



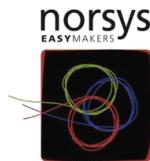
# zenika

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

# MERCI LES SPONSORS !



« Etoile »



« Flocon »





# LES SPEAKERS



**Antoine Cailly**

Consultant Front-End &  
Formateur



**Adrien Wattez**

Consultant Back-End &  
Formateur



© ZENIKA 2021 All rights reserved - Proprietary & confidential

# INTRODUCTION

# Il était une fois...

Avant on avait une identité sur chaque site/app, c'était chiant !

Avec OpenID connect, on peut se connecter avec notre identité Google sur plusieurs sites, c'est moins chiant !

Mais cette identité appartient à  
Google.

Si Google meurt, mon identité meurt.

Si Google me bloque, j'ai perdu mon  
accès à tous les sites d'un coup.

“Je fais pas confiance à Google”

Se connecter à plusieurs services avec une identité qui m'appartient ?

a.k.a. une identité souveraine ou Self Sovereign Identity (SSI).



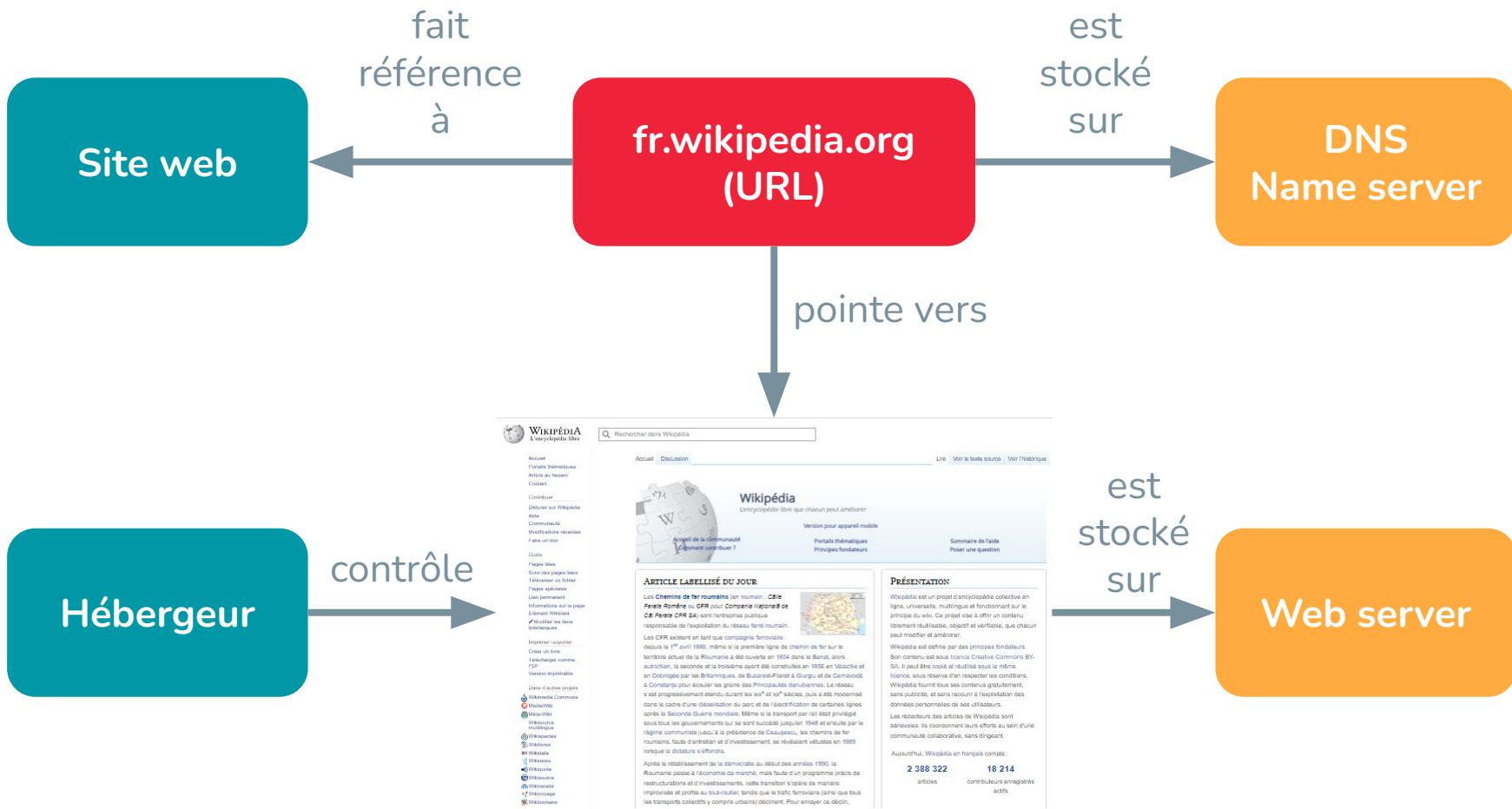
# CHAPITRE 1

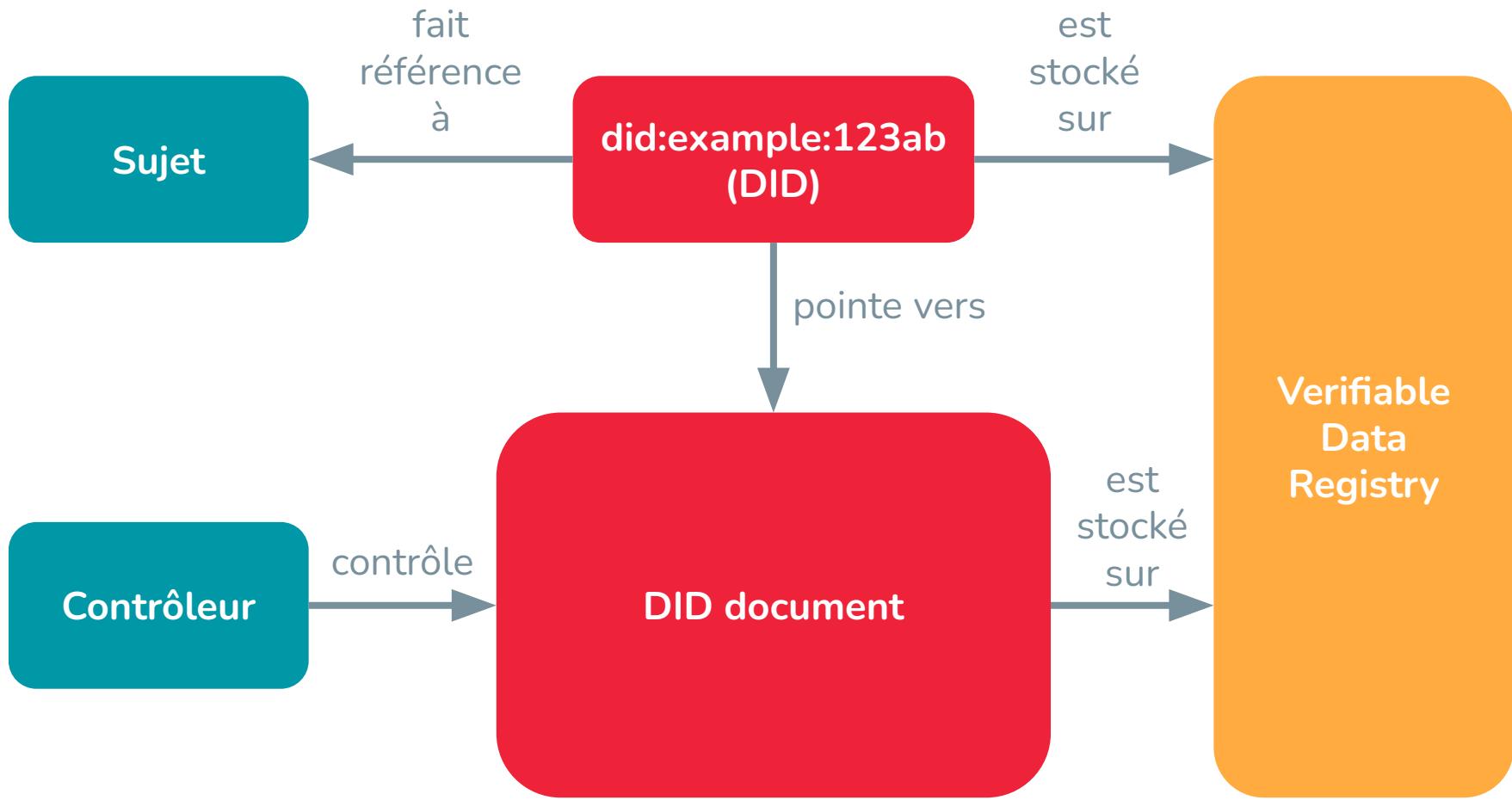
## Les Decentralized IDentifiers (DID)



**UNE IDENTITÉ QUI  
M'APPARTIENT**

Je crée un DID et un DID document.





