



zenika

Identité numérique décentralisée et droit  
d'être soi : protéger son intégrité sur  
Internet





# LES SPEAKERS



**Antoine Cailly**

Consultant Front-End &  
Formateur



**Adrien Wattez**

Consultant Back-End &  
Formateur



# CHAPITRE 1

## Les Verifiable Credentials (VC) et les Verifiable Presentations (VP)

“Bonjour,  
je voudrais récupérer un colis”

- Vous avez une pièce d'identité ?

11.02.2030

 **RÉPUBLIQUE FRANÇAISE** 

CARTE NATIONALE D'IDENTITÉ / IDENTITY CARD

NOM / Surname  
**MARTIN**

Prénoms / Given names  
**Maëlys-Gaëlle, Marie**

SEXE / Sex **F** NATIONALITÉ / Nationality **FRA** DATE DE NAISS. / Date of birth  
**13 07 1990**

LIEU DE NAISSANCE / Place of birth  
**PARIS**

NOM D'USAGE / Alternate name  
**NOM D'USAGE**

N° DU DOCUMENT / Document No. **X4RTBPFW4** DATE D'EXPIR. / Expiry date  
**11 02 2030**

*Signature* **384213**



© ZENIKA 2021 All rights reserved - Proprietary & confidential



# CECI N'EST PAS UNE IDENTITÉ





# CECI EST UNE COLLECTION DE DÉCLARATIONS À VOTRE SUJET QUE VOUS PRÉSENTEZ





# CECI EST UNE COLLECTION DE DÉCLARATIONS À VOTRE SUJET QUE VOUS PRÉSENTEZ



## ... DONT L'ÉMETTEUR (ETAT FRANCAIS) EST VÉRIFIABLE

“Je vois que vous avez fait la Zenika Academy ?”



- Oui, voici mon diplôme

DELIVRE PAR ZENIKA

# ZENIKA ACADEMY

Vu le procès-verbal de l'examen établi le 15 mars 2022  
par le président du jury, examinateur, ayant autorité sur les diplomes en ligne.  
Le Zenika Academy  
du site [www.mon-diplome.fr](http://www.mon-diplome.fr)  
est conféré à Maëlys MARTIN

pour en jouir avec les droits et prérogatives qui y sont attachés

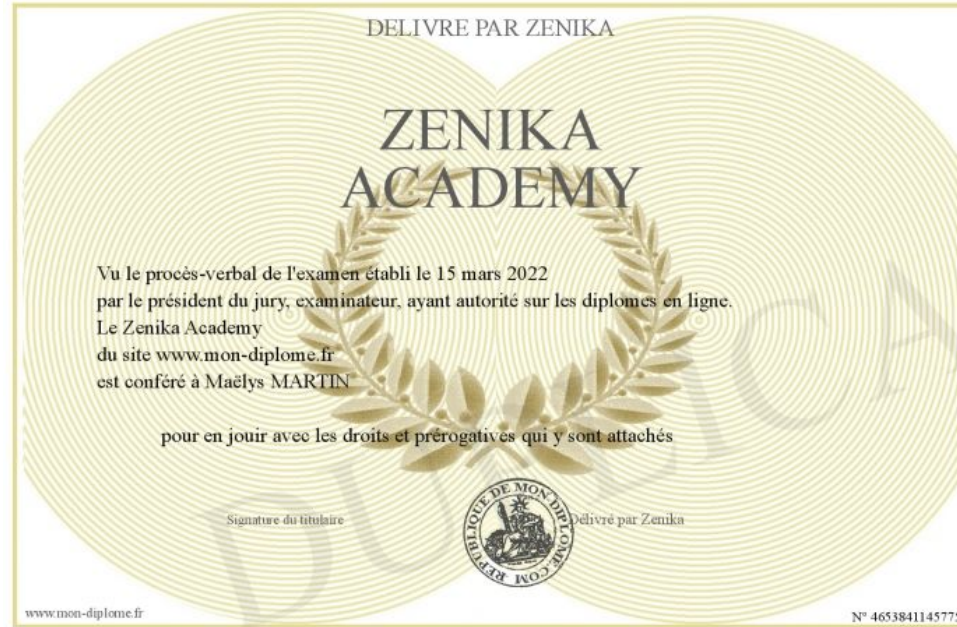
Signature du titulaire



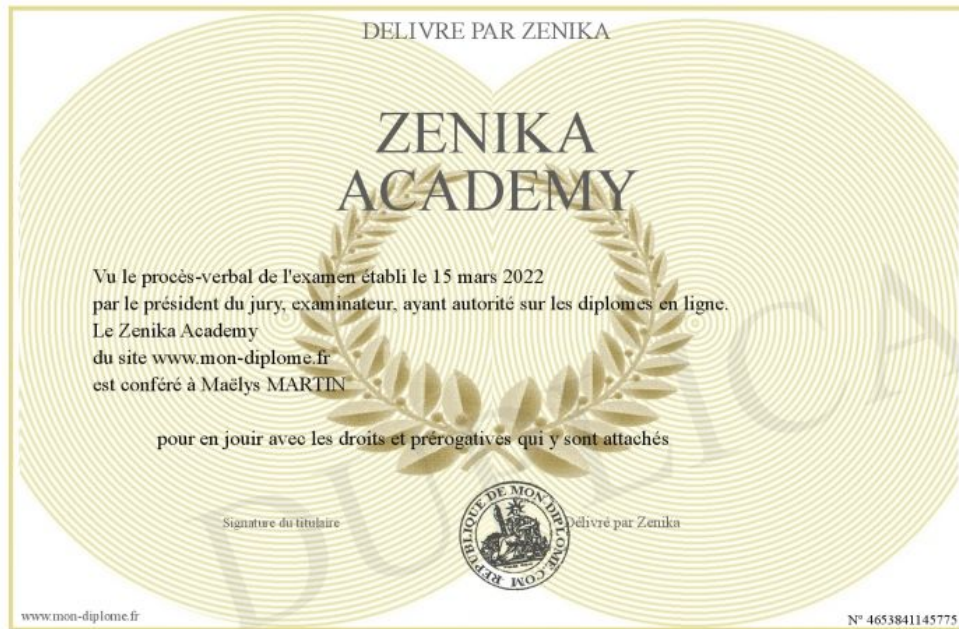
Delivré par Zenika

[www.mon-diplome.fr](http://www.mon-diplome.fr) N° 4653841145775

# CECI N'EST PAS UNE FORMATION

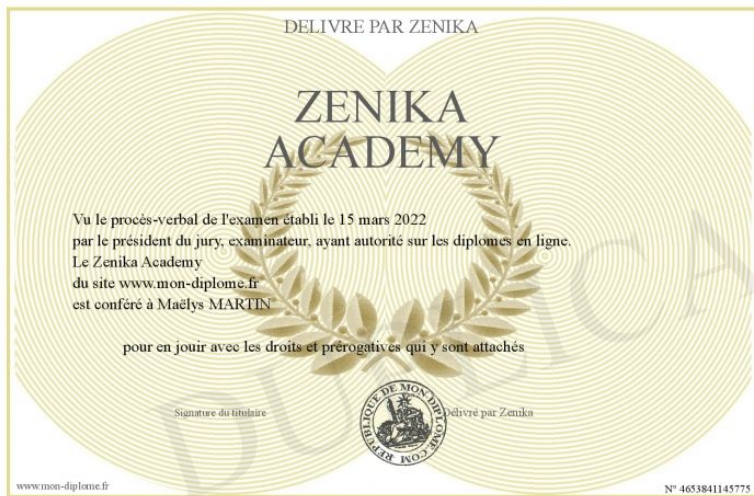


# CECI EST UNE COLLECTION DE DÉCLARATIONS À VOTRE SUJET QUE VOUS PRÉSENTEZ





# CECI EST UNE COLLECTION DE DÉCLARATIONS À VOTRE SUJET QUE VOUS PRÉSENTEZ



## ... DONT L'ÉMETTEUR (ZENIKA) EST VÉRIFIABLE

Vous avez compris ?





ceci est une VERIFIABLE PRESENTATION (VP) qui contient des VERIFIABLE CREDENTIALS (VC)



une VP est une collection de DÉCLARATIONS à propos d'un SUJET et dont l'émetteur est VÉRIFIABLE

