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

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] 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] .

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

1.3 When creating a did:jwk (Sample 1.1), the RSA[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]. 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.

1.6 A DID should be in the form of a text (.txt) file. Issuers and holders should be allowed to download and save their DID.

1.7 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:eyJrdHkiOiJSU0EiLCJuIjoicHVYb3VRS1Vha2t2X2JUZWQ4dkNYLU9FTG1jUzhqQ21DWE9WZF
p2b3l5c0wxTWMyMWZGSzBxMXBIN1dMRU1hOUFhd1hQSk1sckdEdmcxT0FiS1h0TkMwZ2hHMTR
2dzVqQXpieldsb3F3c25jaGlQRk5ENWt6aTNfUmNpYzlxZlpGUnN3aUdjUkNtRHNKUnlqX244MDhVZk
NGdkRnYVZzVjlNNVJhMmNZMHlYQkJDM29tRkpJNXBkTEEySTFFRFZuMWJkTzFaRXQtUFY3Z3c0MW
FQZHdhNzd2cTBNRkFDaTNyS0wtTEdzWkNxYlo1Q0ZsNjJFMWNYMU5KZmd1d3BoMDJHMEdRSjZI
MnhBSFdnU3BkVUtXcTNQdXJrWVl3VGkwTFJXR015Mk5sSzdwVUxPMlFwem1GN2tWRmdhbW5fb0
VOMFlhVkoxbVgzVE02UEVHVzZFdDFRIiwiZSI6IkFRQUIifQ
```

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

```
{

 "kty": "RSA",
 "n": "puXouQKUakkv_bTed8vCX-
OELmcS8jCmCXOVdZvoyysL1Mc21fFK0q1pH7WLEMa9AawXPJMlrGDvg1OAbKXtNC0ghG14vw5jAz
bzWloqwsnchiPFND5kzi3_Rcic9qfZFRswiGcRCmDsJRyj_n808UfCFvDgaVsV9M5Ra2cY0yXBBC3omF
JI5pdLA2I1EDVn1bdO1ZEt-PV7gw41aPdwa77vq0MFACi3rKL-
LGsZCqbZ5CFl62E1cX1NJfguwph02G0GQJ6H2xAHWgSpdUKWq3PurkYYwTi0LRWGMy2NlK7pULO2
QpzmF7kVFgamn_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
nVyY1FzeEYycmJSc2F5VmJXRWVvcEZIOTNyQ3JlR056UjJBQWtMRG9mSWZ2QU1aR2xWOW5WZTIy
MXRScmE4NU9vUEdSZVhQWmh2aVQ2WGpXQ2tHY3N5U1ZYZHNrX192R1VNeGF0b2FNM1A1Q1c
yRDAxbGJSc1RDVW1EMG50M01mU1lQNkkzVnFuSVQ5eGVSaDBpZGJQQXFkUkQtSVdINDNHMEhs
R0JMeWc3QjNfTnlRc2Y1b2RvUkU2b0NwZ09sdVR3bkh6SmptV081RzVGWmFIdnFmZXdYeXhKbmh
WYmFLU3BRbGpUUFp1SXZQMERLX3FvV1h4MFNYUk4tbmJuUkxtaG5QNUQwM0lZenR1R1J4RVM
3djdPdG5kY2JSOUNLaWNaRjNJdUdoOS0zdTJRdHY5UlNRIiwiZSI6IkFRQUIifQ",
"verificationMethod": [
 {
   "id": "#0",
   "type": "JsonWebKey2020",
   "controller": "did:jwk:eyJrdHkiOiJSU0EiLCJuIjoiOW5iMGtyZFdNUjBBSFhzdjh2dzcybzNvdGZCQ
0RfY0tnenVyY1FzeEYycmJSc2F5VmJXRWVvcEZIOTNyQ3JlR056UjJBQWtMRG9mSWZ2QU1aR2xWO
W5WZTIyMXRScmE4NU9vUEdSZVhQWmh2aVQ2WGpXQ2tHY3N5U1ZYZHNrX192R1VNeGF0b2FN
M1A1Q1cyRDAxbGJSc1RDVW1EMG50M01mU1lQNkkzVnFuSVQ5eGVSaDBpZGJQQXFkUkQtSVdIN