Focus sur le DID Document.



## DID DOCUMENT

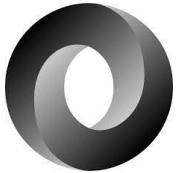
Identifiant  
du sujet

Identifiant  
du contrôleur  
(facultatif)

Vérification

Services

## DID DOCUMENT



JSON

```
{  
  "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"  
  }]  
}
```

## DID DOCUMENT



Linked Data  
(JSON-LD)

```
{  
  "@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"  
      ]  
}
```

Identifiant  
du sujet

Identifiant  
du contrôleur  
(facultatif)



## DID DOCUMENT

Vérification

```
{  
  "@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

Vérification

```
{  
  "@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":  
      "zH3C2AVvLMv6gmMNm3uVAjZpfkcJCwDwnZn6z3wXmqPV"  
  }],  
  "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

Moi seul peut modifier mon DID  
document.



# DES CHIFFRES ET DES LETTRES

L'**identité numérique** requiert le traitement de données qui peuvent être **sensibles**. Le recours à des technologies permettant de les authentifier et de les **protéger** est alors nécessaire. Les données numériques peuvent être **chiffrées** et/ou **signées numériquement**.

- Le **chiffrement** permet de garantir la **confidentialité** des données ; seule la personne autorisée peut déchiffrer les données.
- La **signature numérique** permet d'assurer l'**intégrité des données**, et de pouvoir les authentifier. Elle est notamment basée sur le chiffrement asymétrique.

# CRYPTOGRAPHIE ASYMÉTRIQUE

Cryptographie à clé publique ou cryptographie asymétrique.

CLÉ PRIVÉE

#      #

un incroyable  
nombre  
premier.

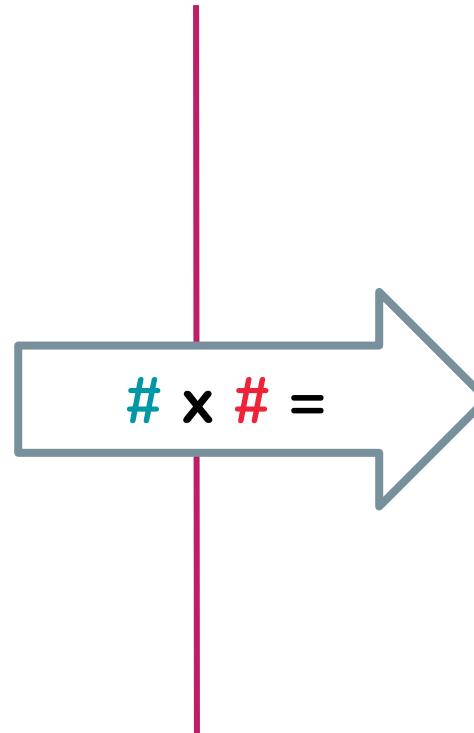
un autre  
incroyable  
nombre  
premier.



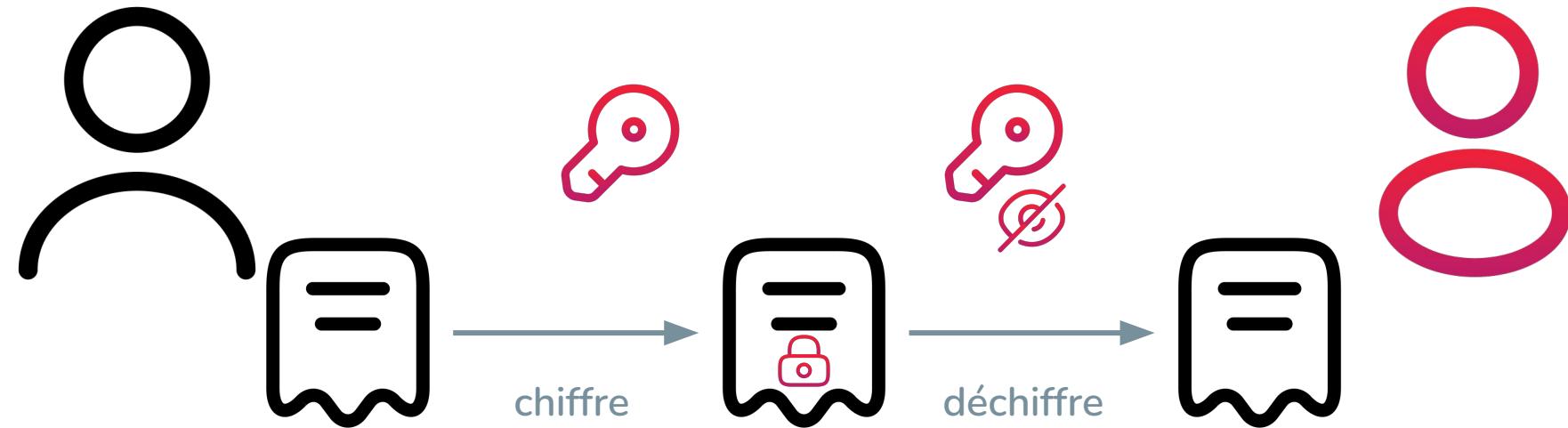
CLÉ PUBLIQUE

#

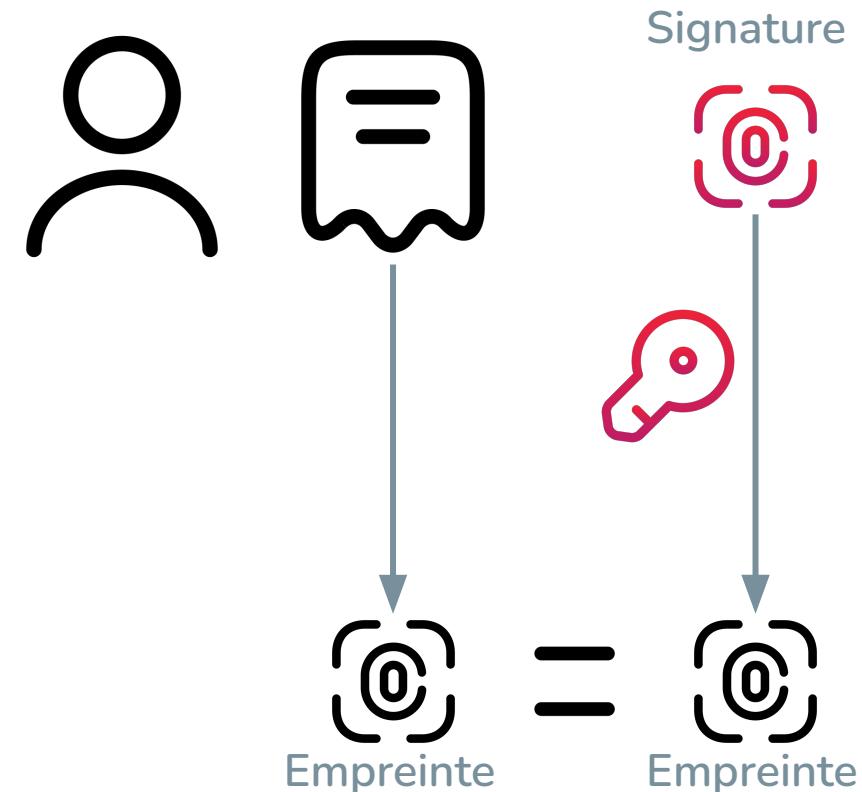
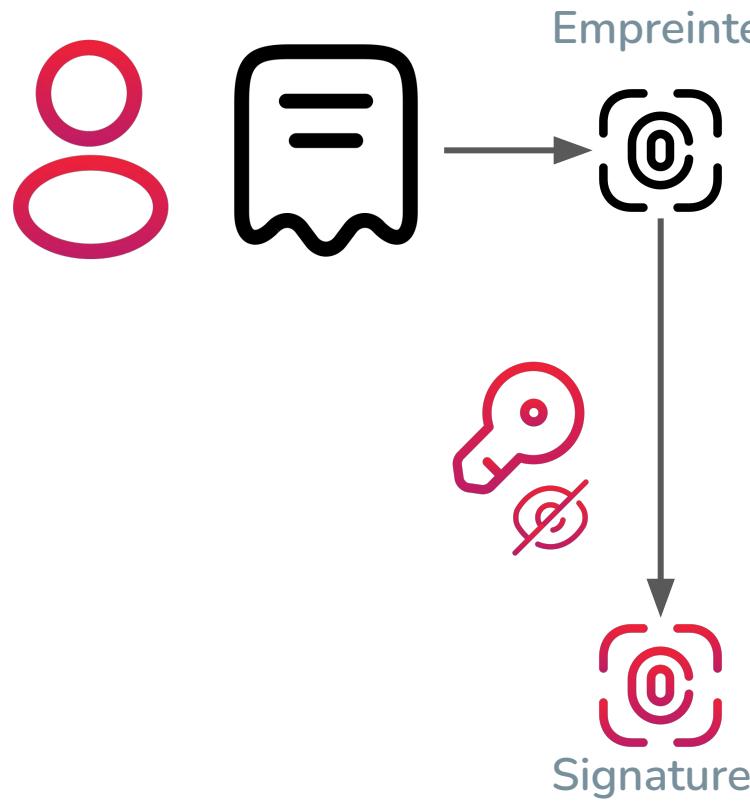
Le produit de ses deux nombres premiers utilisés pour produire la clé privée.  
L'opération inverse est quasiment impossible.



