# A Simple Specification for a Digital Wallet for W3C Verifiable Credentials in Education and Training

**Anil Ripla**

**Lara Maharaj**

**RCL Global LLC**

**23/07/2025**

## **Abstract**

The wide variations in implementation of the W3C Verifiable Credential (VC) and Decentralized Identifier (DID) specification for applications in education and training has made the development of a wallet application to support these variations very difficult. The W3C specifications are very flexible and allow for different DID Methods, Credential Proof Formats and Cryptographic Algorithms. To support all these methods, formats and algorithms are almost impossible. A narrower subset outlined in this specification will make the adoption of the technology much easier.

This specification for a wallet application allows for a cost effective and simple solution for the implementation of a wallet application to store verifiable credentials. This specification sets out a single DID Method, Credential Proof Format and Cryptographic Algorithm for issuer applications to exchange data with a digital wallet application. It also provides a specific data model for the education and training achievement in alignment with the Open Badges Specification to ensure standardization of the Verifiable Credential data. This specification will allow issuer applications to create Verifiable Credentials for education and training and allow the holders to save these credentials in third party wallet applications.

Contents

[Specification for a Digital Wallet for W3C Verifiable Credentials for Education and Training 1](#_Toc204180877)

[**Abstract** 1](#_Toc204180878)

[**I. Introduction** 3](#_Toc204180879)

[II. Digital Wallet 3](#_Toc204180880)

[III. Verifiable Credentials Eco-system 3](#_Toc204180881)

[Holder 3](#_Toc204180882)

[Issuer 3](#_Toc204180883)

[Verifier 3](#_Toc204180884)

[IV. Specification 3](#_Toc204180885)

[1. Holder and Issuer Identification 3](#_Toc204180886)

[2 Holder DID in the Digital Wallet 6](#_Toc204180887)

[3. Verifiable Credential Data Model 7](#_Toc204180888)

[4. Verifiable Credential Format 9](#_Toc204180889)

[V. Conclusion 12](#_Toc204180890)

[Issuer Application 12](#_Toc204180891)

[Digital Wallet Application 12](#_Toc204180892)

[VI. References 12](#_Toc204180893)

# **I. Introduction**

**This paper outlines a simple specification for a digital wallet to be used to store Verifiable Credentials created for education and training. The W3C Verifiable Credentials Data Model v2.0**[[1]](#endnote-1) **is a specification for the data structure of digital credentials that can be cryptographically verified and shared electronically. Software** applications that interchange data with the digital wallet must follow the requirements of the W3C specification. Such applications may include issuer applications that create verifiable credentials.

# **II. Digital Wallet**

**The digital wallet can be a mobile application, a cloud-based or web application. A mobile digital wallet should be able to function offline without an internet connection.**

# **III. Verifiable Credentials Eco-system**

## Holder

A holder is issued with a Verifiable Credential to demonstrate his/her achievement.

## Issuer

An issuer issues a Verifiable Credential to a holder to recognize the holder’s achievement.

## Verifier

A verifier will review a holder’s credential to decide on the holder’s achievement, e.g., an employer may review a credential to decide on hiring the holder.

# IV. Specification

## 1. Holder and Issuer Identifiers

1.1 Holders and issuers will be identified with a Decentralized Identifier (DID)[[2]](#endnote-2) .

1.2 The DID should be created with the did:jwk[[3]](#endnote-3) method. This is the only DID method supported.

1.3 When creating a did:jwk (Sample 1.1), the RSA[[4]](#endnote-4) cryptographic algorithm should be used with a 2048-bit key size. Only RSA public and private asymmetric keys are supported.

1.4 A DID document (Sample 1.3) will be generated from the did:jwk.

1.5 The public key of the DID owner should be directly obtainable from the DID document as a JSON Web Key (JWK)[[5]](#endnote-5). The JWK (Sample 1.2) must include the public key parameters and should not reference the key from an external source such as a website. A kid will be ignored in a JWK.

* 1. A DID should be in the form of a text (.txt) file. Issuers and holders should be allowed to download and save their DID.
  2. Issuers and holders should be allowed to download and save their private keys. The private key (Sample 1.4) should be in the form of a (.txt) file.