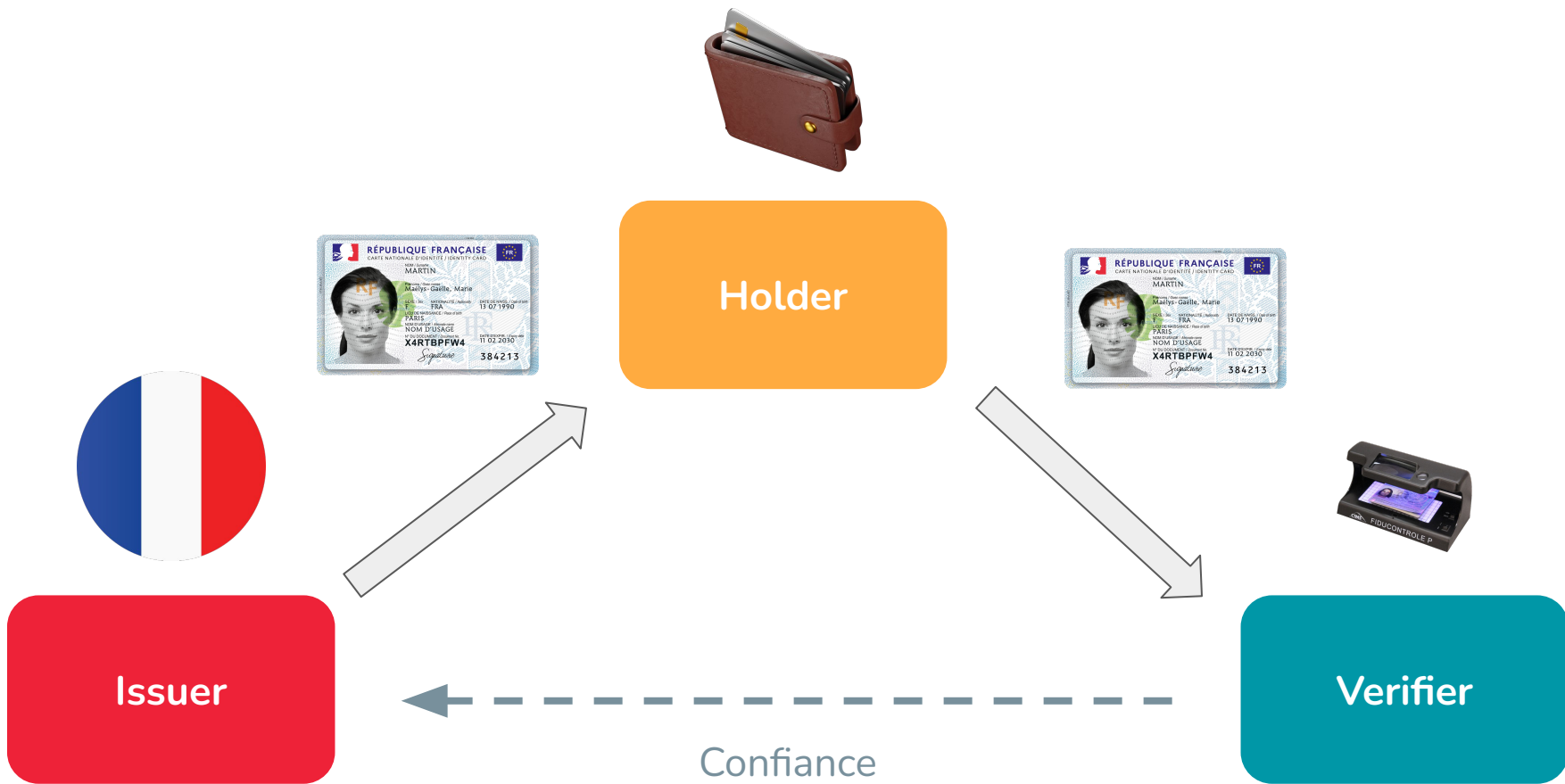
ceci est une VERIFIABLE PRESENTATION (VP) qui contient des VERIFIABLE CREDENTIALS (VC)

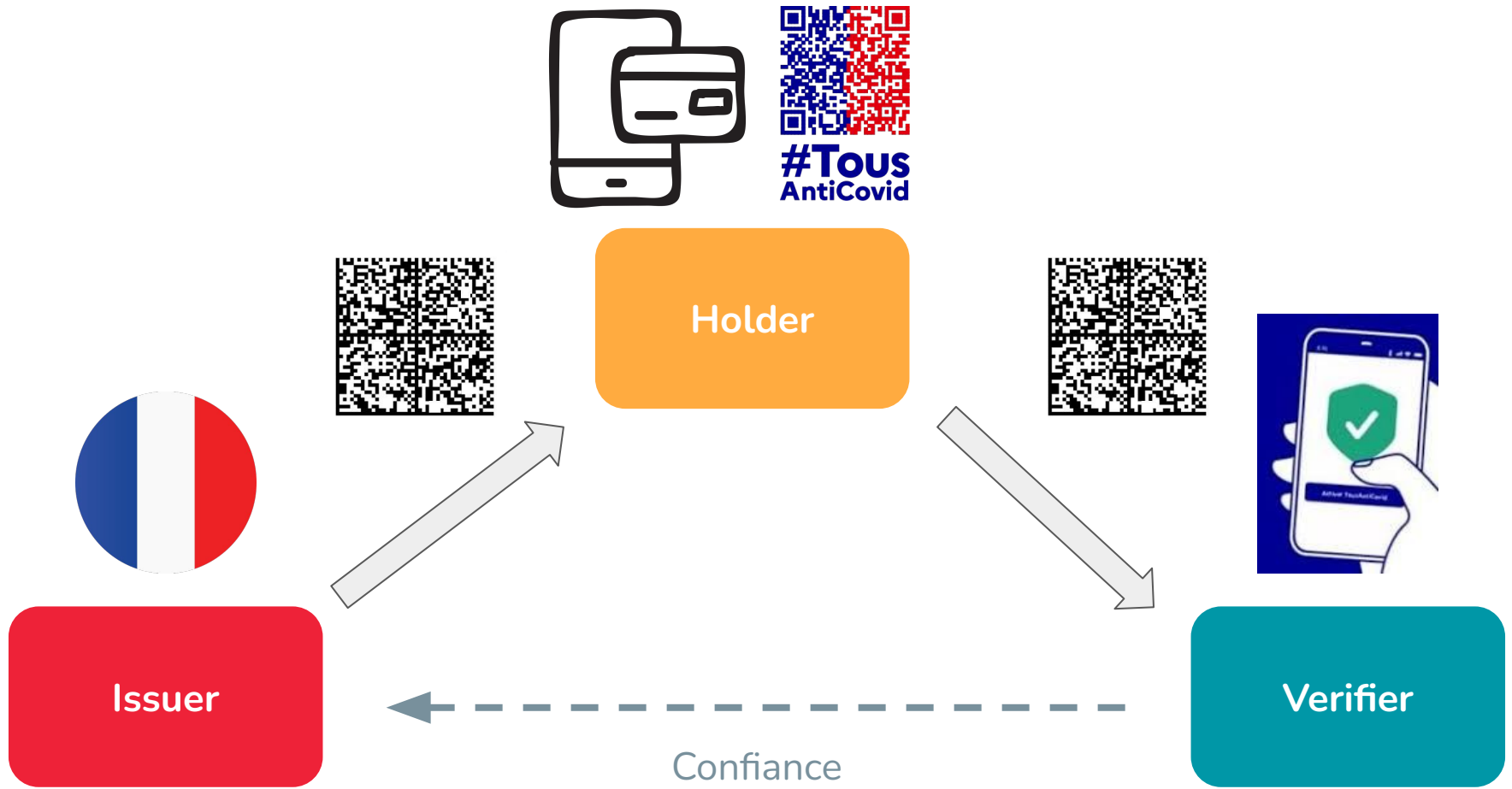


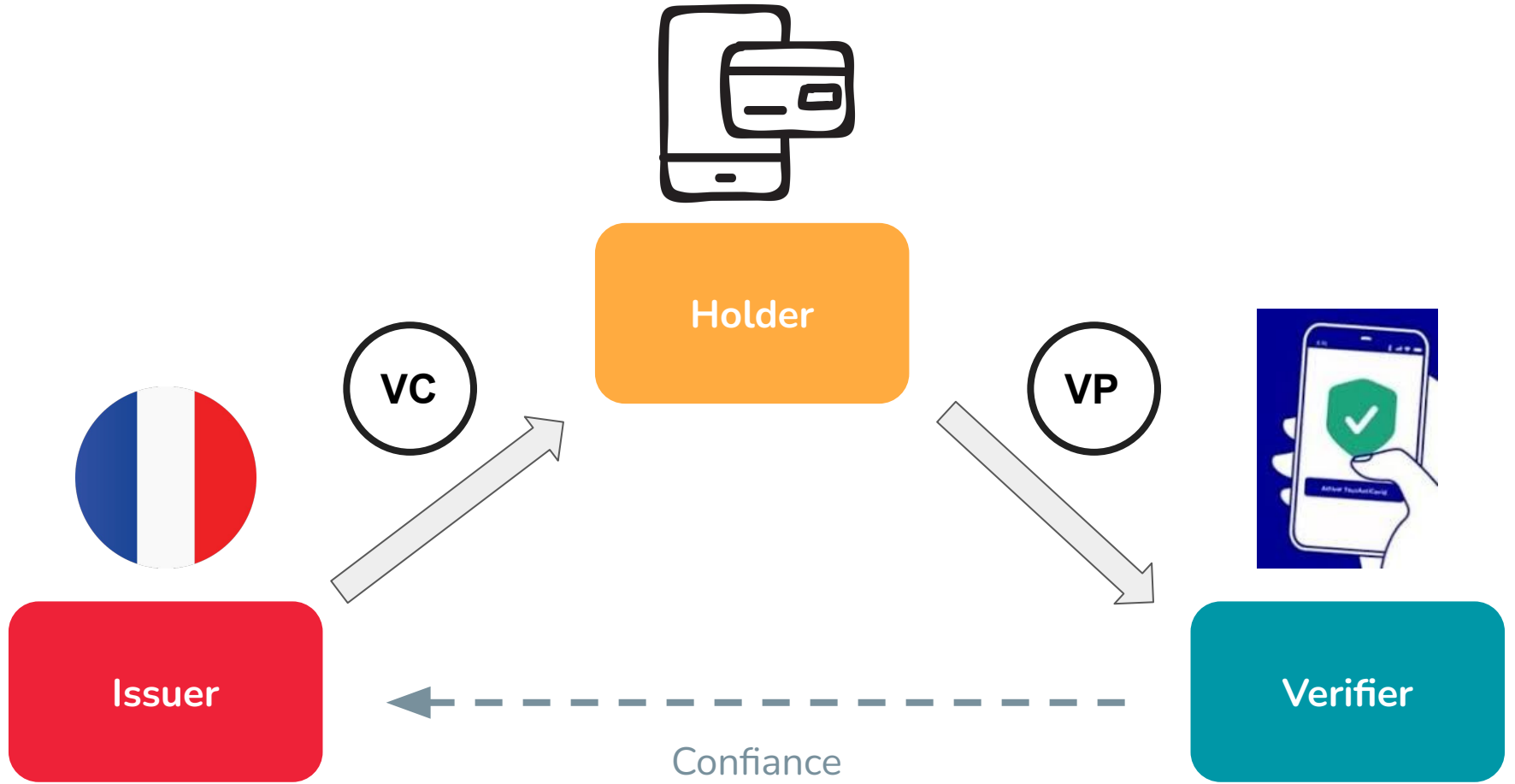
une VP est une collection de DÉCLARATIONS à propos d'un SUJET et dont l'émetteur est VÉRIFIABLE