# CHIFFREMENT



# SIGNATURE



# ELLES SONT OU MES CLÉS ?

Dans un modèle décentralisé, les utilisateurs créent leur propre identité à l'aide de leurs outils de création d'identité locaux (tels que ceux fournis par une application de portefeuille numérique). La nouvelle identité réside dans le portefeuille local de l'utilisateur, qui reste en toute sécurité sur les propres appareils de l'utilisateur.



# ELLES SONT OU MES CLÉS ?



## 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":  
          "zH3C2AVvLMv6gmMNm3uVAjZpfkcJCwDwnZn6z3wXmqPV"  
      }],  
      "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/ed25519-2018/v1",  
    "https://w3id.org/security/suites/x25519-2019/v1",  
    "https://w3id.org/security/suites/secp256k1-2019/v1",  
    "https://w3id.org/security/suites/jws-2020/v1"  
,  
  "verificationMethod": [  
    {  
      "id": "did:example:123#key-0",  
      "type": "Ed25519VerificationKey2018",  
      "controller": "did:example:123",  
      "publicKeyBase58": "3M5RCDjPTWPkKSN3sxUmmMqHbmRPegYP1tjcKyrDbt9J"  
    },  
    {  
      "id": "did:example:123#key-1",  
      "type": "JsonWebKey2020",  
      "controller": "did:example:123",  
      "publicKeyJwk": {  
        "kty": "EC",  
        "crv": "P-256",  
        "x": "Er6KSSnAjI70ObRWhlaMgqyIOQYrDJTE94ej5hybQ2M",  
        "y": "pPVzCOTJwgikPjuUE6UebfZySqEJ0ZtsWFpj7YSPGEk"  
      }  
    }  
  ]  
}
```



# WHAT DID YOU DOCUMENT ?

1. L'ID ou le DID (pour de l'auto-description)
2. Différentes clés publiques (pour la vérification)
3. Différentes méthodes d'authentifications / d'usages