DNHMEhsR0JMeWc3QjNfTnlRc2Y1b2RvUkU2b0NwZ09sdVR3bkh6SmptV081RzVGWmFIdnFmZXdY
eXhKbmhWYmFLU3BRbGpUUFp1SXZQMERLX3FvV1h4MFNYUk4tbmJuUkxtaG5QNUQwM0lZenR1
R1J4RVM3djdPdG5kY2JSOUNLaWNaRjNJdUdoOS0zdTJRdHY5UlNRIiwiZSI6IkFRQUIifQ",
"publicKeyJwk": {
            "kty": "RSA",
            "n":"9nb0krdWMR0AHXsv8vw72o3otfBCD_cKgzurcQsxF2rbRsayVbWEeopFH93rCreG
NzR2AAkLDofIfvAMZGlV9nVe221tRra85OoPGReXPZhviT6XjWCkGcsySVXdsk__vGUMxatoaM3P5C
W2D01lbRsTCUmD0nt3MfSYP6I3VqnIT9xeRh0idbPAqdRD-
IWH43G0HlGBLyg7B3_NyQsf5odoRE6oCpgOluTwnHzJjmWO5G5FZaHvqfewXyxJnhVbaKSpQljTPZuI
vP0DK_qoWXx0SXRN-nbnRLmhnP5D03IYztuGRxES7v7OtndcbR9CKicZF3IuGh9-3u2Qtv9RSQ",
           "e": "AQAB”
       }
    }
  ]
}
```

Sample 1.4: Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEA9nb0krdWMR0AHXsv8vw72o3otfBCD/cKgzurcQsxF2rbRsayVbWEeopFH93rCr
eGNzR2AAkLDofIfvAMZGlV9nVe221tRra85OoPGReXPZhviT6XjWCkGcsySVXdsk//vGUMxatoaM3P
5CW2D01lbRsTCUmD0nt3MfSYP6I3VqnIT9xeRh0idbPAqdRD+IWH43G0HlGBLyg7B3/NyQsf5odoRE
6oCpgOluTwnHzJjmWO5G5FZaHvqfewXyxJnhVbaKSpQljTPZuIvP0DK/qoWXx0SXRN+nbnRLmhnP5
D03IYztuGRxES7v7OtndcbR9CKicZF3IuGh9+3u2Qtv9RSQIDAQABAoIBAQDGYGzvAp5fnaYQ
FK09eQR8H6jleGLUEtXlV0vhC08SODISv6+fCSF+uHh289pRn/Jp0NIBqUW7BlO8yF5RG+/TFhmpqG
RCfKeB4VsRqUlUjLOJ1lWJt/WdxU3OdUyiT33aF8O1/wdlA/OHAUuO+Y7fyOEDoqZ17ma8UNGStnC
wURe9vL+afJ8rZBGkX0Y5Tbg++qiss6ZnTpeHMlTuoFQyMYIwZG4lXixvjRJ5DaOrLps3yM1me4p6zTO
snbFxY09FrsTQMv+Hb1scitGkSiUN4gzKXy74vQKWo/dqlDL5P7cLUFtcDyGpOeDDigH3pszbxaU2sW
oD3Q7NXCyoi74ZAoGBAP9TusTQYQ7lIvdzyFEedgSK8hHfeqmB6pj6u/w7sIQLTDiXlU7G7SqY7rRa+R
y91n/nJxeR7emRAKS3PYb3rHtFIdiPnlU+FjpX/pSKmz3r4QGAP5bqjB6SUCoXH+gFvPa3F1C/RidtIwZ
H7EKd7hHcZ9GmxWdrBxbefpjpXJRXAoGBAPcdPw0X1g+9jDCgzOAHXAnjnNJmnQ5sriSM25kYsv03
YgdHNEtE3pshFMVV3h0SeNbWWzJzWHh7o6/MOiDfSLw4mi9s86mseu/5NRE2f8x10q7RB3pUw1T
p8DApG9H4ElSPVHB70Bg9wKx2I7kPWxjwLWZ/iqzIH1BWBwFUysNfAoGBAL51v/GGm5AX3vCFvty
8Az86Qn6QnRiK3+wDxWzPPcoR/2aLtIXSICJReGazIfaNqc85J9EOO1Gqp7c3NT9Ty6ccl7XK1Eo0CTK
2ZyJ5DnqvVOXgvA6goatAa2oqW9OhTCchxtOmCvfoEmNiDVxYILnUFuGuLL0LentVt0vrb/L7AoGBAJ
sbkGf3fjWDFGuxgudbtzm91MF8Bzj2npfykiQWjMLD8JQA7aIRKGjW6uKycyhsX8z532RbYjy93pCJ8
DKR9GWwYZdDG+50hPX7xoN3YeBEVGnGapsueSzjag/QvdWdkGPjU20HSibtG/MkdGfEa7nLh7O+e
pzZQE58sQj04BChAoGBAOfg1+NgQIkezTX2w/n87gqRW/C6QjnZw68Xgqs8T6ZwEEGiE8NJw7/aab
ORnrkSVL5B+Zy+1WGtSRH6StZb+HTN7g8jfqWDvifRccmEs3DVRzcNk2F747b6emNDaJg3RtCCF5vx
vaMmDs0Z4sFuEtYjig6GKEMUIOUq2O15IuxW
----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.