# THE TRUST TRIANGLE







# NZ COVID Pass - Technical Specification v1

This repository is home to the technical specification for the New Zealand COVID Pass.

The New Zealand COVID Pass is a cryptographically signed document which can be represented in the form of a QR Code that enables an individual to express proof of having met certain health policy requirements in regards to COVID-19 such as being vaccinated against the virus.

...

`vc` : Verifiable Credential CWT claim, this claim **MUST** be present and its value **MUST** follow the structure of [verifiable credential claim structure](#). This claim is mapped to the [JWT Verifiable Credential claim](#). The `vc` claim is currently unregistered and therefore **MUST** be encoded as a Major Type 3 string as defined by [\[RFC7049\]](#).

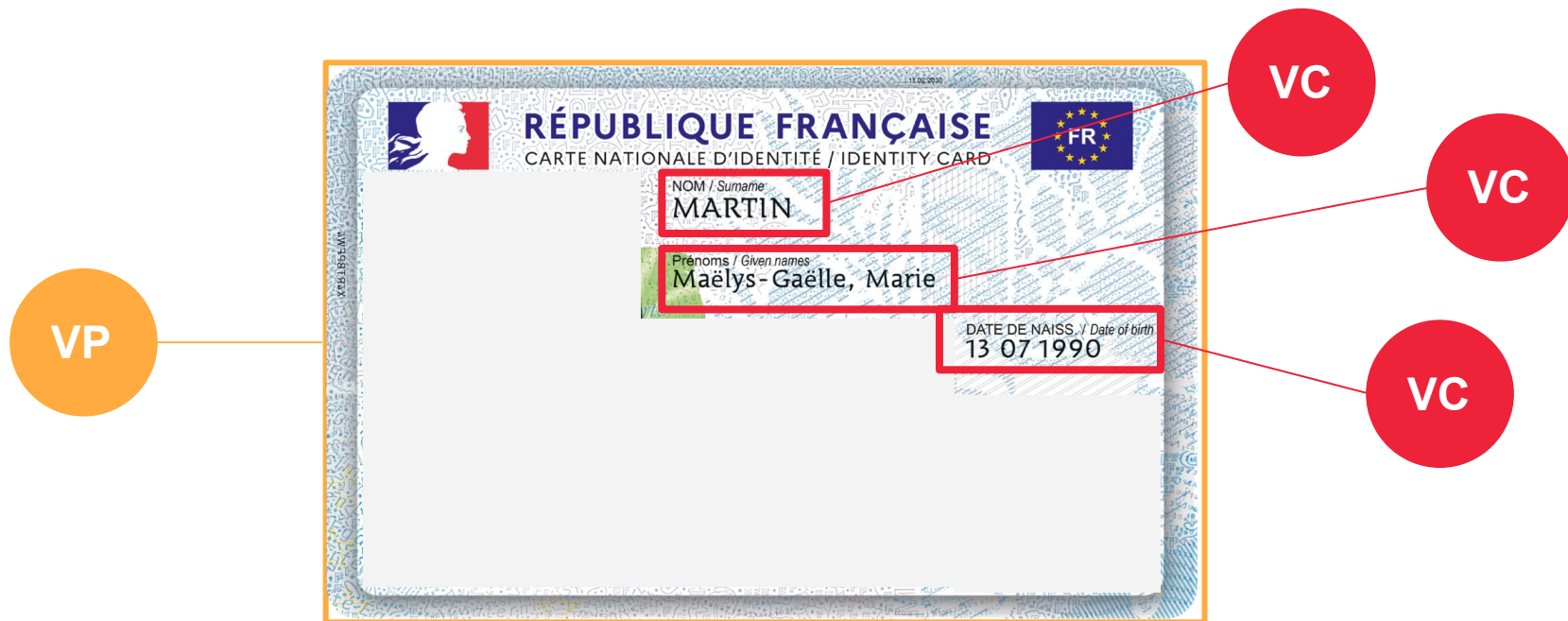
<https://nzcp.covid19.health.nz/>

**Il y a trop d'info sur mon pass sanitaire !  
(et sur ma carte d'identité aussi !)**





# LE HOLDER PEUT CHOISIR LES VC QU'IL INCLUT DANS LA VP



# VC + ZERO KNOWLEDGE PROOFS = Possibilité de limiter la quantité d'information transmise au strict minimum



Qu'est ce qu'on peut mettre dans les déclarations ?





# PROUVER QUELQUE CHOSE...

- que vous connaissez : diplôme, certification, etc.
- que vous possédez : habitation, voiture, compte bancaire, etc.
- que vous êtes : âge, taille, poids, nationalité, etc.
- qui s'est passé : emploi, vaccination, présence à un événement, etc.

En version numérique ça donne quoi ?



## VERIFIABLE CREDENTIAL

Métadonnées

Déclarations

Vérification



# Version JSON simplifiée (une seule VC)



```
{
  "@context": [ ... ],
  "id": "IDFRAX4RTBPFW46",
  "type": "VerifiableCredential",
  "issuer": "FRA",
  "issuanceDate": "2020-11-02T00:00:00Z",
  "credentialSubject": {
    "id": "2 69 05 49 588 157 80",
    "nom": "MARTIN",
    "prénoms": "Maëlys-Gaëlle, Marie",
    "dateNaissance": "1900-07-13"
  },
  ...
},
"proof": {
  
  
  
  
}
}
```

Métadonnées

Déclarations

Vérification

Propriété

2021



# CHAPITRE 2

## Les Decentralized IDentifiers (DID)





# Le sujet d'une VC est désigné par son identifiant

```
{
  "@context": [ ... ],
  "id": "IDFRAX4RTBPFW46",
  "type": "VerifiableCredential",
  "issuer": "FRA",
  "issuanceDate": "2020-11-02T00:00:00Z",
  "credentialSubject": {
    "id": "2 69 05 49 588 157 80",
    "nom": "MARTIN",
    "prénoms": "Maëlys-Gaëlle, Marie",
    "dateNaissance": "1900-07-13"
    ...
  },
  "proof": {
    ...
  }
}
```

# Le sujet d'une VC est désigné par son identifiant



```
{
  "@context": [ ... ],
  "id": "IDFRAX4RTBPFW46",
  "type": "VerifiableCredential",
  "issuer": "FRA",
  "issuanceDate": "2020-11-02T00:00:00Z",
  "credentialSubject": {
    "id": "2 69 05 49 588 157 80",
    "nom": "MARTIN",
    "prénoms": "Maëlys-Gaëlle, Marie",
    "dateNaissance": "1900-07-13"
    ...
  },
  "proof": {
    ...
  }
}
```

Numéro national  
d'identification (NNI)

=

Numéro de sécurité  
sociale en France



Un identifiant unique et universel ?





## C'EST PARTI

En cliquant sur Connexion, vous acceptez nos [Conditions d'utilisation](#). Consultez notre [Politique de confidentialité](#) et notre [Politique relative aux cookies](#) pour pour savoir comment nous traitons vos données.



SE CONNECTER AVEC LA POSTE



CONNEXION AVEC LES IMPÔTS



CONNEXION AVEC UN NUMÉRO  
DE TÉL.

[Problème de connexion ?](#)





## C'EST PARTI

En cliquant sur Connexion, vous acceptez nos [Conditions d'utilisation](#). Consultez notre [Politique de confidentialité](#) et notre [Politique relative aux cookies](#) pour pour savoir comment nous traitons vos données.



SE CONNECTER AVEC GOOGLE



CONNEXION AVEC FACEBOOK



CONNEXION AVEC UN NUMÉRO  
DE TÉL.