4. Différents services (interopérabilité / interaction)
5. ~~Timestamp (pour l'historique)~~
6. ~~Une preuve / signature (pour l'intégrité)~~

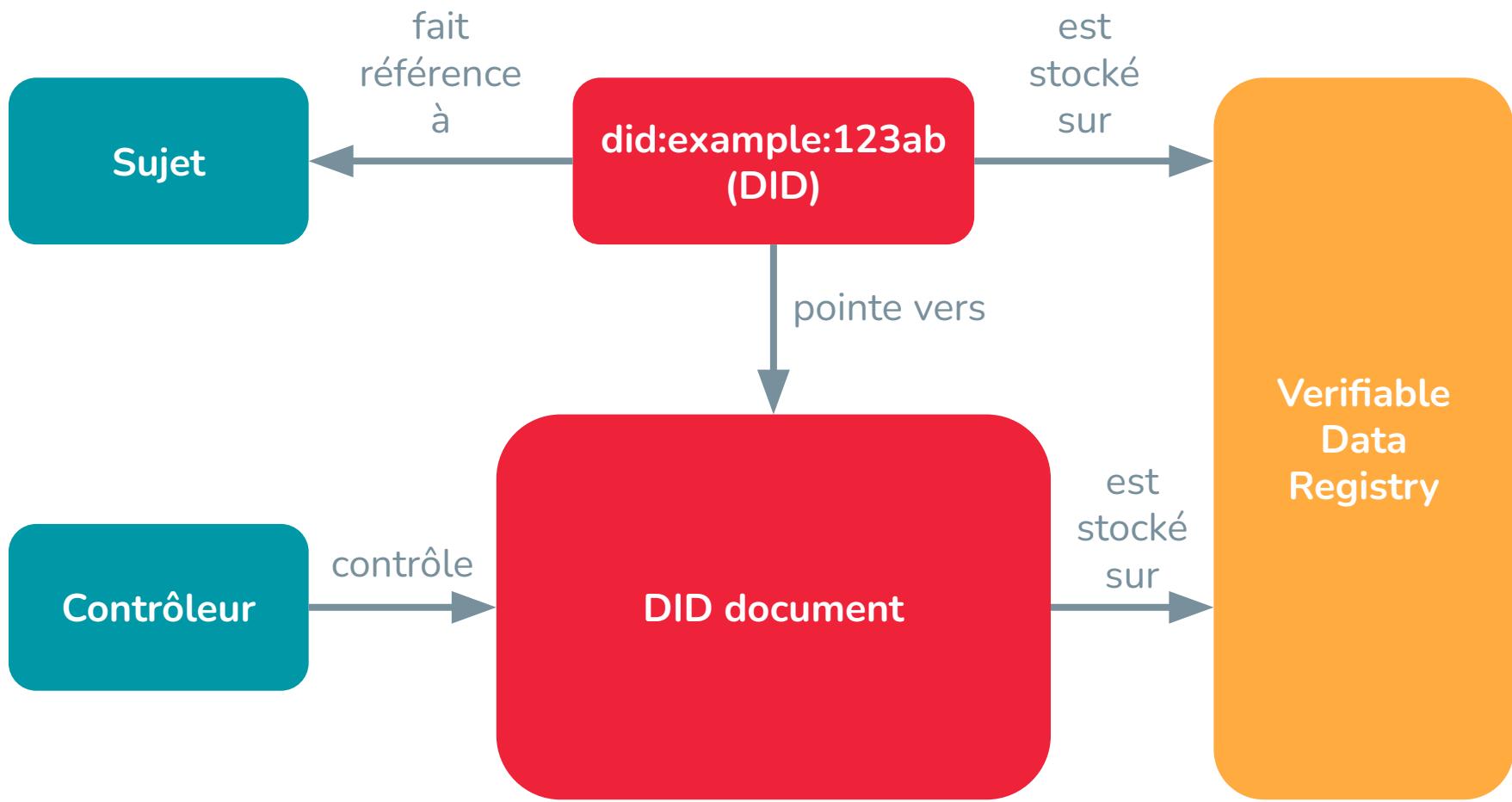


<https://www.w3.org/TR/did-core/>



## SE CONNECTER À PLUSIEURS SERVICES

Mais du coup c'est quoi un DID ?





# OUPS! I DID IT AGAIN

Un **DID**, ou Decentralized Identifier (**Decentralized ID**) est en réalité un **URI**.  
Les **DIDs** suivent le même pattern que les **URN** afin d'être *flexible*.

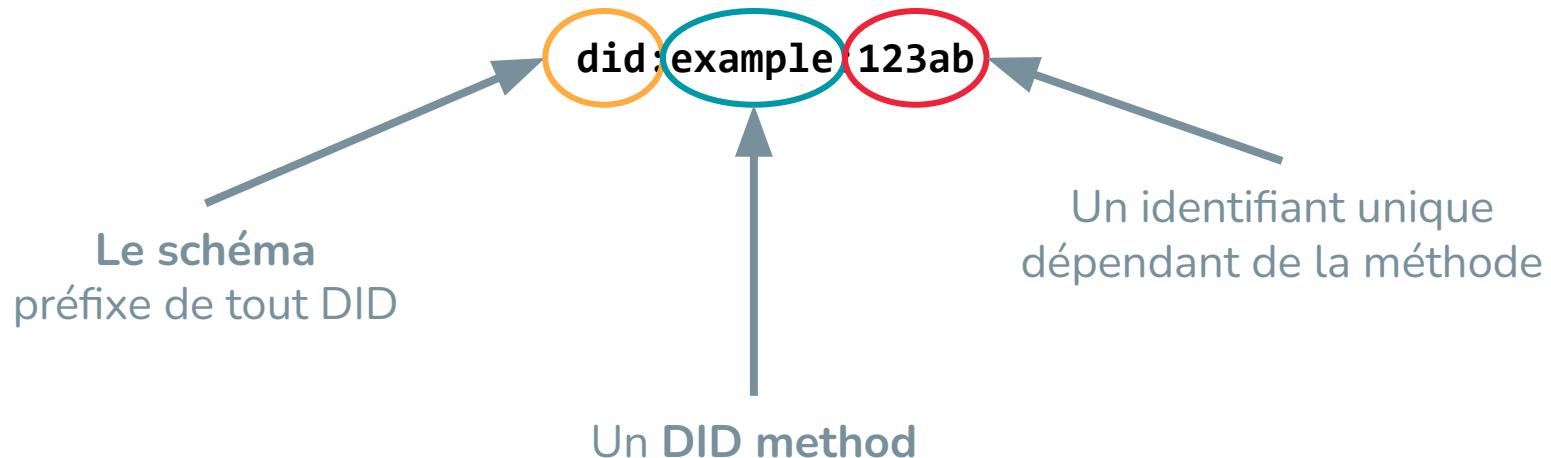
**did:example:123ab**

Un URN **ISBN** (International Standard Book Number) [RFC 3187](#):

**URN:ISBN:951-0-18435-7**

# OUPS! I DID IT AGAIN

Un DID, ou Decentralized Identifier (**Decentralized ID**) est en réalité un **URI**.



# LA FAMEUSE MÉTHODE DID

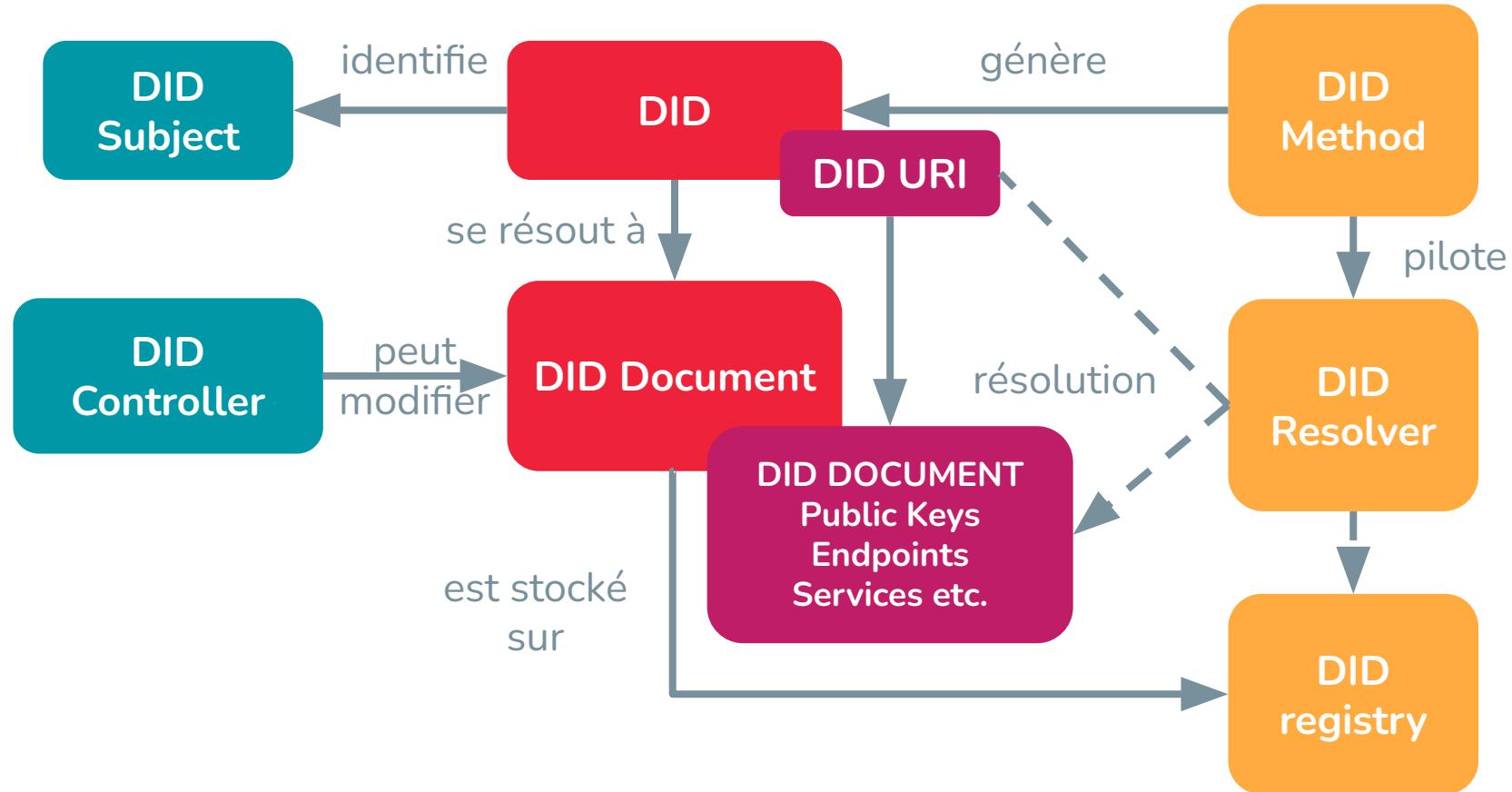
Un **DID Method**, est une définition de l'implémentation du DID. Un **DID method** est souvent associées à un registre de données vérifiable particulier (**DID Registry**). Chaque DID dispose d'une méthode qui spécifie le protocole permettant de récupérer/manipuler le DID en question.



**bitcoin**  
**did:btcr:8yv2-xzpq-qqqq-9yce-nk**

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

# L'ARCHITECTURE DID



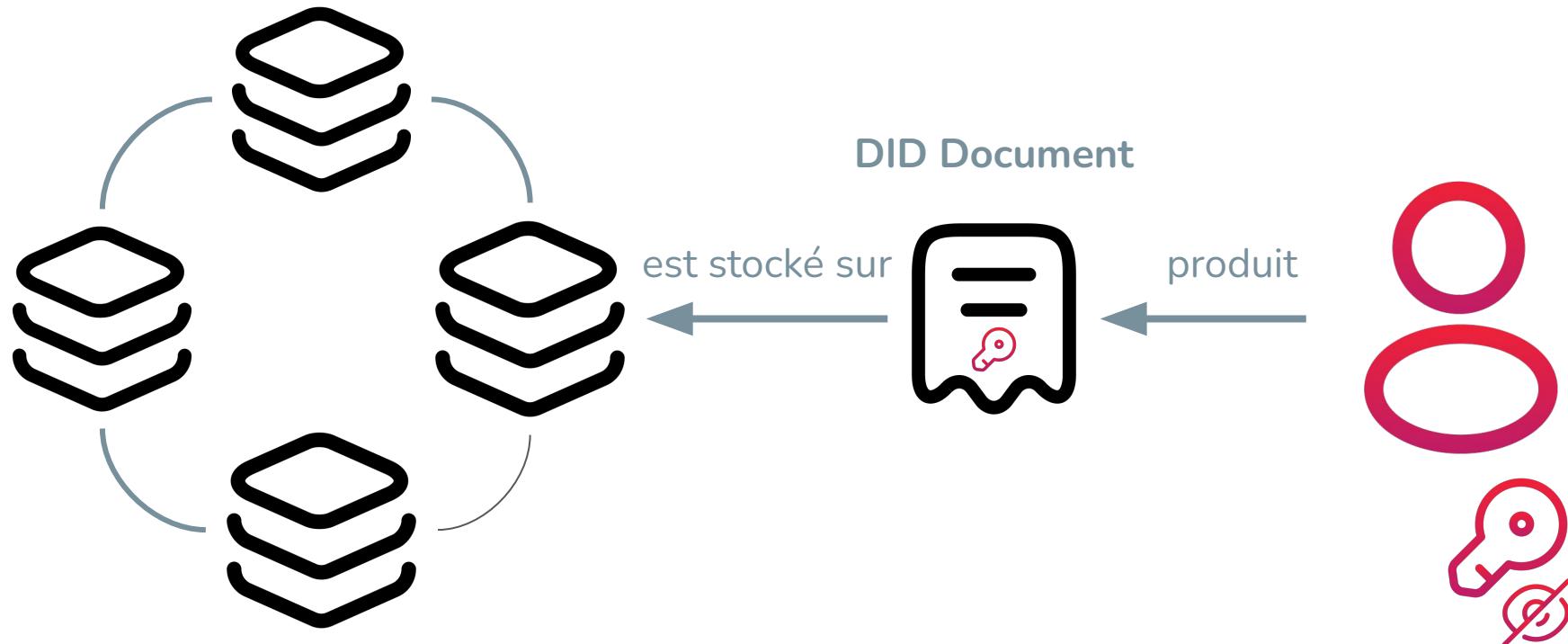


# DID YOU SAY TOO MANY NEW WORDS ?

- **DID:** identifiant sous forme d'une chaîne de caractères
- **Méthode:** utilisée pour générer les identifiants (DID)
- **Document:** associé au DID, contenant plusieurs informations
- **Contrôleur:** composant permettant de gérer le document
- **Résolveur:** composant permettant d'obtenir le document DID à partir de l'identifiant