Sample 1.1 : did:jwk

did:jwk:eyJrdHkiOiJSU0EiLCJuIjoicHVYb3VRS1Vha2t2X2JUZWQ4dkNYLU9FTG1jUzhqQ21DWE9WZFp2b3l5c0wxTWMyMWZGSzBxMXBIN1dMRU1hOUFhd1hQSk1sckdEdmcxT0FiS1h0TkMwZ2hHMTR2dzVqQXpieldsb3F3c25jaGlQRk5ENWt6aTNfUmNpYzlxZlpGUnN3aUdjUkNtRHNKUnlqX244MDhVZkNGdkRnYVZzVjlNNVJhMmNZMHlYQkJDM29tRkpJNXBkTEEySTFFRFZuMWJkTzFaRXQtUFY3Z3c0MWFQZHdhNzd2cTBNRkFDaTNyS0wtTEdzWkNxYlo1Q0ZsNjJFMWNYMU5KZmd1d3BoMDJHMEdRSjZIMnhBSFdnU3BkVUtXcTNQdXJrWVl3VGkwTFJXR015Mk5sSzdwVUxPMlFwem1GN2tWRmdhbW5fb0VOMFlhVkoxbVgzVE02UEVHVzZFdDFRIiwiZSI6IkFRQUIifQ

Sample 1.2: Public Json Web Key (JWK) used to create the did:jwk

{

"kty": "RSA",  
 "n": "puXouQKUakkv\_bTed8vCX- OELmcS8jCmCXOVdZvoyysL1Mc21fFK0q1pH7WLEMa9AawXPJMlrGDvg1OAbKXtNC0ghG14vw5jAzbzWloqwsnchiPFND5kzi3\_Rcic9qfZFRswiGcRCmDsJRyj\_n808UfCFvDgaVsV9M5Ra2cY0yXBBC3omFJI5pdLA2I1EDVn1bdO1ZEt-PV7gw41aPdwa77vq0MFACi3rKL-LGsZCqbZ5CFl62E1cX1NJfguwph02G0GQJ6H2xAHWgSpdUKWq3PurkYYwTi0LRWGMy2NlK7pULO2QpzmF7kVFgamn\_oEN0YaVJ1mX3TM6PEGW6Et1Q",  
 "e": "AQAB"  
}

Sample 1.3: DID Document using the did:jwk Method

{  
"@context": [  
 "https://www.w3.org/ns/did/v1",   
 {  
 "@vocab": "https://www.iana.org/assignments/jose#   
 }  
 ],

"id": "did:jwk:eyJrdHkiOiJSU0EiLCJuIjoiOW5iMGtyZFdNUjBBSFhzdjh2dzcybzNvdGZCQ0R fY0 tne nVyY1FzeEYycmJSc2F5VmJXRWVvcEZIOTNyQ3JlR056UjJBQWtMRG9mSWZ2QU1aR2xWOW5WZTIyMXRScmE4NU9vUEdSZVhQWmh2aVQ2WGpXQ2tHY3N5U1ZYZHNrX192R1VNeGF0b2FNM1A1Q1cyRDAxbGJSc1RDVW1EMG50M01mU1lQNkkzVnFuSVQ5eGVSaDBpZGJQQXFkUkQtSVdINDNHMEhsR0JMeWc3QjNfTnlRc2Y1b2RvUkU2b0NwZ09sdVR3bkh6SmptV081RzVGWmFIdnFmZXdYeXhKbmhWYmFLU3BRbGpUUFp1SXZQMERLX3FvV1h4MFNYUk4tbmJuUkxtaG5QNUQwM0lZenR1R1J4RVM3djdPdG5kY2JSOUNLaWNaRjNJdUdoOS0zdTJRdHY5UlNRIiwiZSI6IkFRQUIifQ",  
"verificationMethod": [  
 {  
 "id": "#0",  
 "type": "JsonWebKey2020",  
 "controller": "did:jwk:eyJrdHkiOiJSU0EiLCJuIjoiOW5iMGtyZFdNUjBBSFhzdjh2dzcybzNvdGZCQ  
0RfY0tnenVyY1FzeEYycmJSc2F5VmJXRWVvcEZIOTNyQ3JlR056UjJBQWtMRG9mSWZ2QU1aR2xWOW5WZTIyMXRScmE4NU9vUEdSZVhQWmh2aVQ2WGpXQ2tHY3N5U1ZYZHNrX192R1VNeGF0b2FNM1A1Q1cyRDAxbGJSc1RDVW1EMG50M01mU1lQNkkzVnFuSVQ5eGVSaDBpZGJQQXFkUkQtSVdINDNHMEhsR0JMeWc3QjNfTnlRc2Y1b2RvUkU2b0NwZ09sdVR3bkh6SmptV081RzVGWmFIdnFmZXdYeXhKbmhWYmFLU3BRbGpUUFp1SXZQMERLX3FvV1h4MFNYUk4tbmJuUkxtaG5QNUQwM0lZenR1R1J4RVM3djdPdG5kY2JSOUNLaWNaRjNJdUdoOS0zdTJRdHY5UlNRIiwiZSI6IkFRQUIifQ",  
"publicKeyJwk": {  
 "kty": "RSA",  
 "n":"9nb0krdWMR0AHXsv8vw72o3otfBCD\_cKgzurcQsxF2rbRsayVbWEeopFH93rCreG   
NzR2AAkLDofIfvAMZGlV9nVe221tRra85OoPGReXPZhviT6XjWCkGcsySVXdsk\_\_vGUMxatoaM3P5CW2D01lbRsTCUmD0nt3MfSYP6I3VqnIT9xeRh0idbPAqdRD-IWH43G0HlGBLyg7B3\_NyQsf5odoRE6oCpgOluTwnHzJjmWO5G5FZaHvqfewXyxJnhVbaKSpQljTPZuIvP0DK\_qoWXx0SXRN-nbnRLmhnP5D03IYztuGRxES7v7OtndcbR9CKicZF3IuGh9-3u2Qtv9RSQ",  
 "e": "AQAB”  
 }  
 }  
 ]  
}