[Problème de connexion ?](#)



# L'identifiant du sujet dans les VC



```
{
  "@context": [ ... ],
  "id": "ABC123456789",
  "type": "VerifiableCredential",
  "issuer": "FRA",
  "issuanceDate": "2020-11-02T00:00:00Z",
  "credentialSubject": {
    "id": "maelys-gaëlle.martin@gmail.com",
    "nom": "MARTIN",
    "prénoms": "Maëlys-Gaëlle, Marie",
    "dateNaissance": "1900-07-13"
    ...
  },
  "proof": {
    ...
  }
}
```

**Mon identifiant ne m'appartient pas**

**Si Google meurt, mon identifiant meurt**

**Si Google me bloque, je perd l'accès à tous les sites**

**Je ne décide pas de ce que Google va faire de mes données**

The Google logo, consisting of the word "Google" in its characteristic multi-colored font (blue, red, yellow, green, red).The Microsoft logo, featuring the four-pane Windows logo (red, green, blue, yellow) to the left of the word "Microsoft" in a grey sans-serif font.The Facebook logo, the word "facebook" in white lowercase letters on a dark blue rectangular background.

# Un identifiant généré par moi-même ?

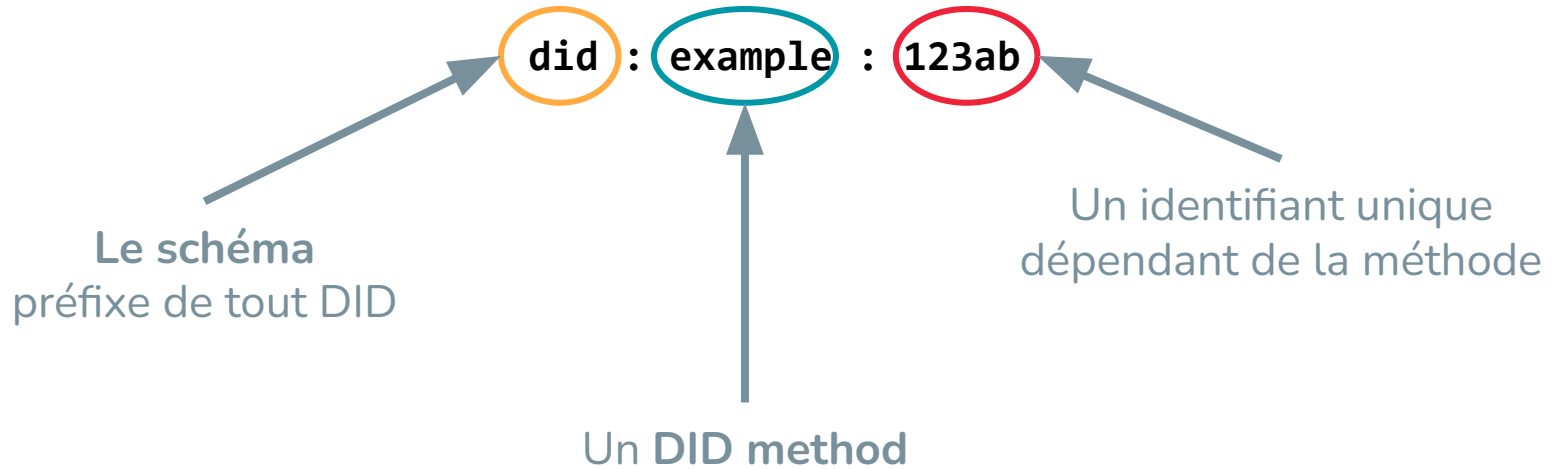


```
{
  "@context": [ ... ],
  "id": "ABC123456789",
  "type": "VerifiableCredential",
  "issuer": "FRA",
  "issuanceDate": "2020-11-02T00:00:00Z",
  "credentialSubject": {
    "id": "???",
    "nom": "MARTIN",
    "prénoms": "Maëlys-Gaëlle, Marie",
    "dateNaissance": "1900-07-13"
    ...
  },
  "proof": {
    ...
  }
}
```



# OUPS! I DID IT AGAIN

Un **DID**, ou Decentralized Identifier (**D**ecentralized **I**D) est en réalité un **URI**.





# Prouver son identité (classique)



maelys-gaelle.martin@gmail.com  
+  
Mot de passe

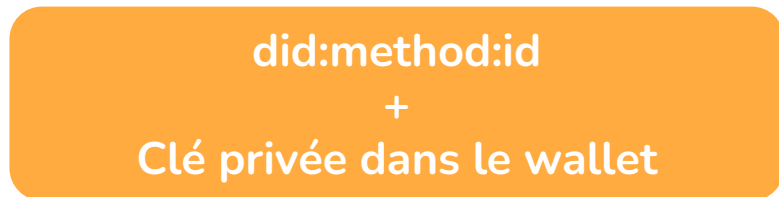


Hash du mot de passe



# Prouver son identité (DID)

Subject



Verifiable Data Registry



# Prouver son identité (did:btcr)



did:btcr:8yv2-xzpq-qqqq-9yce-nk  
+  
Clé privée dans le wallet



DID Document  
contenant la clé  
publique



<https://weboftrustinfo.github.io/btcr-tx-playground.github.io/>



# Prouver son identité (did:web)



did:web:john-doe.me  
+  
Clé privée dans le wallet



<https://john-doe.me/.well-known/did.json>

DID Document  
contenant la clé  
publique





did:btcr:



did:sov:



did:ion:



ethereum

did:ethr:



SOLANA

did:sol:



did:key:



did:dns: & did:web:



Method Name	Status	DLT or Network	Author Links	Link
did:3:	PROVISIONAL	Ceramic Network	<a href="#">Joel Thorstensson</a>	<a href="#">3ID DID Method</a>
did:abt:	PROVISIONAL	ABT Network	ArcBlock	<a href="#">ABT DID Method</a>
did:aergo:	PROVISIONAL	<a href="#">Aergo</a>	<a href="#">Blocko</a>	<a href="#">Aergo DID Method</a>
did:ala:	PROVISIONAL	Alastria	Alastria National Blockchain Ecosystem	<a href="#">Alastria DID Method</a>
did:amo:	PROVISIONAL	AMO blockchain mainnet	<a href="#">AMO Labs</a>	<a href="#">AMO DID Method</a>
did:bba:	PROVISIONAL	Ardor	<a href="#">Attila Aldemir</a>	<a href="#">BBA DID Method</a>
did:bid:	PROVISIONAL	bif	teleinfo caict	<a href="#">BIF DID Method</a>
did:bnb:	PROVISIONAL	Binance Smart Chain	Ontology Foundation	<a href="#">Binance DID Method</a>

Marcos Allende, Sandra

<https://www.w3.org/TR/did-spec-registries>



# DIF Universal Resolver

## SUPPORTED METHODS:

did:ace	did:elem	did:github	did:key	did:ont	did:stack
did:bba	did:emtrust	did:hcr	did:kilt	did:orb	did:tz
did:btr	did:eosio	did:icon	did:lit	did:oyd	did:unisot
did:ccp	did:ethr	did:indy	did:meta	did:pkh	did:v1
did:dns	did:evan	did:io	did:moncon	did:schema	did:vaa
did:dock	did:factom	did:ion	did:mydata	did:sol	did:web
did:ebsi	did:gatc	did:jolo	did:nacl	did:sov	did:work

did-url

did:ion:EiClkZMDxPKqC9c-umQfTkR8vZ9JPhL\_xLDI9Nfk3

Resolve

Clear

Examples

RESULT

DID DOCUMENT

RESOLUTION METADATA

DOCUMENT METADATA

<https://dev.uniresolver.io/>



Il faut que j'utilise le même DID  
partout ?





# DISSOCIATIVE IDENTITY DISORDER DID ?

*“Someone with DID has multiple, distinct personalities.”*

On peut créer **plusieurs DID** (sur la **même méthode** si vous le souhaitez) de la même manière qu'on peut créer plusieurs comptes Google

`did:btcr:xz35-jznz-q9yu-ply`

`did:btcr:xkrn-xz7q-qsye-28p`

`did:ion:EiClkZMDxPKqC9c-umQfTKR8vvZ9JPh1_xLDI9Nfk38w5w`

# AVANTAGE : UN PSEUDO COMME IDENTITÉ

Il est possible de créer un DID et un DID document qui ne contiennent aucunes informations personnelles à votre sujet



Il y a une fonction mot de passe oublié  
j'espère ?



Il était une fois en 2013...



# Il a jeté son disque dur à la poubelle et perdu 7 500 bitcoins

En faisant le ménage, un informaticien britannique a jeté par inadvertance un vieux disque dur. Or, celui-ci contenait un portemonnaie bitcoin dont la valeur actuelle dépasse les ~~5 millions d'euros~~. Le retrouver est mission impossible.

*172 millions d'euros aujourd'hui*



# Un grand pouvoir implique de grandes responsabilités

Le concept d'**identité souveraine** redonne du contrôle aux utilisateurs, mais leur donne aussi de **nouvelles responsabilités**.





**Lea Kissner** ✓

@LeaKissner

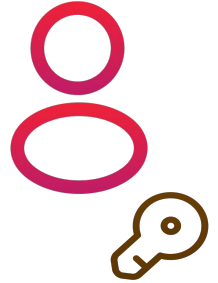
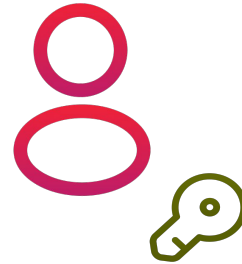
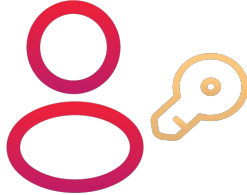
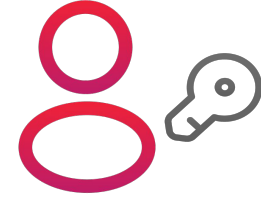


Crypto is a tool for turning a whole swathe of problems into key management problems. Key management problems are way harder than (virtually all) cryptographers think.