- **Sujet:** sujet de l'identification
- **Registre de données vérifiables:** stocke et maintient les identifiants (DID Registry)

Je publie mon DID document sur un registre dans lequel j'ai confiance et accessible à tous les services.

# UN REGISTRE ACCESSIBLE PAR TOUS 🤔



# SOUVENEZ-VOUS DE CES MÉTHODES

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

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



did:btcr:



did:sov:



did:ion:



ethereum

did:ethr:



SOLANA

did:sol:



did:key:



did:dns: vs did:web:

# 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 (mais il faut sécuriser les clés privées).

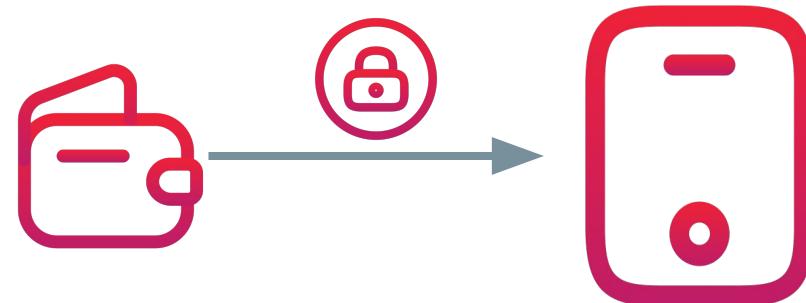
Il ne faut pas oublier que le concept d'**identité auto-souveraine** redonne du contrôle aux utilisateurs, mais leur donne aussi de **nouvelles responsabilités**.

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

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

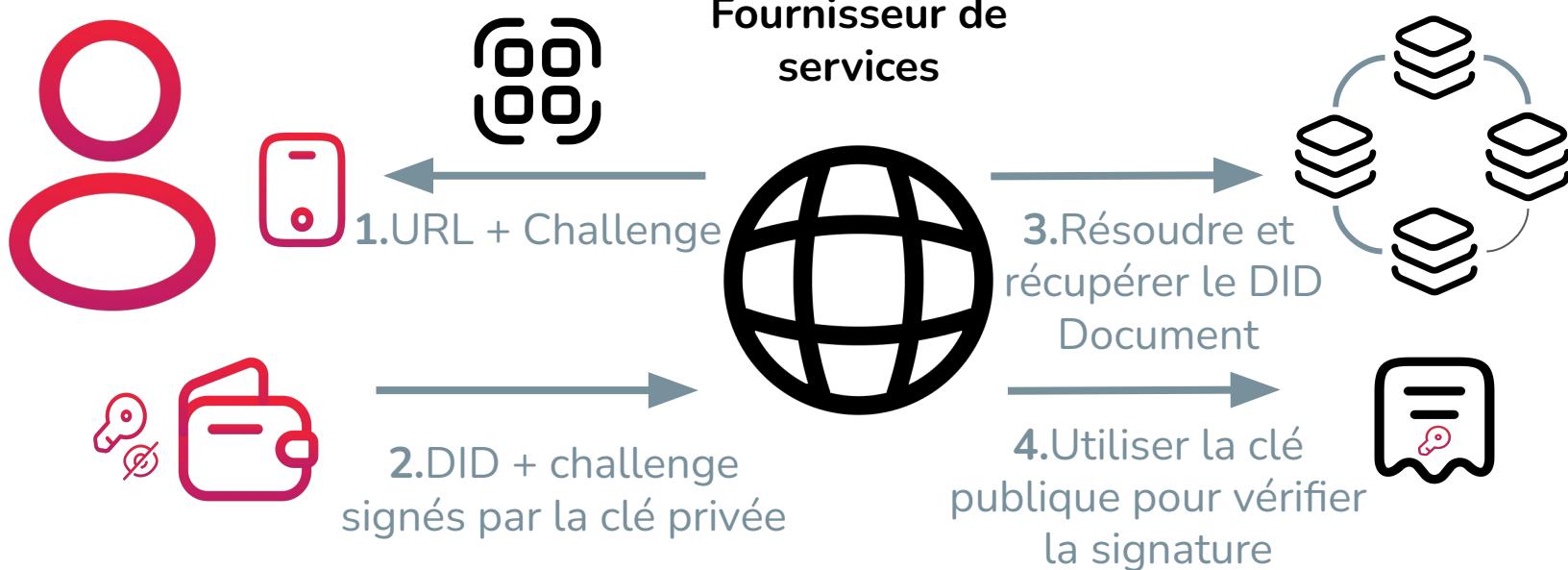
`did:ion:EiC1kZMDxPKqC9c-umQfT`

`kR8vvZ9JPh1_xLDI9Nfk38w5w`



Je veux utiliser mon DID. Prouver que  
c'est le mien et m'authentifier avec.

# DID I CONNECT ?



# AVANTAGE : UN PSEUDO COMME IDENTITÉ

L'identité numérique n'est pas non plus une solution miracle contre le traitement abusif des données personnelles.



Oups, certains services me demandent  
de prouver que je suis majeur !



## CHAPITRE 2

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





# PROUVER SON IDENTITÉ

Attester si on est majeur d'où la nécessité de VC.