2.5 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].

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. data:image/.png;base64,iVBORw0KGgoACCEugAA…… 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]. 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-
HSOyAudsAkqzKr3pG22YEFccFgA67U3jLFlt1pDh2jso9XZEKKRkrV0KfSbbU3VGKhX8vSV0xZcdgjGL
F_dbIjHtXLChQxdIw0U6uUd857Tkz-
srAXHIy1ycnxgLAinqy3L8SgMbIVRtB_f1La3WVY2uS2V3T4bpbGyUPQfi7JFfGhjpnA97-
GB0eh30z1nBje6StDFFMZnbQQyOZIczeKKB_vChn0N0bN1Xmhb3tDycU1tTLdFZT6KP1QeQ10g7
8-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
cUVnODJnSnd6YUxXZGhId0NmSHFJY1hTbUJjV2w4akpNWWREbmpRdGdwam9FRDlPQk9sazhFZy1IU095QXVkc0FrcXpLcjNwR
zIyWUVGY2NGZ0E2N1UzakxGbHQxcERoMmpzbzlYWkVLS1JrclYwS2ZTYmJVM1ZHS2hYOHZTVjB4WmNkZ2pHTEZfZGJJakh0WE
xDaFF4ZEl3MFU2dVVkODU3VGt6LXNyQVhISXkxeWNueGdMQWlucXkzTDhTZ01iSVZSdEJfZjFMYTNXVlkydVMyVjNUNGJwYkd
5VVBRZmk3SkZmR2hqcG5BOTctR0IwZWgzMHoxbkJqZTZTdERGRk1abmJRUXlPWkljemVLS0JfdkNobjBOMGJOMVhtaGIzdER5Y
1UxdFRMZEZaVDZLUDFRZVExMGc3OC1RIiwiZSI6IkFRQUIifQ",
      "type": ["Profile"],
      "name": "Ray Consulting Limited"
      },
 "validFrom": "2025-05-19T00:00:00Z",
 "validUntil": "2030-05-19T00:00:00Z",
"credentialSubject": {
   "id": "did:jwk:eyJrdHkiOiJSU0EiLCJuIjoicHVYb3VRS1Vha2t2X2JUZWQ4dkNYLU9FTG1j
UzhqQ21DWE9WZFp2b3l5c0wxTWMyMWZGSzBxMXBIN1dMRU1hOUFhd1hQSk1sckdEdmcxT0FiS1h0TkMwZ2hHMTR2dzVq
QXpieldsb3F3c25jaGlQRk5ENWt6aTNfUmNpYzlxZlpGUnN3aUdjUkNtRHNKUnlqX244MDhVZkNGdkRnYVZzVjlNNVJhMmNZM
HlYQkJDM29tRkpJNXBkTEEySTFFRFZuMWJkTzFaRXQtUFY3Z3c0MWFQZHdhNzd2cTBNRkFDaTNyS0wtTEdzWkNxYlo1Q0ZsNjJF
MWNYMU5KZmd1d3BoMDJHMEdRSjZIMnhBSFdnU3BkVUtXcTNQdXJrWVl3VGkwTFJXR015Mk5sSzdwVUxPMlFwem1GN2tW
RmdhbW5fb0VOMFlhVkoxbVgzVE02UEVHVzZFdDFRIiwiZSI6IkFRQUIifQ",
    "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
OWdWSi1lcUVnODJnSnd6YUxXZGhId0NmSHFJY1hTbUJjV2w4akpNWWREbmpRdGdwam9FRDlPQk9sazhFZy1IU095QXVkc0Fr
cXpLcjNwRzIyWUVGY2NGZ0E2N1UzakxGbHQxcERoMmpzbzlYWkVLS1JrclYwS2ZTYmJVM1ZHS2hYOHZTVjB4WmNkZ2pHTEZfZ
GJJakh0WExDaFF4ZEl3MFU2dVVkODU3VGt6LXNyQVhISXkxeWNueGdMQWlucXkzTDhTZ01iSVZSdEJfZjFMYTNXVlkydVMyVjN