Head of Privacy Engineering and Chief information security officer @Twitter

<https://twitter.com/leakissner/status/1198595109756887040>

# Shamir's secret sharing (SSS)

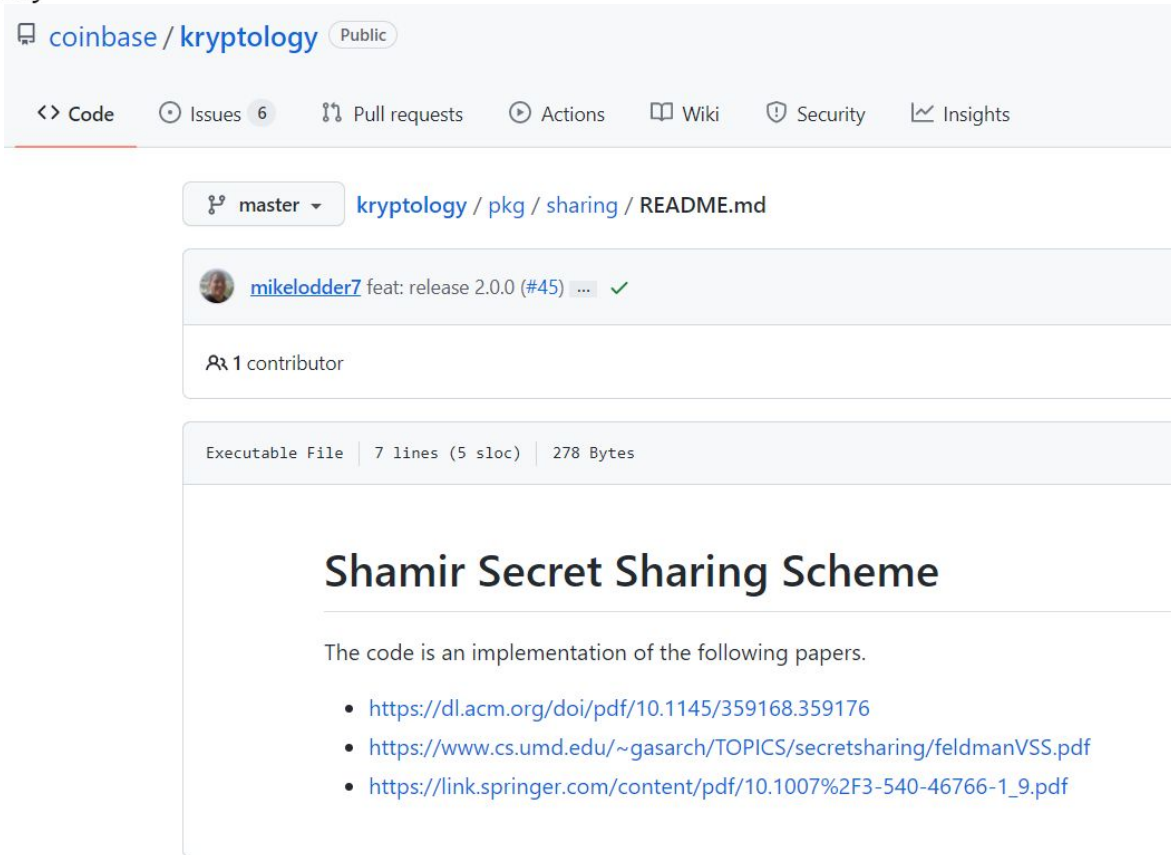




P2SH multisig is one way of dividing bitcoin keys;  
Coinbase uses Shamir's Secret Sharing which safely  
protects multiple currencies.

<https://twitter.com/coinbase/status/738837596709740544>


<https://github.com/coinbase/kryptology/blob/master/pkg/sharing/README.md>



coinbase / kryptology Public

<> Code Issues 6 Pull requests Actions Wiki Security Insights

master kryptology / pkg / sharing / README.md

 [mikelodder7](#) feat: release 2.0.0 (#45) ... ✓

1 contributor

Executable File | 7 lines (5 sloc) | 278 Bytes

## Shamir Secret Sharing Scheme

The code is an implementation of the following papers.

- <https://dl.acm.org/doi/pdf/10.1145/359168.359176>
- <https://www.cs.umd.edu/~gasarch/TOPICS/secretsharing/feldmanVSS.pdf>
- [https://link.springer.com/content/pdf/10.1007%2F3-540-46766-1\\_9.pdf](https://link.springer.com/content/pdf/10.1007%2F3-540-46766-1_9.pdf)

Utilisé dans le monde  
des crypto-monnaies



# KERI (Key Event Receipt Infrastructure)

<https://keri.one/>

Solution de gestion de clés décentralisée et autonome

- Pré-rotation des clés :
  - la **prochaine clé** est pré-générée et n'est pas devinable par quelqu'un d'extérieur
  - en cas de perte ou de vol de clé, le contrôle est rétabli en effectuant une rotation de clé qui instaure la **prochaine clé** comme clé courante valide
  - la **prochaine clé** peut être stockée ailleurs pour éviter les attaques



## CHAPITRE 3

did:union-européenne:madame-martin ? (EIDAS et EBSI)

# LE RÈGLEMENT EIDAS

La Commission européenne a lancé une initiative intitulée "**Self-sovereign identity**", l'objectif étant de mettre l'utilisateur en maîtrise de la gestion de son identité numérique en s'appuyant sur la réglementation applicable au niveau européen, à savoir le **Règlement eIDAS**.

La réglementation **eIDAS** (**E**lectronic **I**dentification **A**nd **T**rust **S**ervices) est le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein des 28 états membres de la communauté européenne.

*Vidéo sympa ici* 

<https://joinup.ec.europa.eu/collection/ssi-eidas-bridge>



# eIDAS



# EUROPEAN BLOCKCHAIN PARTNERSHIP (EBP)

Le Partenariat européen de la blockchain (EBP) est une initiative conjointe de la Commission européenne, des 27 États membres de l'Union Européenne, de la Norvège et du Lichtenstein (membres de l'Association Européenne de Libre-Échange) signé le **10 avril 2018**.

Le partenariat met en place l'**European Blockchain Services Infrastructure (EBSI)**. L'objectif est d'utiliser la blockchain pour créer des services transfrontaliers. EBSI (v1 - phase pilote) sortie au mois de juillet 2020 est basée sur deux protocoles open source à permission utilisables par tous : Hyperledger Fabric et Hyperledger Besu.

<https://blockchain.univ-lille.fr/wiki/2-lebsi-infrastructure-europeenne-de-service-blockchain/>

# Prouver son identité (did:ebsi)



did:ebsi:0xf3beac30c498d9e2686  
5f34fcaa57dbb935b0d74  
+  
Clé privée dans le wallet



EBSI



**DID Document  
contenant la clé  
publique**





# CHAPITRE 4

Show me the code !



## VERIFIABLE CREDENTIAL

Métadonnées

Déclarations

Vérification



## Métadonnées

## VERIFIABLE CREDENTIAL

```
{
  "@context": [ ... ],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2021-07-02T11:12:42Z",
  "credentialSubject": {
    "id": "did:example:123456789abcdefghi",
    "degree": "Bachelor of Science",
    "degreeType": "BachelorDegree",
    "degreeSchool": "Example University"
  },
  "proof": {
    "type": "Ed25519Signature2018",
    "created": "2021-07-07T00:45:40Z",
    "jws": "eyJhbGciOiJIJFZERTQSIiwiaWF0IjoiMjAyMS00Ny00OC0wMC00NTM0IiwiaXNjaWkiOiJkaWQ6ZXNjaWki",
    "proofPurpose": "assertionMethod",
    "verificationMethod":
      "https://example.edu/issuers/565049/keys/1"
  }
}
```

## Déclarations

### VERIFIABLE CREDENTIAL

```
{
  "@context": [ ... ],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2021-07-02T11:12:42Z",
  "credentialSubject": {
    "id": "did:example:123456789abcdefghi",
    "degree": "Bachelor of Science",
    "degreeType": "BachelorDegree",
    "degreeSchool": "Example University"
  },
  "proof": {
    "type": "Ed25519Signature2018",
    "created": "2021-07-07T00:45:40Z",
    "jws": "eyJhbGciOiJIJFZERTQSIiwiaWF0IjoiMjAyMS00Ny00M1Q0OjA0OjQ0IiwiaXNja3kiOiJ0eXBlIjoiYXNja3kiLCJ0eXBlIjoiYXNja3kiLCJ0eXBlIjoiYXNja3ki",
    "proofPurpose": "assertionMethod",
    "verificationMethod":
      "https://example.edu/issuers/565049/keys/1"
  }
}
```

## VERIFIABLE CREDENTIAL

Vérification

```
{
  "@context": [ ... ],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2021-07-02T11:12:42Z",
  "credentialSubject": {
    "id": "did:example:123456789abcdefghi",
    "degree": "Bachelor of Science",
    "degreeType": "BachelorDegree",
    "degreeSchool": "Example University"
  },
  "proof": {
    "type": "Ed25519Signature2018",
    "created": "2021-07-07T00:45:40Z",
    "jws": "eyJhbGciOiJIJZERTQSIIsImI2NCI6ZmFsc2Us...",
    "proofPurpose": "assertionMethod",
    "verificationMethod":
      "https://example.edu/issuers/565049/keys/1"
  }
}
```