# CECI N'EST PAS UNE IDENTITÉ



# CECI EST UNE COLLECTION DE DÉCLARATIONS À VOTRE SUJET



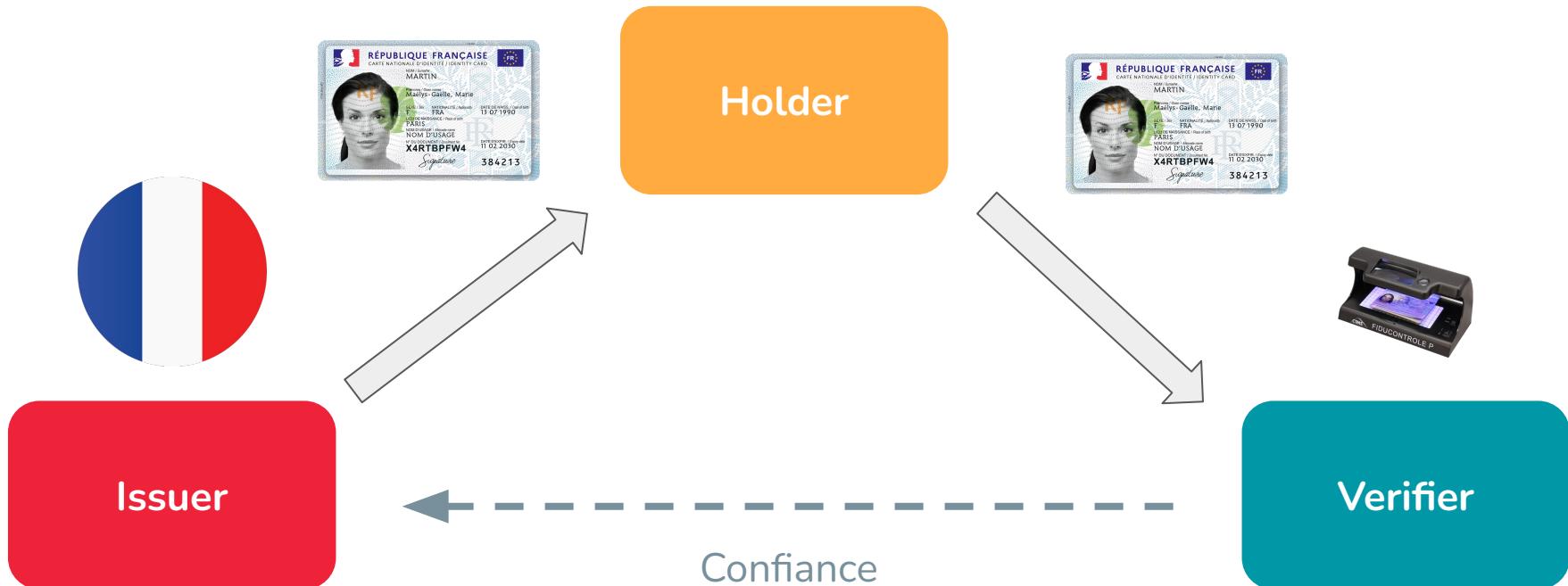
# CECI EST UNE COLLECTION DE DÉCLARATIONS À VOTRE SUJET

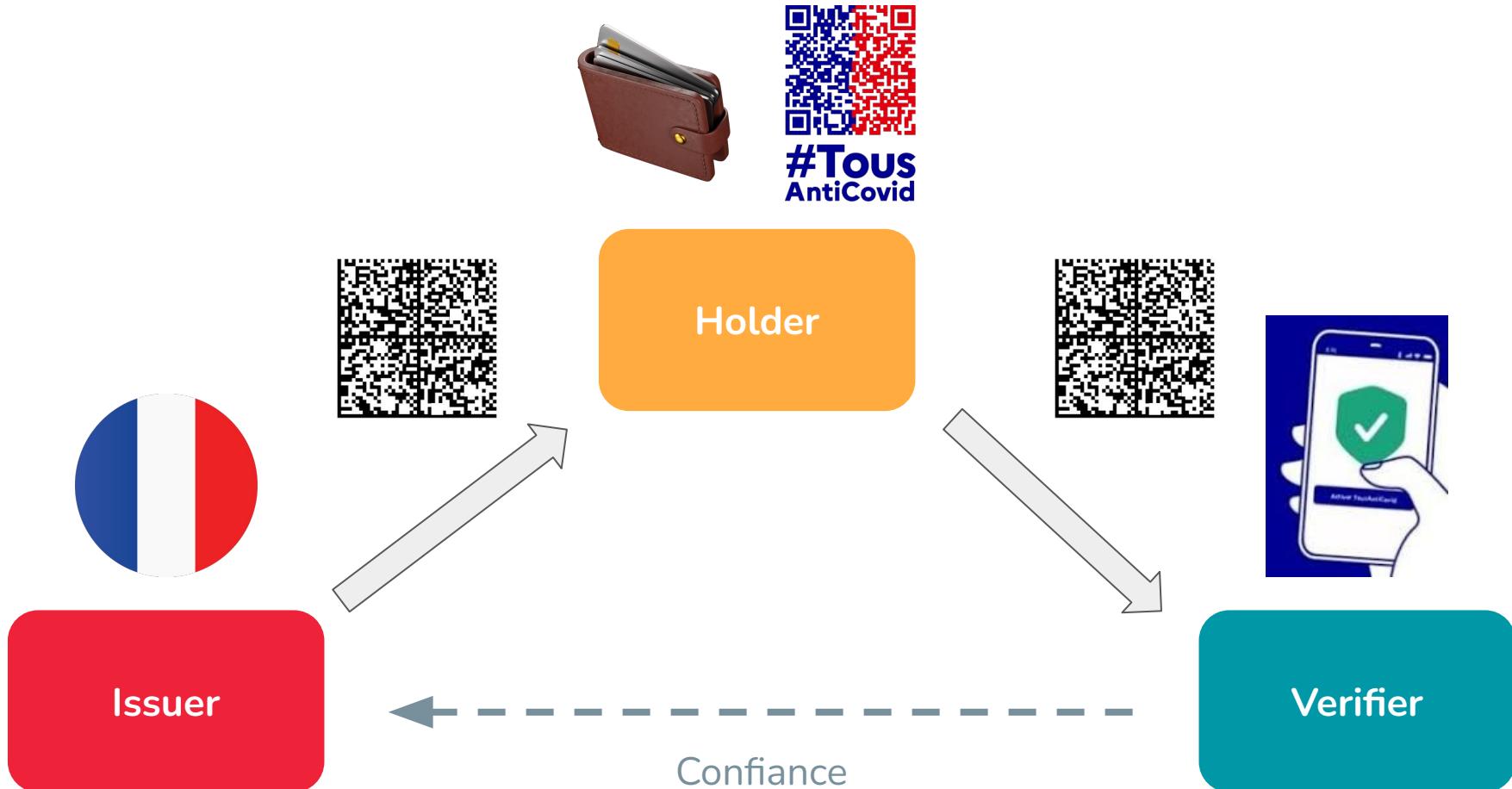


... DONT L'ÉMETTEUR (ETAT FRANCAIS) EST VÉRIFIABLE



## THE TRUST TRIANGLE



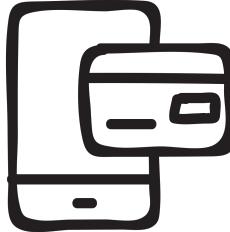
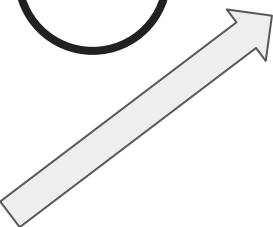


L'état français dit que  
Mme Martin a 31 ans



Issuer

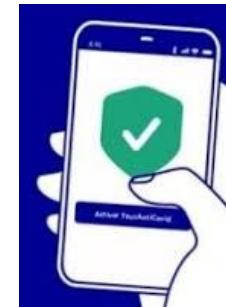
VC



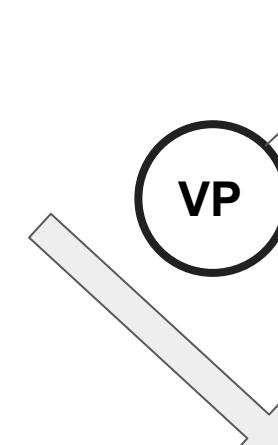
Holder

L'état français dit que  
Mme Martin a 31 ans,  
Je suis Mme Martin

VP



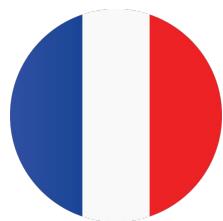
Verifier



Confiance

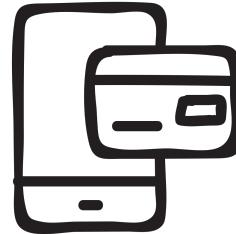
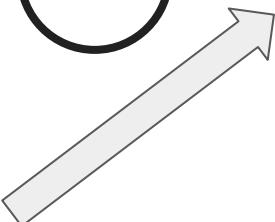


L'état français dit que  
Mme Martin a 31 ans



Issuer

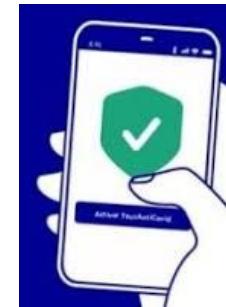
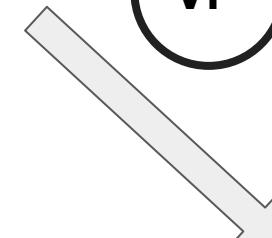
VC



Holder

L'état français dit que  
Mme Martin est majeure  
(Zero Knowledge Proof),  
Je suis Mme Martin

VP



Verifier



Confiance



# LES VERIFIABLE CREDENTIALS

Les **justificatifs vérifiables** sont des **objets** de données constitués de **revendications** formulées par l'émetteur attestant des informations sur un sujet. Ces revendications sont identifiées par un **schéma** et incluent en général les déclarations, l'émetteur et le sujet.

Le DID de l'émetteur peut être utilisé pour créer une **signature numérique** en guise de preuve attestant de ces informations.

<https://verifiablecredential.io/playground?tab=samples>



## VERIFIABLE CREDENTIAL

Métadonnées

Déclarations

Vérification

## VERIFIABLE CREDENTIAL

Métadonnées