Sample 1.4: Private Key

-----BEGIN RSA PRIVATE KEY-----MIIEpgIBAAKCAQEA9nb0krdWMR0AHXsv8vw72o3otfBCD/cKgzurcQsxF2rbRsayVbWEeopFH93rCreGNzR2AAkLDofIfvAMZGlV9nVe221tRra85OoPGReXPZhviT6XjWCkGcsySVXdsk//vGUMxatoaM3P5CW2D01lbRsTCUmD0nt3MfSYP6I3VqnIT9xeRh0idbPAqdRD+IWH43G0HlGBLyg7B3/NyQsf5odoRE6oCpgOluTwnHzJjmWO5G5FZaHvqfewXyxJnhVbaKSpQljTPZuIvP0DK/qoWXx0SXRN+nbnRLmhnP5D03IYztuGRxES7v7OtndcbR9CKicZF3IuGh9+3u2Qtv9RSQIDAQABAoIBAQDGYGzvAp5fnaYQ  
  
----END RSA PRIVATE KEY-----

## 2 Holder DID in the Digital Wallet

2.1 A holder must be able to upload their DID as a .txt file to the digital wallet.

2.2 The digital wallet should save the DID in its storage system.

2.3 Before the DID can be saved, the digital wallet must allow the holder to upload their private key to verify that the holder owns the public key specified in the DID.

**2.4 The wallet shall not save the holder’s private key in storage. The private key should only be used to verify the holder’s ownership of the public key in the DID.**

* 1. The digital wallet should allow the holder to save multiple DIDs from various issuer platforms.

## 3. Verifiable Credential Data Model

3.1 A verifiable credential for education and training contains data related to the credential itself, the issuer of the credential and the holder of the verifiable credential.

3.2 The data model should be aligned to the Open Badges Specification[[6]](#endnote-6).

3.3 AchievementCredential

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Required** | **Notes** |
| @context | List of strings | Yes | Should include: "https://www.w3.org/ns/credentials/v2", "https://purl.imsglobal.org/spec/ob/v3p0/context-3.0.3.json" |
| Id | string | Yes |  |
| type | List of strings | Yes | Should include: "VerifiableCredential",  "OpenBadgeCredential" |
| issuer | Profile | Yes |  |
| validFrom | string | Yes | Should be formatted date: e.g. 2025-05-19T00:00:00Z |
| validUntil | string | Yes | Should be formatted date: e.g. 2025-05-19T00:00:00Z |
| credentialSubject | AchievementSubject | Yes |  |
| iss | string | Optional |  |
| jti | string | Optional |  |
| sub | string | Optional |  |