## VERIFIABLE PRESENTATION

Métadonnées

## VERIFIABLE CREDENTIAL(s)

Métadonnées

Déclarations

Vérification

Vérification

## Métadonnées

## VERIFIABLE PRESENTATION

```
{
  "@context": [ ... ],
  "id": "http://example.edu/presentations/1436",
  "type": "VerifiablePresentation",
  "verifiableCredential": [
    { ... },
    { ... }
  ],
  "proof": {
    "type": "RsaSignature2018",
    "created": "2018-09-14T21:19:10Z",
    "proofPurpose": "authentication",
    "verificationMethod":
      "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",
    "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
    "domain": "4jt78h47fh47",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2Us..."
  }
}
```

## VERIFIABLE CREDENTIAL(S)

## VERIFIABLE PRESENTATION

```
{
  "@context": [ ... ],
  "id": "http://example.edu/presentations/1436",
  "type": "VerifiablePresentation",
  "verifiableCredential": [
    { ... },
    { ... }
  ],
  "proof": {
    "type": "RsaSignature2018",
    "created": "2018-09-14T21:19:10Z",
    "proofPurpose": "authentication",
    "verificationMethod":
      "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",
    "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
    "domain": "4jt78h47fh47",
    "jws": "eyJhbGciOiJIUzI1NiIsImI2NCI6ZmFsc2Us..."
  }
}
```

## Vérification

## VERIFIABLE PRESENTATION

```
{
  "@context": [ ... ],
  "id": "http://example.edu/presentations/1436",
  "type": "VerifiablePresentation",
  "verifiableCredential": [
    { ... },
    { ... }
  ],
  "proof": {
    "type": "RsaSignature2018",
    "created": "2018-09-14T21:19:10Z",
    "proofPurpose": "authentication",
    "verificationMethod":
      "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",
    "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
    "domain": "4jt78h47fh47",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2Us..."
  }
}
```



## DID DOCUMENT

Identifiant  
du sujet

Identifiant  
du contrôleur  
(facultatif)

Vérification

Services



## DID DOCUMENT

Identifiant  
du sujet

Identifiant  
du contrôleur  
(facultatif)

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "did:example:123456789abcdefghi",
  "authentication": [
    "did:example:123456789abcdefghi#keys-1"
  ],
  "verificationMethod": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase":
      "zH3C2AVvLMv6gmMnam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }],
  "service": [{
    "id": "did:example:123#linked-domain",
    "type": "LinkedDomains",
    "serviceEndpoint": "https://bar.example.com"
  }]
}
```

## Vérification

## DID DOCUMENT

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "did:example:123456789abcdefghi",
  "authentication": [
    "did:example:123456789abcdefghi#keys-1"
  ],
  "verificationMethod": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase":
      "zH3C2AVvLMv6gmMnam3uVAjZpfcJCwDwnZn6z3wXmqPV"
  }],
  "service": [{
    "id": "did:example:123#linked-domain",
    "type": "LinkedDomains",
    "serviceEndpoint": "https://bar.example.com"
  }]
}
```

## Vérification

## DID DOCUMENT

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "did:example:123456789abcdefghi",
  "authentication": [
    "did:example:123456789abcdefghi#keys-1"
  ],
  "verificationMethod": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase":
      "zH3C2AVvLMv6gmMnam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }],
  "service": [{
    "id": "did:example:123#linked-domain",
    "type": "LinkedDomains",
    "serviceEndpoint": "https://bar.example.com"
  }]
}
```

## DID DOCUMENT

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "did:example:123456789abcdefghi",
  "authentication": [
    "did:example:123456789abcdefghi#keys-1"
  ],
  "verificationMethod": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase":
      "zH3C2AVvLMv6gmMnam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }],
  "service": [{
    "id": "did:example:123#linked-domain",
    "type": "LinkedDomains",
    "serviceEndpoint": "https://bar.example.com"
  }]
}
```

Services



# CHAPITRE 5

C'est le moment de se lancer ?

# TECHNOLOGY RADAR

ADOPT

TRIAL

ASSESS

HOLD



Decentralized identity



Verifiable credentials





# LES ACTEURS DU MONDE DE L'IDENTITÉ DÉCENTRALISÉE

evernym



RSA

W3C



sovrin

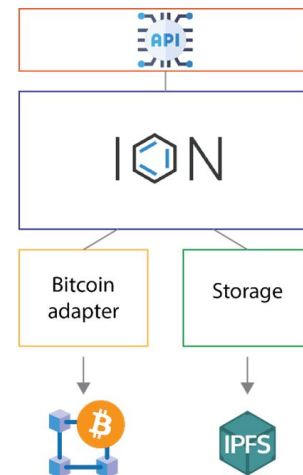
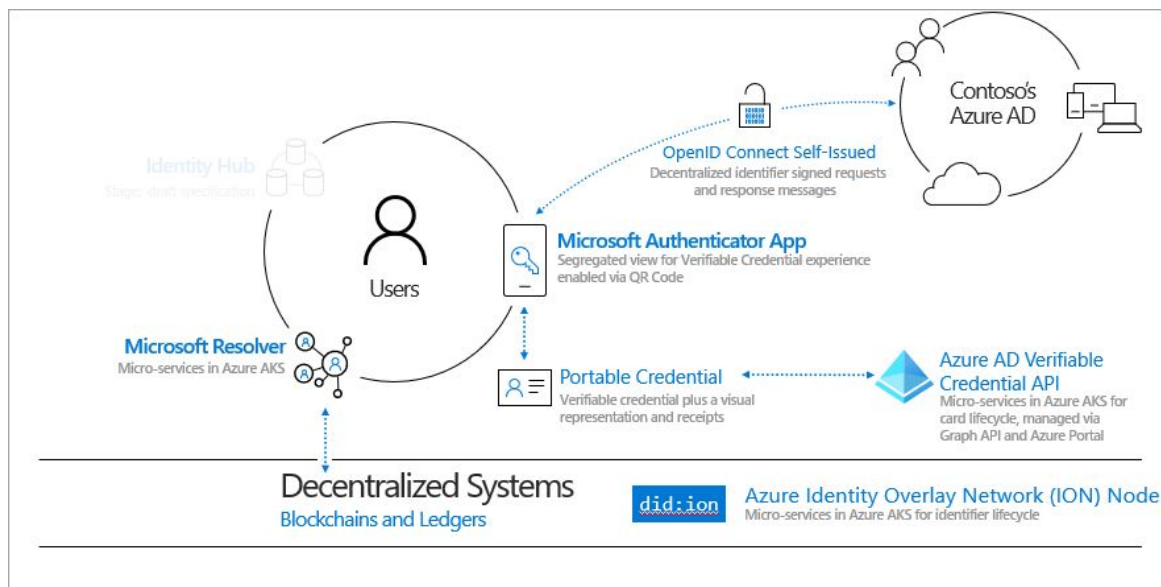


HYPERLEDGER



# AZURE AD VERIFIABLE CREDENTIALS

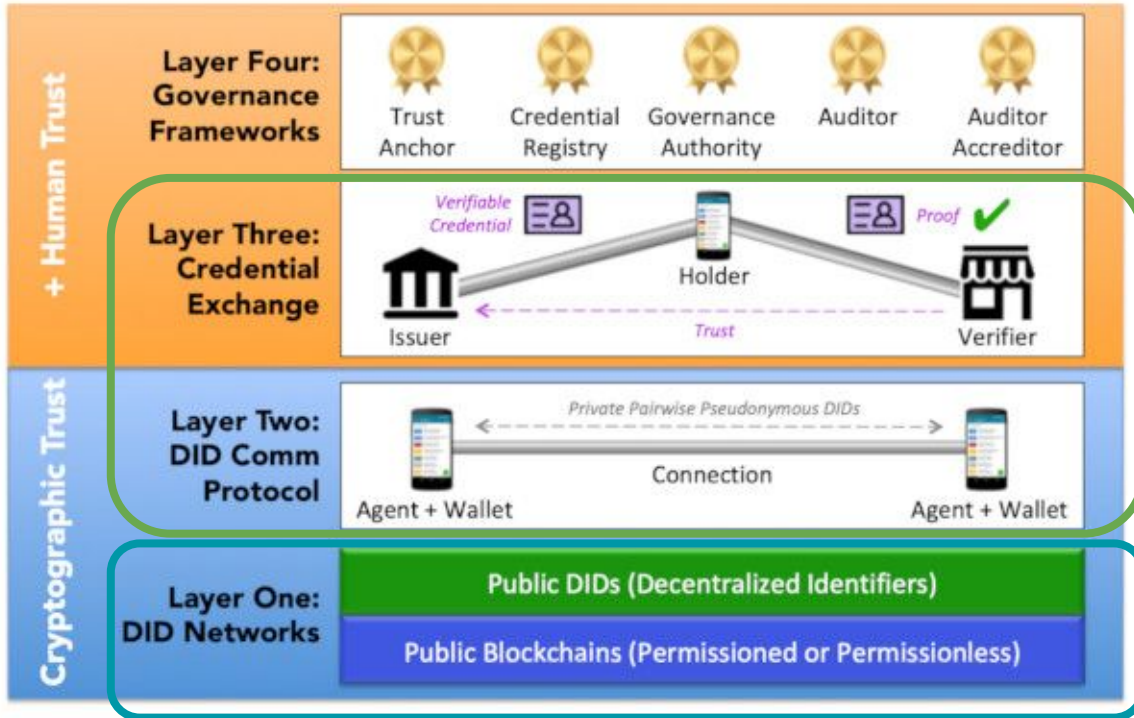
Azure AD Verifiable Credentials sortie en avril 2021 est basé sur ION (Identity Overlay Network).







