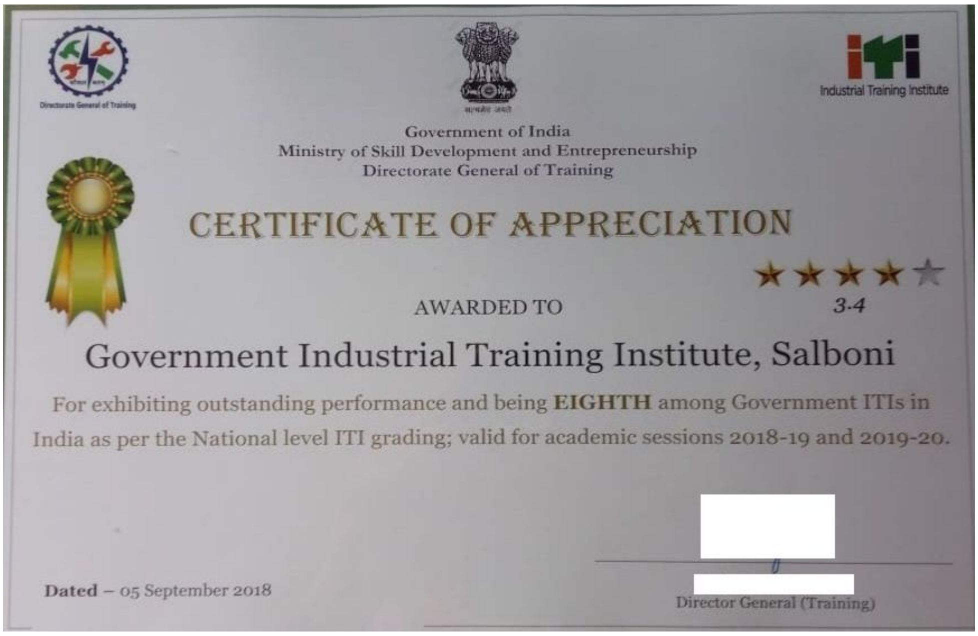
```
https://certs.example.gov/o/acmeauto/0781ABCDEAC191
   {
      "type": ["Profile", "Extension", "SignatoryExtension"],
      "id": "https://certs.example.gov/o/acmeauto/0781ABCDEAC191",
      "name": "Acme Automotive Assessments Institute",
      "image": "https://example.assessor.org/cert-logo.png",
      "publicKey": {                <<<<<          2. Assessor publicKey
        "id": "https://example.assessor.org/keys/1",
        "type": "CryptographicKey",
        "owner": "https://certs.example.gov/o/acmeauto/0781ABCDEAC191",
        "publicKeyPem": "-----BEGIN PUBLIC KEY-----\n... <<INSERT KEY>>
...\n-----END PUBLIC KEY-----\n"
      }
    }
```

```
  {
    "type": ["IdentityObject", "Extension", "extensions:SignatoryExtension"],
    "identity": "urn:in.gov.ka-dot.dl:<KA DL #>",
    "name": "<Name of signatory>",
    "image": "https://example.asdc.org/p/ceo/sign-image.jpg",
    "designation": "CEO, Automotive Skills Development Council"
  }
```

Table 3: JSON-LD representation of a course completion certificate

3. Recognition of Performance

Building on top of the examples, we inspect a certificate of appreciation which recognises the standard of the recipient's performance. In this example the recipient of the certificate is a training institute.



Directorate General of Training

Industrial Training Institute

Government of India
Ministry of Skill Development and Entrepreneurship
Directorate General of Training

CERTIFICATE OF APPRECIATION

★★★★☆
3.4

AWARDED TO

Government Industrial Training Institute, Salboni

For exhibiting outstanding performance and being **EIGHTH** among Government ITIs in India as per the National level ITI grading; valid for academic sessions 2018-19 and 2019-20.