3.4 Profile

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Required** | **Notes** |
| id | string | Yes | Should be DID of issuer |
| type | List of strings | Yes | Should include: “Profile” |
| name | string | Yes |  |

3.5 AchievementSubject

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Required** | **Notes** |
| id | string | Yes | Should be the DID of the holder |
| type | List of strings | Yes | Should include: “AchievementSubject“ |
| achievement | Achievement | Yes |  |
| identifier | IdentityObject | Optional |  |
| image | Image | Optional |  |

3.6 Achievement

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Required** | **Notes** |
| id | string | Yes |  |
| type | List of strings | Yes | Should include: "Achievement" |
| name | string | Yes |  |
| description | string | Yes |  |
| criteria | Criteria | Yes |  |

3.7 Criteria

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Required** | **Notes** |
| id | string | Optional | Reference to web resource will be ignored |
| narrative | string | Yes |  |

3.8 IdentityObject

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Required** | **Notes** |
| type | string | Yes | Should be: “IdentityObject” |
| hashed | bool | Yes | Should be false |
| identityType | string | Yes | Should be: “name” |
| identityHash | string | Yes | Should be plain text of holder’s name |

3.9 Image

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Required** | **Notes** |
| id | string | Yes | Should be the image of the holder photo in data:uri format, eg. ……  The image should be displayable offline. A link to a web image will be ignored. |
| type | string | Yes | Should be : “Image” |

## 

## 4. Verifiable Credential Format

4.1 Verifiable Credentials should be presented as a JSON Web Token (JWT)[[7]](#endnote-7). Conceptually, the JWT contains the following sections:

[header].[payload].[signature]

4.2 The header (Sample 4.1) of the JWT should include the JWK specified in the Issuer's DID. The JWK should contain the Issuer's public key parameters. The kid, if included, will be ignored.

Sample 4.1 : JWT decoded header

{  
 "alg": "RS256",  
 "typ": "JWT",  
 "jwk": {  
 "kty": "RSA",  
 "n": "xICdahlIZ5Zenx2yR8Tr\_9gVJ- eqEg82gJwzaLWdhHwCfHqIcXSmBcWl8jJMYdDnjQtgpjoED9OBOlk8Eg-HSOyAudsAkqzKr3pG22YEFccFgA67U3jLFlt1pDh2jso9XZEKKRkrV0KfSbbU3VGKhX8vSV0xZcdgjGLF\_dbIjHtXLChQxdIw0U6uUd857Tkz-srAXHIy1ycnxgLAinqy3L8SgMbIVRtB\_f1La3WVY2uS2V3T4bpbGyUPQfi7JFfGhjpnA97-GB0eh30z1nBje6StDFFMZnbQQyOZIczeKKB\_vChn0N0bN1Xmhb3tDycU1tTLdFZT6KP1QeQ10g78-Q",  
 "e": "AQAB"  
 }  
}