# HYPERLEDGER IDENTITY WORKING GROUP



**HYPERLEDGER**  
**URSA**



**HYPERLEDGER**  
**ARIES**



**HYPERLEDGER**  
**INDY**

© ZENIKA 2021 All rights reserved - Proprietary & confidential



# IBM Digital Health Pass

## Digital Health Pass is designed for various entities

### For issuers

Pharmacies and labs can issue verifiable credentials—such as test results or COVID-19 vaccine certificates—and send to an individual's smartphone.

[See how](#) →

### For individuals

An individual can receive health credentials, load them into their smartphone and share with an organization as proof of health status.

[Learn more](#) →

### For verifiers

Check the health and safety of employees and individuals upon entrance—whether it's the workplace, a stadium, airport or elsewhere.

[Discover more](#) →



jack ✓  
@jack



this will likely be our most important contribution to the internet. proud of the team. [#web5](#)

(RIP web3 VCs 🤔)

[developer.tbd.website/projects/web5/](https://developer.tbd.website/projects/web5/)

Traduire le Tweet

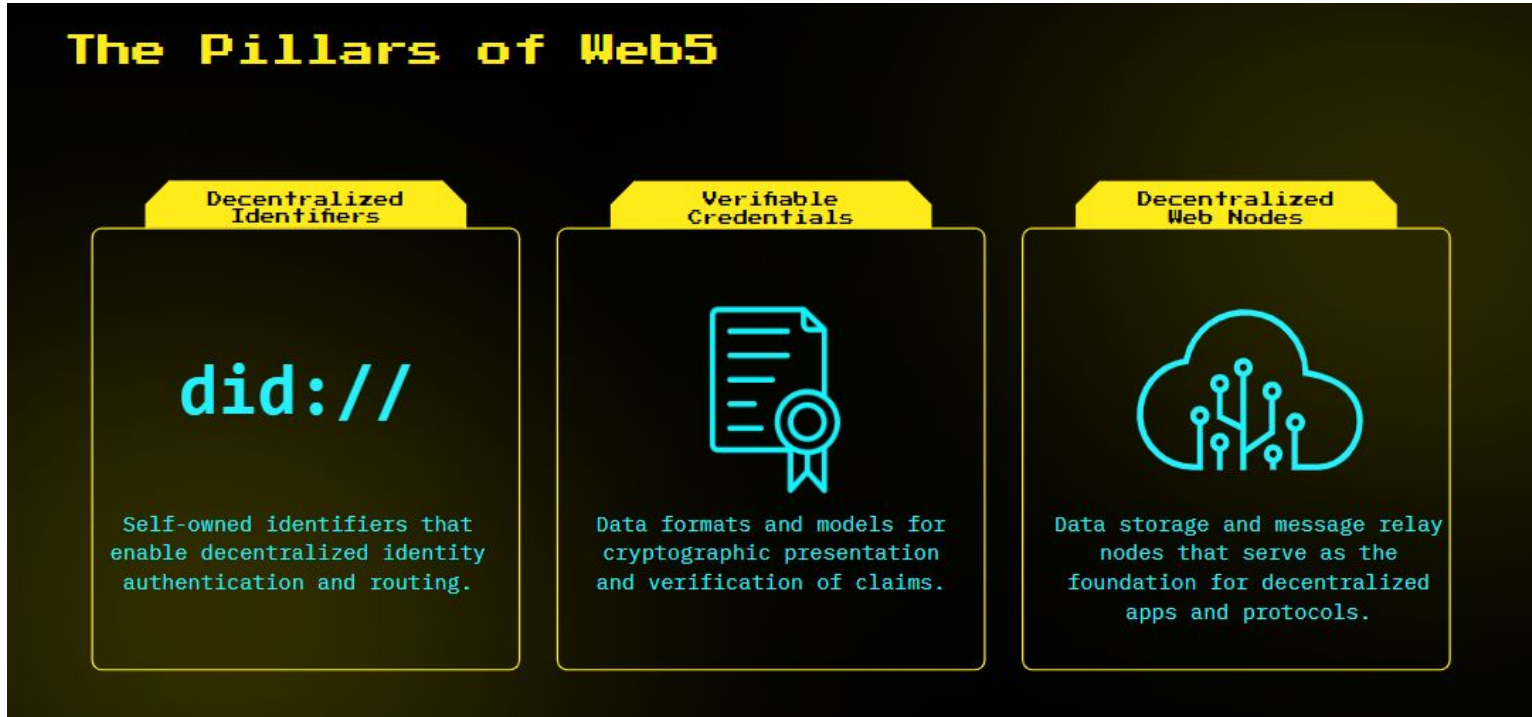


**TBD** ✓ @TBD54566975 · 10 juin

Web5: An extra decentralized web platform  
[docs.google.com/presentation/d...](https://docs.google.com/presentation/d...)

7:35 PM · 10 juin 2022 · Twitter Web App

# “Web 5” by TBD



<https://docs.google.com/presentation/d/1SaHGyY9TjPg4a0VNLCsfchoVG1yU3ffTDsPRcU99H1E/edit>

<https://developer.tbd.website/projects/web5/>



**jwerle** @josephwerle · 11 juin



Now everyone cares about DIDs. Awesome



3



1



5



**jwerle**



@josephwerle

I guess now that a billionaire cares, the herd follows

[Traduire le Tweet](#)

8:40 PM · 11 juin 2022 · Twitter for Android



# CAS D'ÉTUDE



did:twit ?

# did:twit

Specs :

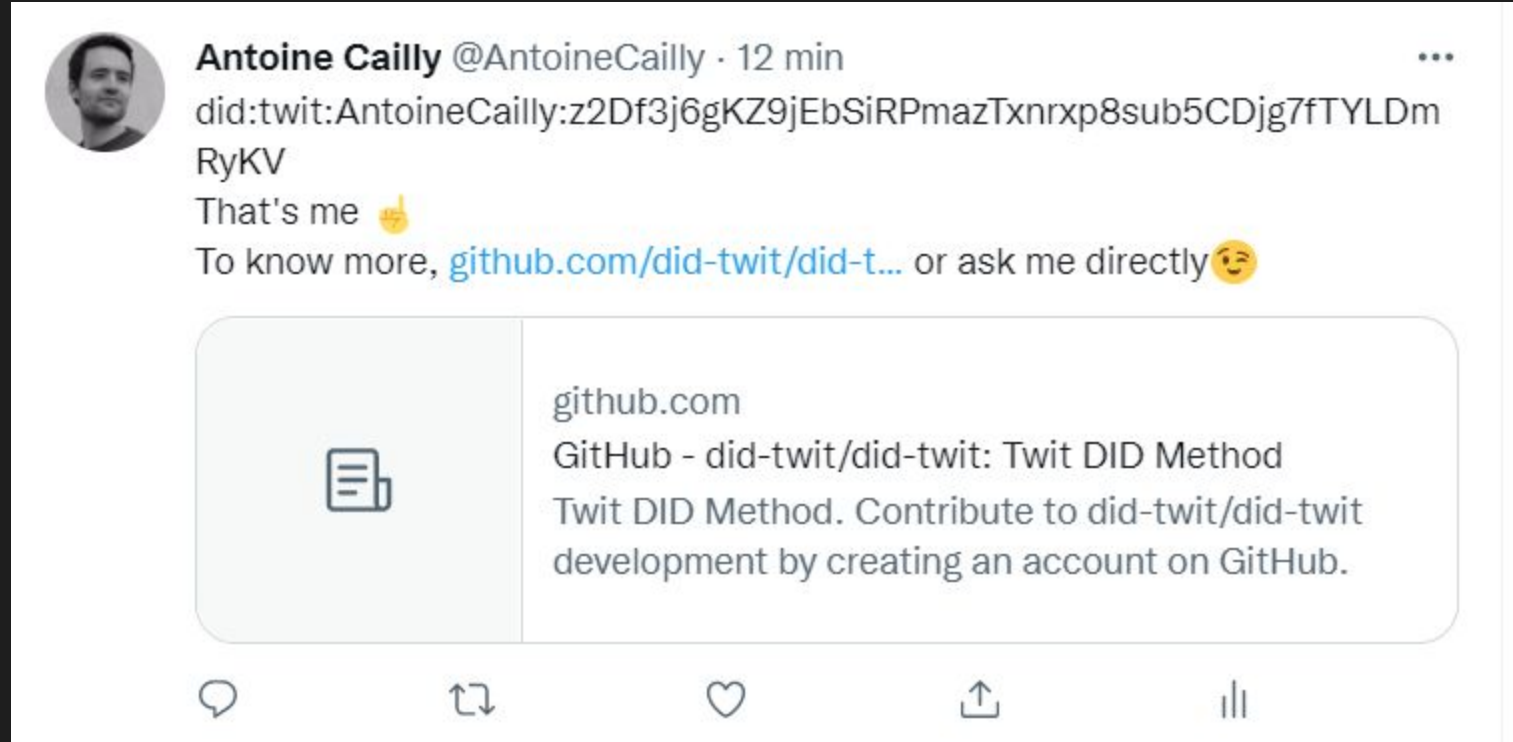
<https://github.com/did-twit/did-twit/blob/master/spec/index.md>

CLI :

<https://github.com/did-twit/did-twit-cli>



# Create / Read




A screenshot of a tweet from Antoine Cailly (@AntoineCailly) posted 12 minutes ago. The tweet contains a DID URL, a thumbs up emoji, and a link to a GitHub repository. Below the text is a link preview for the GitHub repository 'did-twit/did-twit'. The interface includes standard social media interaction icons at the bottom.