```
{  
  "@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": "eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2Us...",  
    "proofPurpose": "assertionMethod",  
    "verificationMethod":  
      "https://example.edu/issuers/565049/keys/1"  
  }  
}
```

## VERIFIABLE CREDENTIAL

### Déclarations

```
{  
    "@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": "eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2Us...",  
        "proofPurpose": "assertionMethod",  
        "verificationMethod":  
            "https://example.edu/issuers/565049/keys/1"  
    }  
}
```

## 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": "eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2Us...",  
        "proofPurpose": "assertionMethod",  
        "verificationMethod":  
            "https://example.edu/issuers/565049/keys/1"  
    }  
}
```

Vérification

**Je suis coquette! Je ne veux pas  
divulguer ma date de naissance et  
donc mon age.**



## VERIFIABLE PRESENTATION

Métadonnées

## VERIFIABLE CREDENTIAL

Métadonnées

Déclarations

Vérification

Vérification

## VERIFIABLE PRESENTATION

Métadonnées

```
{  
  "@context": [ ... ],  
  "id": "http://example.edu/credentials/1872",  
  "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 PRESENTATION

VERIFIABLE  
CREDENTIAL(S)

```
{  
  "@context": [ ... ],  
  "id": "http://example.edu/credentials/1872",  
  "type": "VerifiablePresentation",  
  "verifiableCredential": [  
    { ... },  
    { ... }  
],  
  "proof": {  
    "type": "RsaSignature2018",  
    "created": "2018-09-14T21:19:10Z",  
    "proofPurpose": "authentication",  

```



## VERIFIABLE PRESENTATION