4.3 The payload (Sample 4.2) of the JWT should contain the credential’s data.

Sample 4.2 : JWT decoded payload

{  
 "@context": ["https://www.w3.org/ns/credentials/v2", "https://purl.imsglobal.org/spec/ob/v3p0/context-3.0.3.json"],  
 "id": "b08d340b24f64fe2b1a4b8af6e9458bc",  
 "type": ["VerifiableCredential","OpenBadgeCredential"],  
 "issuer": {"id":"did:jwk:eyJrdHkiOiJSU0EiLCJuIjoieElDZGFobElaNVplbngyeVI4VHJfOWdWSi1l  
cUVnODJnSnd6YUxXZGhId0NmSHFJY1hTbUJjV2w4akpNWWREbmpRdGdwam9FRDlPQk9sazhFZy1IU095QXVkc0FrcXpLcjNwRzIyWUVGY2NGZ0E2N1UzakxGbHQxcERoMmpzbzlYWkVLS1JrclYwS2ZTYmJVM1ZHS2hYOHZTVjB4WmNkZ2pHTEZfZGJJakh0WExDaFF4ZEl3MFU2dVVkODU3VGt6LXNyQVhISXkxeWNueGdMQWlucXkzTDhTZ01iSVZSdEJfZjFMYTNXVlkydVMyVjNUNGJwYkd5VVBRZmk3SkZmR2hqcG5BOTctR0IwZWgzMHoxbkJqZTZTdERGRk1abmJRUXlPWkljemVLS0JfdkNobjBOMGJOMVhtaGIzdER5Y1UxdFRMZEZaVDZLUDFRZVExMGc3OC1RIiwiZSI6IkFRQUIifQ",  
 "type": ["Profile"],  
 "name": "Ray Consulting Limited"  
 },  
 "validFrom": "2025-05-19T00:00:00Z",  
 "validUntil": "2030-05-19T00:00:00Z",  
"credentialSubject": {  
 "id": "did:jwk:eyJrdHkiOiJSU0EiLCJuIjoicHVYb3VRS1Vha2t2X2JUZWQ4dkNYLU9FTG1j  
UzhqQ21DWE9WZFp2b3l5c0wxTWMyMWZGSzBxMXBIN1dMRU1hOUFhd1hQSk1sckdEdmcxT0FiS1h0TkMwZ2hHMTR2dzVqQXpieldsb3F3c25jaGlQRk5ENWt6aTNfUmNpYzlxZlpGUnN3aUdjUkNtRHNKUnlqX244MDhVZkNGdkRnYVZzVjlNNVJhMmNZMHlYQkJDM29tRkpJNXBkTEEySTFFRFZuMWJkTzFaRXQtUFY3Z3c0MWFQZHdhNzd2cTBNRkFDaTNyS0wtTEdzWkNxYlo1Q0ZsNjJFMWNYMU5KZmd1d3BoMDJHMEdRSjZIMnhBSFdnU3BkVUtXcTNQdXJrWVl3VGkwTFJXR015Mk5sSzdwVUxPMlFwem1GN2tWRmdhbW5fb0VOMFlhVkoxbVgzVE02UEVHVzZFdDFRIiwiZSI6IkFRQUIifQ",  
 "type": ["AchievementSubject"],  
 "achievement": {  
 "id": "015301207aa74f5fa548ac55bb884996",  
 "type": ["Achievement"],  
 "name": "Sample Verifiable Credential",  
 "description": "This credential is an example of a Verifiable Credential.",  
 "criteria": { "narrative": "To achieve this credential, a user can download this Verifiable Credential and use it for demonstration purposes.  
 }  
 }  
 },  
 "iss": "did:jwk:eyJrdHkiOiJSU0EiLCJuIjoieElDZGFobElaNVplbngyeVI4VHJf  
OWdWSi1lcUVnODJnSnd6YUxXZGhId0NmSHFJY1hTbUJjV2w4akpNWWREbmpRdGdwam9FRDlPQk9sazhFZy1IU095QXVkc0FrcXpLcjNwRzIyWUVGY2NGZ0E2N1UzakxGbHQxcERoMmpzbzlYWkVLS1JrclYwS2ZTYmJVM1ZHS2hYOHZTVjB4WmNkZ2pHTEZfZGJJakh0WExDaFF4ZEl3MFU2dVVkODU3VGt6LXNyQVhISXkxeWNueGdMQWlucXkzTDhTZ01iSVZSdEJfZjFMYTNXVlkydVMyVjNUNGJwYkd5VVBRZmk3SkZmR2hqcG5BOTctR0IwZWgzMHoxbkJqZTZTdERGRk1abmJRUXlPWkljemVLS0JfdkNobjBOMGJOMVhtaGIzdER5Y1UxdFRMZEZaVDZLUDFRZVExMGc3OC1RIiwiZSI6IkFRQUIifQ",  
 "jti": "b08d340b24f64fe2b1a4b8af6e9458bc",  
 "sub": "did:jwk:eyJrdHkiOiJSU0EiLCJuIjoicHVYb3VRS1Vha2t2X2JUZWQ4dkNYLU9FTG1jUz  
hqQ21DWE9WZFp2b3l5c0wxTWMyMWZGSzBxMXBIN1dMRU1hOUFhd1hQSk1sckdEdmcxT0FiS1h0TkMwZ2hHMTR2dzVqQXpieldsb3F3c25jaGlQRk5ENWt6aTNfUmNpYzlxZlpGUnN3aUdjUkNtRHNKUnlqX244MDhVZkNGdkRnYVZzVjlNNVJhMmNZMHlYQkJDM29tRkpJNXBkTEEySTFFRFZuMWJkTzFaRXQtUFY3Z3c0MWFQZHdhNzd2cTBNRkFDaTNyS0wtTEdzWkNxYlo1Q0ZsNjJFMWNYMU5KZmd1d3BoMDJHMEdRSjZIMnhBSFdnU3BkVUtXcTNQdXJrWVl3VGkwTFJXR015Mk5sSzdwVUxPMlFwem1GN2tWRmdhbW5fb0VOMFlhVkoxbVgzVE02UEVHVzZFdDFRIiwiZSI6IkFRQUIifQ"  
}

4.4 The signature of the JWT should be created by signing the JWT with the issuer's private key. The RS256 signing algorithm must be used.