UNGJwYkd5VVBRZmk3SkZmR2hqcG5BOTctR0IwZWgzMHoxbkJqZTZTdERGRk1abmJRUXlPWkljemVLS0JfdkNobjBOMGJOMVht
aGIzdER5Y1UxdFRMZEZaVDZLUDFRZVExMGc3OC1RIiwiZSI6IkFRQUIifQ",
  "jti": "b08d340b24f64fe2b1a4b8af6e9458bc",
  "sub": "did:jwk:eyJrdHkiOiJSU0EiLCJuIjoicHVYb3VRS1Vha2t2X2JUZWQ4dkNYLU9FTG1jUz
hqQ21DWE9WZFp2b3l5c0wxTWMyMWZGSzBxMXBIN1dMRU1hOUFhd1hQSk1sckdEdmcxT0FiS1h0TkMwZ2hHMTR2dzVqQX
pieldsb3F3c25jaGlQRk5ENWt6aTNfUmNpYzlxZlpGUnN3aUdjUkNtRHNKUnlqX244MDhVZkNGdkRnYVZzVjlNNVJhMmNZMHlY
QkJDM29tRkpJNXBkTEEySTFFRFZuMWJkTzFaRXQtUFY3Z3c0MWFQZHdhNzd2cTBNRkFDaTNyS0wtTEdzWkNxYlo1Q0ZsNjJFM
WNYMU5KZmd1d3BoMDJHMEdRSjZIMnhBSFdnU3BkVUtXcTNQdXJrWVl3VGkwTFJXR015Mk5sSzdwVUxPMlFwem1GN2tWR
mdhbW5fb0VOMFlhVkoxbVgzVE02UEVHVzZFdDFRIiwiZSI6IkFRQUIifQ"
}
```

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

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImp3ayI6eyJrdHkiOiJSU0EiLCJuIjoieElDZGFobElaNVplbngyeVI4VHJfOWdWSi1lcUVnODJnSnd6YUxXZGh
Id0NmSHFJY1hTbUJjV2w4akpNWWREbmpRdGdwam9FRDlPQk9sazhFZy1IU095QXVkc0FrcXpLcjNwRzIyWUVGY2NGZ0E2N1UzakxGbHQxcERo
MmpzbzlYWkVLS1JrclYwS2ZTYmJVM1ZHS2hYOHZTVjB4WmNkZ2pHTEZfZGJJakh0WExDaFF4ZEl3MFU2dVVkODU3VGt6LXNyQVhISXkxeWNue
GdMQWlucXkzTDhTZ01iSVZSdEJfZjFMYTNXVlkydVMyVjNUNGJwYkd5VVBRZmk3SkZmR2hqcG5BOTctR0IwZWgzMHoxbkJqZTZTdERGRk1abmJ
RUXlPWkljemVLS0JfdkNobjBOMGJOMVhtaGIzdER5Y1UxdFRMZEZaVDZLUDFRZVExMGc3OC1RIiwiZSI6IkFRQUIifX0.eyJAY29udGV4dCI6WyJod
HRwczovL3d3dy53My5vcmcvbnMvY3JlZGVudGlhbHMvdjIiLCJodHRwczovL3B1cmwuaW1zZ2xvYmFsLm9yZy9zcGVjL29iL3YzcDAvY29udGV4dC
0zLjAuMy5qc29uIl0sImlkIjoiYjA4ZDM0MGIyNGY2NGZlMmIxYTRiOGFmNmU5NDU4YmMiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiw
iT3BlbkJhZGdlQ3JlZGVudGlhbCJdLCJpc3N1ZXIiOnsiaWQiOiJkaWQ6andrOmV5SnJkSGtpT2lKU1UwRWlMQ0p1SWpvaWVFbERaR0ZvYkVsYU5
WcGxibmd5ZVZJNFZISmZPV2RXU2kxbGNVVm5PREpuU25kNllVeFhaR2hJZDBObVNIRkpZMWhUYlVKalYydzRha3BOV1dSRWJtcFJkR2R3YW05R
lJEbFBRazlzYXpoRlp5MUlVMDk1UVhWa2MwRnJjWHBMY2pOd1J6SXlXVVZHWTJOR1owRTJOMVV6YWt4R2JIUXhjRVJvTW1wemJ6bFlXa1ZMU
zFKcmNsWXdTMlpUWW1KVk0xWkhTMmhZT0haVFZqQjRXbU5rWjJwSFRFWmZaR0pKYWtoMFdFeERhRkY0WkVsM01GVTJkVlZrT0RVM1ZHd