```
{  
    "@context": [ ... ],  
    "id": "http://example.edu/credentials/1872",  
    "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..."  
    }  
}
```

Vérification

# PRÉCISION : UNE VP PEUT CONTENIR PLUSIEURS VC



# PRÉCISION : UNE VP PEUT CONTENIR PLUSIEURS VC



... ET C'EST LE HOLDER QUI CHOISIT LES VC QU'IL INCLUT DANS LA VP

**Précision : DID et VC sont  
indépendants**

**L'utilisation de DID n'implique pas  
obligatoirement l'utilisation de Verifiable  
Credentials**

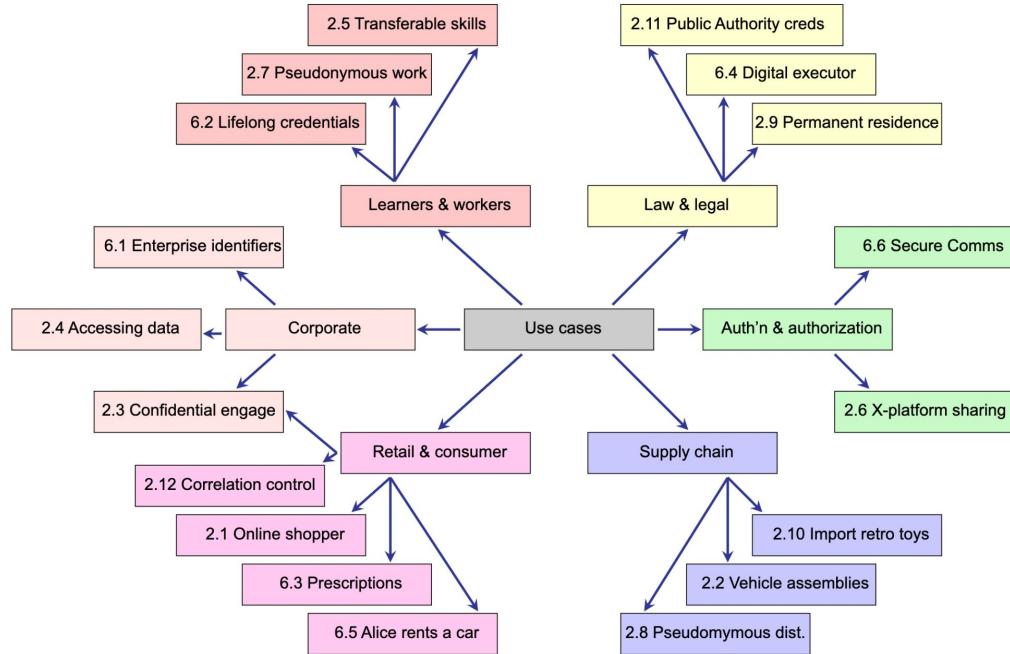
**L'utilisation de Verifiable Credentials n'implique  
pas obligatoirement l'utilisation de DID**



## CHAPITRE 3

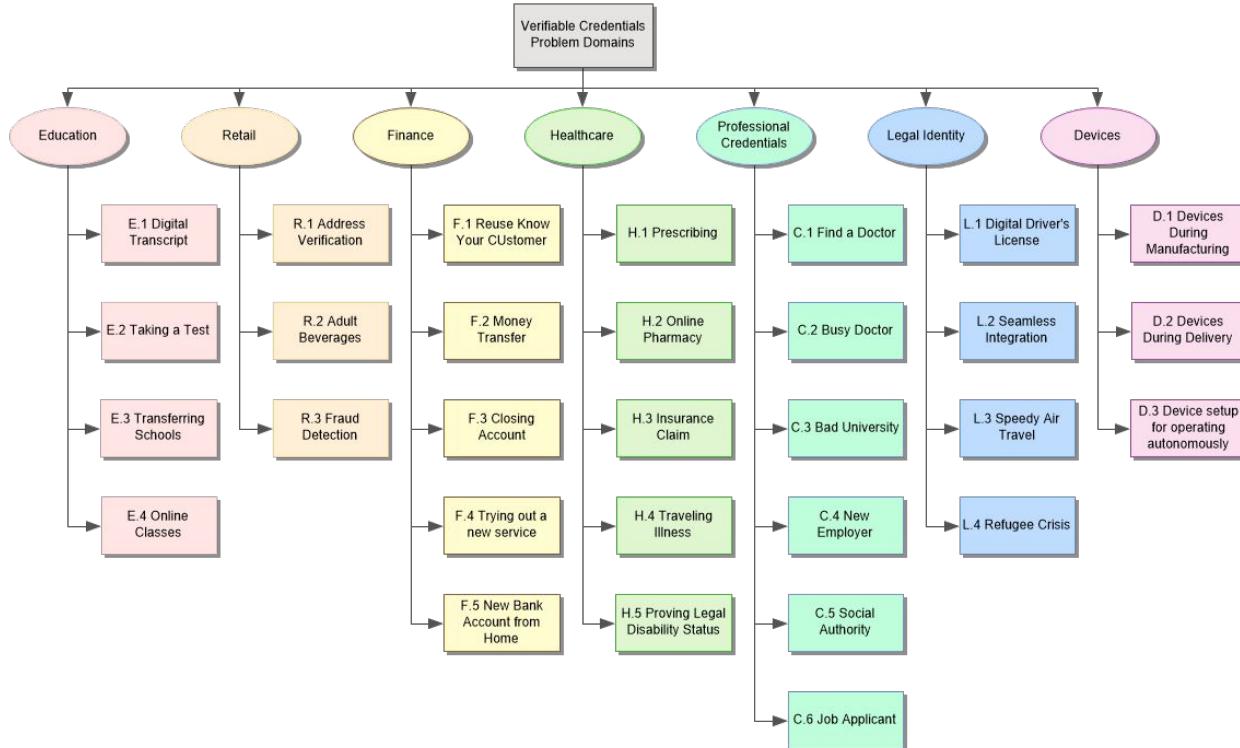
### Usages dans la vie courante

# DANS TOUS LES DOMAINES



<https://www.w3.org/TR/did-use-cases/>

# DANS TOUS LES DOMAINES

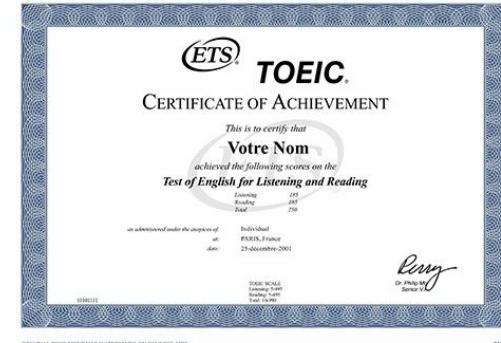
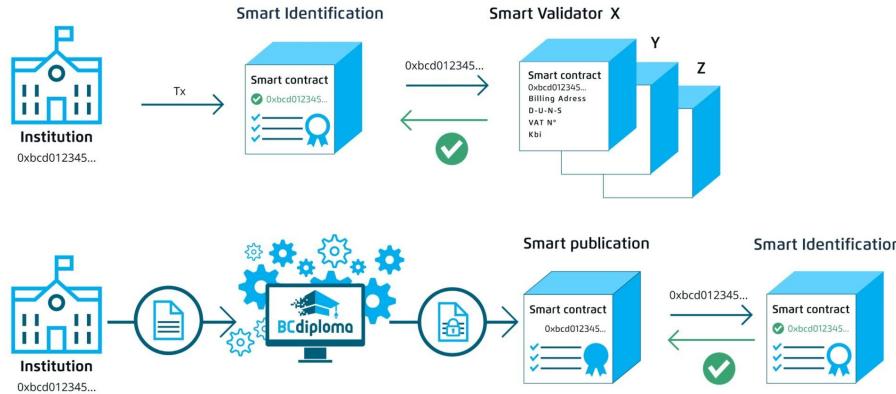


<https://www.w3.org/TR/vc-use-cases>

# BCDIPLOMA

BCdiploma est disponible en production sur Ethereum, Binance Smart Chain et bientôt sur EBSI. L'interopérabilité est l'une des clés de la généralisation de l'utilisation des blockchain digital credentials.

“Les employeurs peuvent vérifier les attestations certifiées en cliquant sur un lien que l'étudiant peut facilement partager”



# 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** (Electronic IDentification And Trust Services) 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.

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





# 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 QUELQUE CHOSE...

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



## CHAPITRE 4

### Maturité



## TECHNOLOGY RADAR

ADOPT

TRIAL

ASSESS

HOLD

Decentralized identity



Verifiable credentials

# LES ACTEURS DU MONDE DE L'IDENTITÉ DÉCENTRALISÉE

e·ernym



RSA®

sovrin



HYPERLEDGER

W3C®

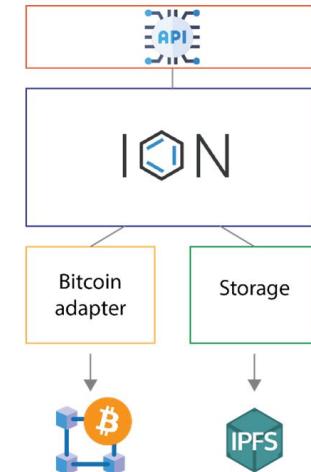
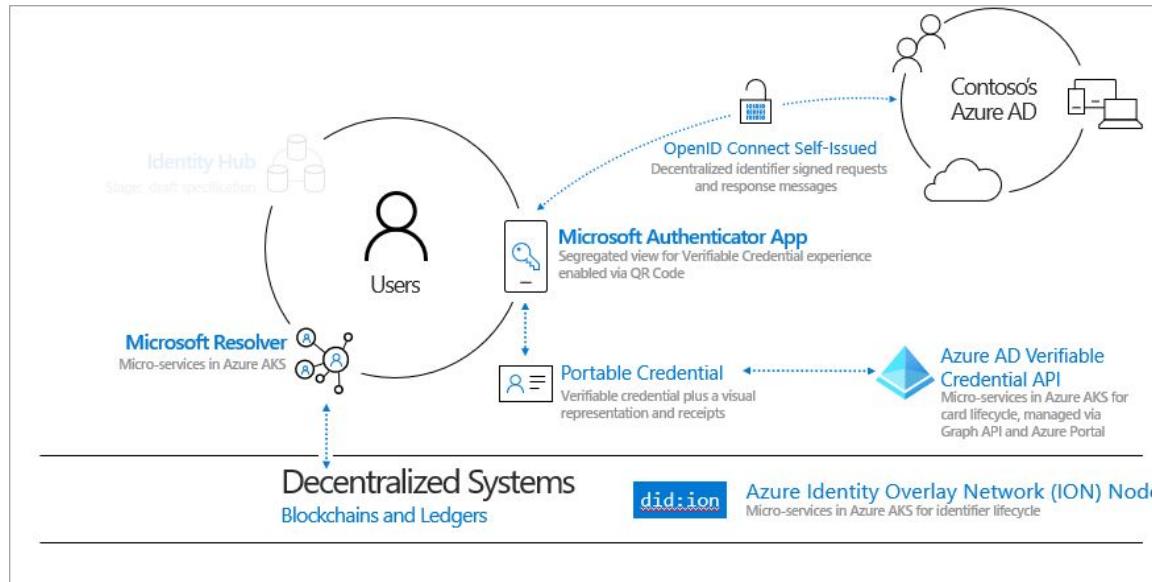


SECURE KEY

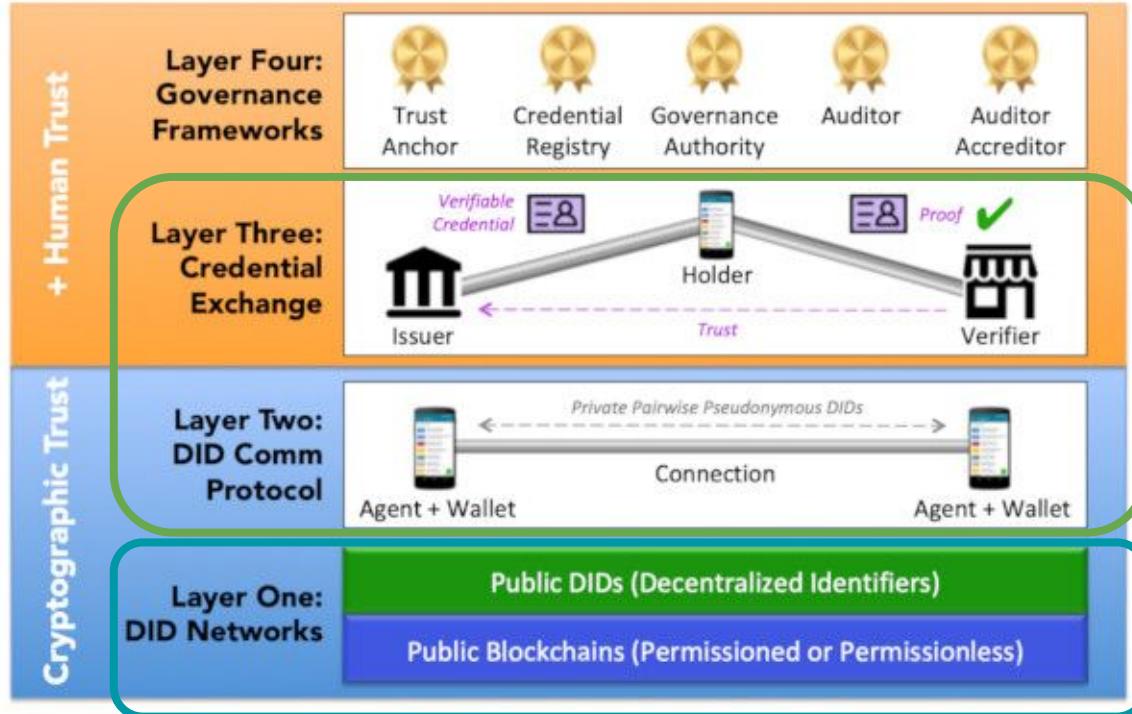


# AZURE AD VERIFIABLE CREDENTIALS

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**



## DEMO

↑

⊕

\*|

~

○

\*

(⊗)

⊖

</>

○

\*

(⊗)

⊖

</>

↑

⊕

\*|

~

</>

⊖

↑

⊕

\*|

~

(⊗)

⊖

</>

did:github

<https://github.com/decentralized-identity/github-did>

<https://github.com/awattez/ghdid>

did-twit ?

[https://github.com/did-twit/did-twit/  
blob/master/spec/index.md](https://github.com/did-twit/did-twit/blob/master/spec/index.md)

# DES QUESTIONS ?



<https://github.com/awattez/ghdid>