[redacted]

[redacted]

Dated – 05 September 2018

Director General (Training)

Fig 6: Sample Certificate of Merit/Rank/Appreciation

Attributes

1. The credential's document identifier is a tag URI where the ID namespace combines the domain of the awarding body with the registration date and adds a id-type (dgt.certificate).
2. Since performance may be awarded systematically, a hosted badge class is created and identified by its URL (the class is also embedded into the assertion).
3. Awarding body is identified by an HTTP URL, along with essential properties of **`name`** and **`publicKey`**. The URL should return a JSON-LD object which can contain additional properties of the awarding body.
4. A signatory to the certificate is added.
5. The certificate is signed with the awarding body's private key.

Sample

```
{
  "id": "tag:msde.gov.in,2015-02-27:dgt.certificate/1800122349",
  "type": ["Assertion", "Extension", "CertificateExtension"],
  "recipient": {
    "type": "urn",
    "hashed": "false",
    "identity": "urn:in.gov.gstn.id:Z000000000000001",
    "name": "Government Industrial Training Institute, Salboni"
  },
  "badge": {                          <<<<<       1. Hosted BadgeClass, URL ID
    "id": "https://dgt.example.gov.in/certs/iti/grading/appreciate",
    "type": "BadgeClass",
    "name": "Certificate of Appreciation in National Level ITI Grading",
    "description": " ... ",
    "image": "data:image/png;base64,<base64-encoded-png-data>",
    "criteria": {
      "type": "Criteria",
      "narrative": "For exhibiting outstanding performance"
    },
    "issuer": "https://certs.example.gov/o/dgt/HJ5327VB1247G" <<<<< 2.
Awarding body with URL ID, publicKey
  "awardedOn": "2018-09-05T10:21:43.087UTC",
  "validFrom": "2018-09-01",
  "expires": "2020-06",
  "evidence": {                        <<<<<       Unsigned AssessedEvidence
    "type": ["Evidence", "Extension", "AssessedEvidence"],
    "id": "urn:uuid:02644c88-d2b7-41ef-a78c-6adf7fbdb268",
    "description": "Rank in National ITI Grading",
    "assessment": {
      "type": ["Assessment","Extension","extensions:RankAssessment"]
      "value": "8",
      "maxValue": "1"
    },
    "assessedBy": "https://dgt.example.gov.in/iti-assessor.json",
    "assessedOn": "2018-08-19T6:30:00Z"
  },
  "verification": {
    "type": "LinkedDataSignatures"
  },
  "signatory": ["https://example.com/dgt/1"],  <<<<< 3. Official signatory
  "signature": [{                      <<<<<      4. Awarding body's signatures
    "type": "LinkedDataSignature2015",
    "creator": "https://dgt.example.gov.in/keys/awarding_body.json",
    "created": "2018-10-23T20:21:34Z",
    "signatureValue": "OGQzNGVkMzVmMmQ3ODIyYzI4ZDY3NjI4NTIyZTk="
  }]
}
```

```
https://certs.example.gov/o/dgt/HJ5327VB1247G
    {
      "type": "AwardingBody",
      "id": "https://certs.example.gov/o/dgt/HJ5327VB1247G",
      "name": "Ministry of Skill Development and Entrepreneurship, Directorate
General of Training",
      "publicKey": {
        "id": "https://dgt.example.gov.in/keys/awarding_body.json",
        "type": "Key",
        "owner": "https://certs.example.gov/o/dgt/HJ5327VB1247G",
        "publicKeyPem": "-----BEGIN PUBLIC KEY-----\n... ... ... ...
...\n-----END PUBLIC KEY-----\n",
      }
    }
```

```
https://example.com/dgt/1
{
    "type": ["urn", "Extension", "SignatoryExtension"],
    "name": "<Name of signatory>",
    "identity": "urn:in.gov.msde.dgt-employee-id:GITI2D37A483ADJ452",
    "designation": "Director General (Training)
}
```