DZMWE55UVZoSVNYa3hlV051ZUdkTVFXbHVjWGt6VERoVFowMWlTVlpTZEVKZlpqRk1ZVE5YVmxreWRWTXlWak5VTkdKd1lrZDVWVkJSWm1r
M1NrWm1SMmhxY0c1Qk9UY3RSMEl3Wldnek1Ib3hia0pxWlRaVGRFUkdSazFhYm1KUlVYbFBXa2xqZW1WTFMwSmZka05vYmpCT01HSk9NVm
h0YUdJemRFUjVZMVV4ZEZSTVpFWmFWRFpMVURGUlpWRXhNR2MzT0MxUklpd2laU0k2SWtGUlFVSWlmUSIsInR5cGUiOlsiUHJvZmlsZSJdLCJ
uYW1lIjoiUmF5IENvbnN1bHRpbmcgTGltaXRlZCJ9LCJ2YWxpZEZyb20iOiIyMDI1LTA1LTE5VDAwOjAwOjAwWiIsInZhbGlkVW50aWwiOiIyMDMw
LTA1LTE5VDAwOjAwOjAwWiIsImNyZWRlbnRpYWxTdWJqZWN0Ijp7ImlkIjoiZGlkOmp3azpleUpyZEhraU9pSlNVMEVpTENKdUlqb2ljSFZZYjNWUl
MxVmhhMnQyWDJKVVpXUTRka05ZTFU5RlRHMWpVemhxUTIxRFdFOVdaRnAyYjNsNWMwd3hUV015TVdaR1N6QnhNWEJJTjFkTVJVMWhPV
UZoZDFoUVNrMXNja2RFZG1jeFQwRmlTMWgwVGtNd1oyaEhNVFIyZHpWcVFYcGllbGRzYjNGM2MyNWphR2xRUms1RU5XdDZhVE5mVW1OcF
l6bHhabHBHVW5OM2FVZGpVa050UkhOS1VubHFYMjQ0TURoVlprTkdka1JuWVZaelZqbE5OVkpoTW1OWk1IbFlRa0pETTI5dFJrcEpOWEJrVEVF
eVNURkZSRlp1TVdKa1R6RmFSWFF0VUZZM1ozYzBNV0ZRWkhkaE56ZDJjVEJOUmtGRGFUTnlTMHd0VEVkeldrTnhZbG8xUTBac05qSkZNV05ZTV
U1S1ptZDFkM0JvTURKSE1FZFJTalpJTW5oQlNGZG5VM0JrVlV0WGNUTlFkWEpyV1ZsM1ZHa3dURkpYUjAxNU1rNXNTemR3VlV4UE1sRndlbTFH
TjJ0V1JtZGhiVzVmYjBWT01GbGhWa294YlZnelZFMDJVRVZIVnpaRmRERlJJaXdpWlNJNklrRlJRVUlpZlEiLCJ0eXBlIjpbIkFjaGlldmVtZW50U3ViamV
jdCJdLCJhY2hpZXZlbWVudCI6eyJpZCI6IjAxNTMwMTIwN2FhNzRmNWZhNTQ4YWM1NWJiODg0OTk2IiwidHlwZSI6WyJBY2hpZXZlbWVudCJdLC
JuYW1lIjoiU2FtcGxlIFZlcmlmaWFibGUgQ3JlZGVudGlhbCIsImRlc2NyaXB0aW9uIjoiVGhpcyBjcmVkZW50aWFsIGlzIGFuIGV4YW1wbGUgb2YgYS
BWZXJpZmlhYmxlIENyZWRlbnRpYWwuIiwiY3JpdGVyaWEiOnsibmFycmF0aXZlIjoiVG8gYWNoaWV2ZSB0aGlzIGNyZWRlbnRpYWwsIGEgdXNlciB
jYW4gZG93bmxvYWQgdGhpcyBWZXJpZmlhYmxlIENyZWRlbnRpYWwgYW5kIHVzZSBpdCBmb3IgZGVtb25zdHJhdGlvbiBwdXJwb3Nlcy4ifX19LCJ
pc3MiOiJkaWQ6andrOmV5SnJkSGtpT2lKU1UwRWlMQ0p1SWpvaWVFbERaR0ZvYkVsYU5WcGxibmd5ZVZJNFZISmZPV2RXU2kxbGNVVm5PRE
puU25kNllVeFhaR2hJZDBObVNIRkpZMWhUYlVKalYydzRha3BOV1dSRWJtcFJkR2R3YW05RlJEbFBRazlzYXpoRlp5MUlVMDk1UVhWa2MwRnJjW
HBMY2pOd1J6SXlXVVZHWTJOR1owRTJOMVV6YWt4R2JIUXhjRVJvTW1wemJ6bFlXa1ZMUzFKcmNsWXdTMlpUWW1KVk0xWkhTMmhZT0haV