**Antoine Cailly** @AntoineCailly · 12 min

did:twit:AntoineCailly:z2Df3j6gKZ9jEbSiRPmazTxnrxp8sub5CDjg7fTYLDmRyKV

That's me 👍

To know more, [github.com/did-twit/did-t...](https://github.com/did-twit/did-twit) or ask me directly 😊

 github.com  
GitHub - did-twit/did-twit: Twit DID Method  
Twit DID Method. Contribute to did-twit/did-twit development by creating an account on GitHub.

🗨️ ↻ ❤️ ↗ 📊

```
did-twit-cli manage create --username="AntoineCailly"
```

Hello

World! .AnUdNwcK36NCyTdDCx8kZbXno9shvKaUZxTZr8tiiTQFHFbzCCwT  
Zo9or4XVzvxGBbSqhMFf2f23RuzbecNXmPeeRYenR74wpgoyRz8sBjyt8Sy  
icbkafrU6nSGtHAXRjBouLVLBJYTibgXvyYs68LXVjf6mrrNTQ5afDPFMmZ  
nSzzNnbpvethNwN6Eqeb4pHi7CCqJWNn5iEvdYqGYFXuXotF9q3xVTasUTF  
UxAVRVXJz8FfhYzZ2ibqsv5K8Ego2hMmDc8rZhcazhGgZHpYqFWtHuq1fjr  
c7jstxjqePx4aD3CNuwpHpGXZqiS9VzLrJjKUb48f2DPfLTNwqKKxv9bEAV  
xS14UVwiXRyo9CwgMctHXDwfsXyL6Jd8hoqLFC1JrFCyqXNX1sPzpj qfSpH  
Mr2GZvyKoDwmAfopLy3gbKCKnBreS2FRRE

```
did-twit-cli tweet --tweet="Hello World!"  
--did="did:twit:AntoineCailly:z2Df3j6gKZ9jEbSiRPmazTxnrxp8sub5CDjg7fTYLDmRyKV" 90
```

# Verify

```
did-twit-cli tweet verify  
--tweet="Hello
```

```
World! .AnUdNwcK36NCyTdDCx8kZbXno9shvKaUZxTZr8tiiTQFHFbzCCwTZo9or4XVzvxGBbSqhMFf2f23R  
uzbecNXmPeeRYenR74wpgoyRz8sBjyt8SyicbkafrU6nSGtHAXrjBouLVLBJYTibgXvyYs68LXVjf6mrrNTQ  
5afDPFMmZnSzzNnbpvethNwN6Eqeb4pHi7CCqJWnN5iEvdYqGYFXuXotF9q3xVTasUTFUxAVRVXJz8FfhYzZ  
2ibqsv5K8Ego2hMmDc8rZhcazhGgZHpYqFwtHuq1fjrc7jstxjqePx4aD3CNUwpHpGXZqiS9VzLrJjKUb48f  
2DPfLTNwqKKxv9bEAVxS14UVwiXRyo9CwgMctHXDwfsXyL6Jd8hoqLFC1JrFCyqXNX1sPzpjqfSpHMr2GZvy  
KoDwmAfopLy3gbKCknBreS2FRRE"  
--did="did:twit:AntoineCailly:z2Df3j6gKZ9jEbSiRPmazTxnrxp8sub5CDjg7fTYLDmRyKV"
```

> Tweet valid.



# Update

Accueil ✦

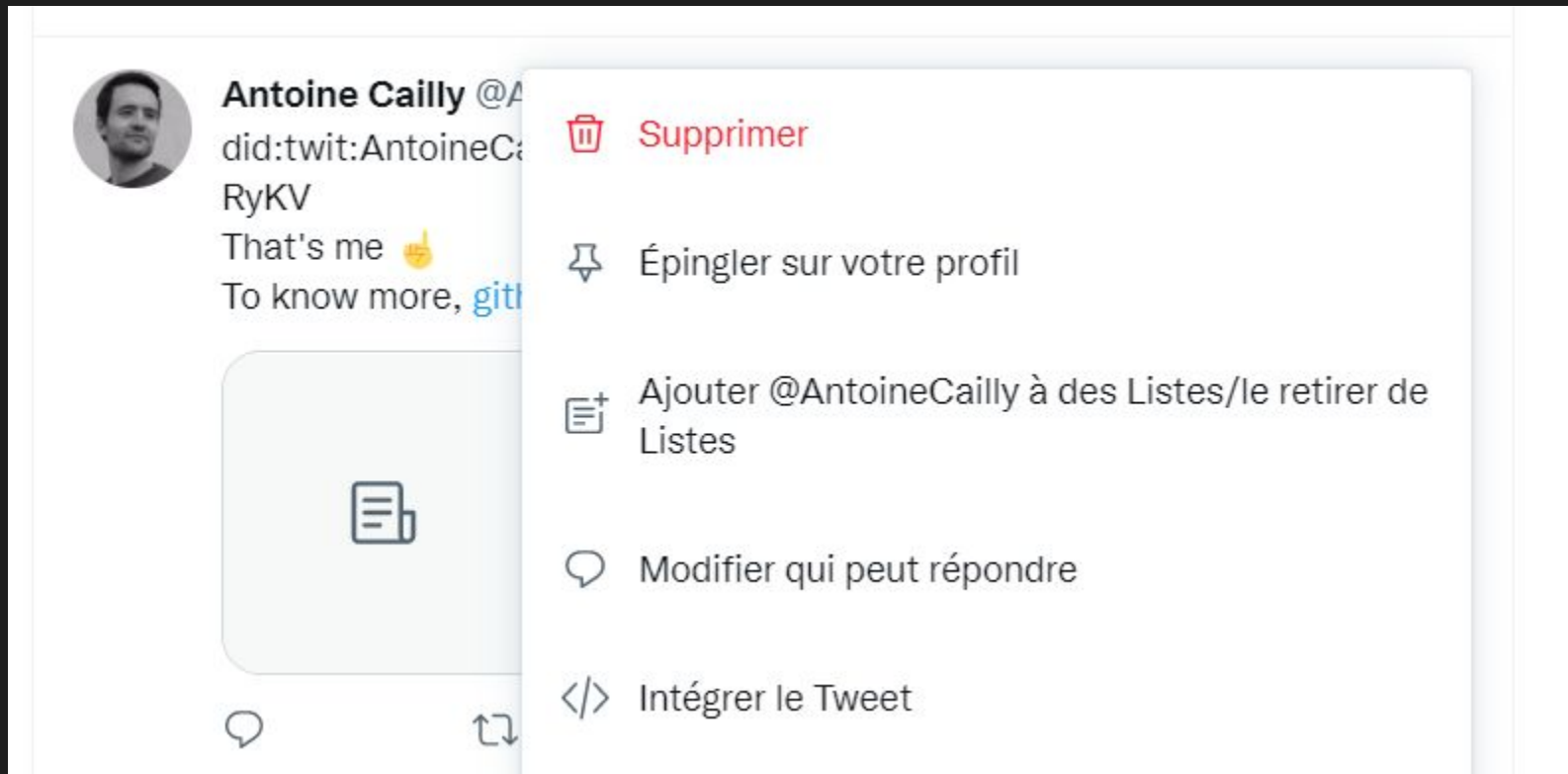
 My new `did:twit` is ...

 **Tout le monde peut répondre**






---

       |  **Tweeter**

# Delete



The image shows a screenshot of a tweet from Antoine Cailly (@AntoineCailly) with a context menu open. The tweet text is partially visible: "That's me 👍 To know more, git". The context menu is open over the tweet and contains the following options:

-  **Supprimer**
-  Épingler sur votre profil
-  Ajouter @AntoineCailly à des Listes/le retirer de Listes
-  Modifier qui peut répondre
-  Intégrer le Tweet

# did:twit

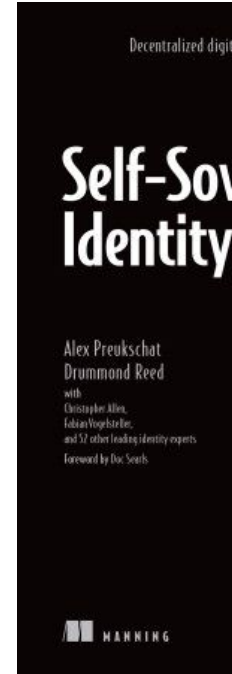
Specs :

<https://github.com/did-twit/did-twit/blob/master/spec/index.md>

CLI :

<https://github.com/did-twit/did-twit-cli>

# DES QUESTIONS ?



*Pour aller (beaucoup) plus loin :*

<https://www.manning.com/books/self-sovereign-identity>



**MERCI**