4.5 In accordance with the JWT specification, the JWT should be derived from:

Y = Base64URLEncode(header) + '.' + Base64URLEncode(payload)  
JWT token = Y + '.' + Base64URLEncode(RSASHA256(Y))

4.6 The JWT (Sample 4.3) should be in the compact form.

4.7 Only .jwt files for verifiable credentials are supported by the digital wallet. An image file with an embedded JWT is not supported.

Sample 4.3: Verifiable Credential formatted as a JWT compact

..S4VDYLi4SviluK8IBdeE4SLTUFCk1OMQLRmp6zI5RK8ZTM3TbgXUWeOTUX6C5NtO7EaNx0wXmbqEGUkoiU9kY\_dutKF1Kv2DG4MTqwNcU\_skivo2Dt9g1atBRlF5Al4aEpIqThRKf0U2LWe80dvKwODki2TI1\_kxsochleNLPETzrbqB9bMbiQ6JcKOsvkV8puIuGzuDdlhmmyH7wG1ySFy4bsPq8DoiBW\_hRMJSxuW1go71v4Di2HxoqZuV9nJUO-vNvApiGYw3eSTzwTvV-TH7mdBlvxEXa3-42FreJQiQ7bsK48WqQ1jllGVoJYYE1FKEV-0rpEWYlIl3Shx7lg

4.8 The file extension for the credential in JWT compact format should be. jwt.

4.9 Holders should be able to download their credential as a .jwt file from an issuer application to upload in the digital wallet.

# V. Conclusion

## Issuer Application

For an issuer application to be able to interchange data with the digital wallet, it must:

* Create a public / private cryptographic key pair using RSA for holders and issuers
* Create a DID for holders and issuers using the did:jwk method
* Allow the holder to download the DID and private key as .txt files
* The holder will save their DID in the digital wallet after verifying ownership with their private key
* Create a verifiable credential for the holder following the specified data model
* Sign the verifiable credential with the issuer’s private key and format it as a JWT compact
* Allow the holder to download the verifiable credential as a .jwt file to upload in the digital wallet

## Digital Wallet Application

The Digital Wallet Application will:

* Allow a holder to upload their DID as a .txt file from an issuer application
* Check that the DID belongs to the holder by matching the public key contained in the DID with the holder’s private key. The wallet application should not save the holders private key in its storage system
* Save the holder’s DID in the wallet’s storage system
* Allow the holder to upload a verifiable credential as a .jwt file
* Check that the credential’s subject DID matches one of the holder’s DID saved in the wallet
* Save the verifiable credential in the wallet’s storage system once the subject DID is verified

# VI. References

1. Verifiable Credentials Data Model v2.0 specification published by W3C: https://www.w3.org/TR/vc-data-model-2.0/ [↑](#endnote-ref-1)
2. Decentralized Identifier (DID) specification published by the W3C: https://www.w3.org/TR/did-1.1/ [↑](#endnote-ref-2)
3. did:jwk method developed by quartzjer : https://github.com/quartzjer [↑](#endnote-ref-3)
4. [] RSA Cryptography Specifications published by Internet Engineering Task Force (IETF): https://datatracker.ietf.org/doc/html/rfc8017 [↑](#endnote-ref-4)
5. JSON Web Key (JWK) published by Internet Engineering Task Force (IETF) : https://datatracker.ietf.org/doc/html/rfc7517 [↑](#endnote-ref-5)
6. Open Badges Specification published by IMS Global https://www.imsglobal.org/spec/ob/v3p0 [↑](#endnote-ref-6)
7. JSON Web Token (JWT) published by Internet Engineering Task Force (IETF): https://datatracker.ietf.org/doc/html/rfc7519 [↑](#endnote-ref-7)