FZqQjRXbU5rWjJwSFRFWmZaR0pKYWtoMFdFeERhRkY0WkVsM01GVTJkVlZrT0RVM1ZHdDZMWE55UVZoSVNYa3hlV051ZUdkTVFXbHVjWGt6
VERoVFowMWlTVlpTZEVKZlpqRk1ZVE5YVmxreWRWTXlWak5VTkdKd1lrZDVWVkJSWm1rM1NrWm1SMmhxY0c1Qk9UY3RSMEl3Wldnek1Ib3
hia0pxWlRaVGRFUkdSazFhYm1KUlVYbFBXa2xqZW1WTFMwSmZka05vYmpCT01HSk9NVmh0YUdJemRFUjVZMVV4ZEZSTVpFWmFWRFpMVUR
GUlpWRXhNR2MzT0MxUklpd2laU0k2SWtGUlFVSWlmUSIsImp0aSI6ImIwOGQzNDBiMjRmNjRmZTJiMWE0YjhhZjZlOTQ1OGJjIiwic3ViIjoiZGlkO
mp3azpleUpyZEhraU9pSlNVMEVpTENKdUlqb2ljSFZZYjNWUlMxVmhhMnQyWDJKVVpXUTRka05ZTFU5RlRHMWpVemhxUTIxRFdFOVdaRnAyYj
NsNWMwd3hUV015TVdaR1N6QnhNWEJJTjFkTVJVMWhPVUZoZDFoUVNrMXNja2RFZG1jeFQwRmlTMWgwVGtNd1oyaEhNVFIyZHpWcVFYcGll
bGRzYjNGM2MyNWphR2xRUms1RU5XdDZhVE5mVW1OcFl6bHhabHBHVW5OM2FVZGpVa050UkhOS1VubHFYMjQ0TURoVlprTkdka1JuWVZa
elZqbE5OVkpoTW1OWk1IbFlRa0pETTI5dFJrcEpOWEJrVEVFeVNURkZSRlp1TVdKa1R6RmFSWFF0VUZZM1ozYzBNV0ZRWkhkaE56ZDJjVEJOUmt
GRGFUTnlTMHd0VEVkeldrTnhZbG8xUTBac05qSkZNV05ZTVU1S1ptZDFkM0JvTURKSE1FZFJTalpJTW5oQlNGZG5VM0JrVlV0WGNUTlFkWEpyV1
ZsM1ZHa3dURkpYUjAxNU1rNXNTemR3VlV4UE1sRndlbTFHTjJ0V1JtZGhiVzVmYjBWT01GbGhWa294YlZnelZFMDJVRVZIVnpaRmRERlJJaXdpWl
NJNklrRlJRVUlpZlEifQ.S4VDYLi4SviluK8IBdeE4SLTUFCk1OMQLRmp6zI5RK8ZTM3TbgXUWeOTUX6C5NtO7EaNx0wXmbqEGUkoiU9kY_dutKF1K
v2DG4MTqwNcU_skivo2Dt9g1atBRlF5Al4aEpIqThRKf0U2LWe80dvKwODki2TI1_kxsochleNLPETzrbqB9bMbiQ6JcKOsvkV8puIuGzuDdlhmmyH7
wG1ySFy4bsPq8DoiBW_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/
[2] Decentralized Identifier (DID) specification published by the W3C: https://www.w3.org/TR/did-1.1/
[3] did:jwk method developed by quartzjer : https://github.com/quartzjer
[][4] RSA Cryptography Specifications published by Internet Engineering Task Force (IETF): https://datatracker.ietf.org/doc/html/rfc8017
[5] JSON Web Key (JWK) published by Internet Engineering Task Force (IETF) : https://datatracker.ietf.org/doc/html/rfc7517
[6] Open Badges Specification published by IMS Global https://www.imsglobal.org/spec/ob/v3p0
[7] JSON Web Token (JWT) published by Internet Engineering Task Force (IETF): https://datatracker.ietf.org/doc/html/rfc7519