Digital Identity or:

How I Learned to Stop Worrying and Love Web3

An introduction to Self-Sovereign Identity, Decentralized Identifiers & Verifiable Credentials

Thomas Carr
Consultant, Software Developer
CGI Federal, Emerging Technologies Practice
June 9, 2023

"On the Internet, nobody knows you're a dog."

Self-Identification

- University of Tennessee (B.A. American Studies, 2015)
- <Misc> (2015-2020)
- Tech Talent South Bootcamp (2020)
- Developer -> Senior Developer, MWW On Demand (2020-2022)
- Interim CIO, Manual Woodworkers & Weavers (2022)
- Consultant & Software Developer, Emerging Technologies, CGI Federal (Present)

A short defense of “Web3”

- Originally coined by Gavin Wood (Ethereum co-founder)
  - Advocates for reorganizing web applications around decentralizing protocols, blockchain technologies, and token-based economics
- Distributed ledger technologies are useful for some things, but are largely overhyped
- Decentralized finance (Defi) is noise. You can safely ignore it.
- “Web3” is posturing
  - Marketing term driven by startups, consultants, and VC/PE firms to sell products & build hype.
  - “Cloud”

Agenda

1

What is digital identity?

2

Why is digital identity important?

3

How can we improve digital identity in web apps?

What is digital identity?

“Digital identity refers to the information utilized by computer systems to represent external identities, including a person, organization, application, or device”

Digital Identity

Must Be

- Machine-readable
- Verifiable
- Secure

Should Be

- Interoperable
- Privacy-preserving
- Context-dependent

Digital Identity Categories

Human

- One to one relationship with a human
- Source of trust comes from government organizations
- Physical identity like Driver’s License & Passport
- Digital identity like external verifications, biometrics, captchas, forms

Organization

- One to one relationship with a business or group of people
- Source of trust comes from government organizations
- Physical identity like offices, stores & employees
- Digital identity like brands & IT systems

Digital Identity Categories

Software Bots

- Software-powered automation, often working on behalf of an organization or a human
- Source of trust comes from code and the organization running it
- Physical identity comes from hardware
- Digital identity comes from IP addresses, Certificate Authorities, PKI

AI Agents

- Generative AI accomplishing tasks on the public internet
- Source of trust comes from underlying algorithms and training data
- Physical identity comes from hardware
- Digital identity has characteristics of both software and people

Enterprise Identity

- Active Directory Info
  - Username
  - Emails
  - Passwords
  - Title
  - Role
  - Team
  - Physical/Digital Badge
  - Devices
- Employment Eligibility (I-9)
- Background Check
- Certifications
- Subject Matter Expertise

Social Identity

- Auth Identifiers
  - Username
  - Emails
  - Passwords
  - Device/MFA
- Profile Info
  - Name
  - Age/Birthday
- Relationship Graph
  - Friends, Follows & Connections
- Content
  - Posts, tweets, etc.
- Generic tracking (cookies)

Why is digital identity important?

Hint: *It's about user experience*

"On the Internet, nobody knows you're a dog."

Thomas Carr

htcarr3 · he/him

Software Developer / IT Consultant

Edit profile

16 followers · **87** following

@CGIFederalInc, @protocollar, @verdafy

Knoxville, TN

01:39 (UTC -04:00)

https://htcarr.com/

in/htcarr3

@htcarr3

Popular repositories

devise-passkeys — Public

Forked from ruby-passkeys/devise-passkeys

Devise extension to use passkeys instead of passwords

Ruby ☆ 1

tle_dataset — Public

tle_dataset

image-stego — Public

Forked from dennis-tra/image-stego

Steganography-based image integrity - Merkle tree nodes embedded into image chunks so that each chunk's integrity can be verified on its own.

Go

120 contributions in the last year

Jun Jul Aug Sep Oct Nov

Heroku account

Create apps, connect databases and add-on services, and collaborate on your apps.

Your app platform

A platform for apps, with app management & instant scaling, for development and production.

Deploy now

Go from code to running app in minutes. Deploy, scale, and deliver your app to the world.

First name *

First name

Last name *

Last name

Email address *

Email address

Company name

Company name

Role *

Role

Country/Region *

Country/Region

Primary development language *

Select a language

I'm not a robot

reCAPTCHA
Privacy - Terms

CREATE AN ACCOUNT

HEY

Welcome back. Let's sign in.

Enter your email address

And your password

Sign in

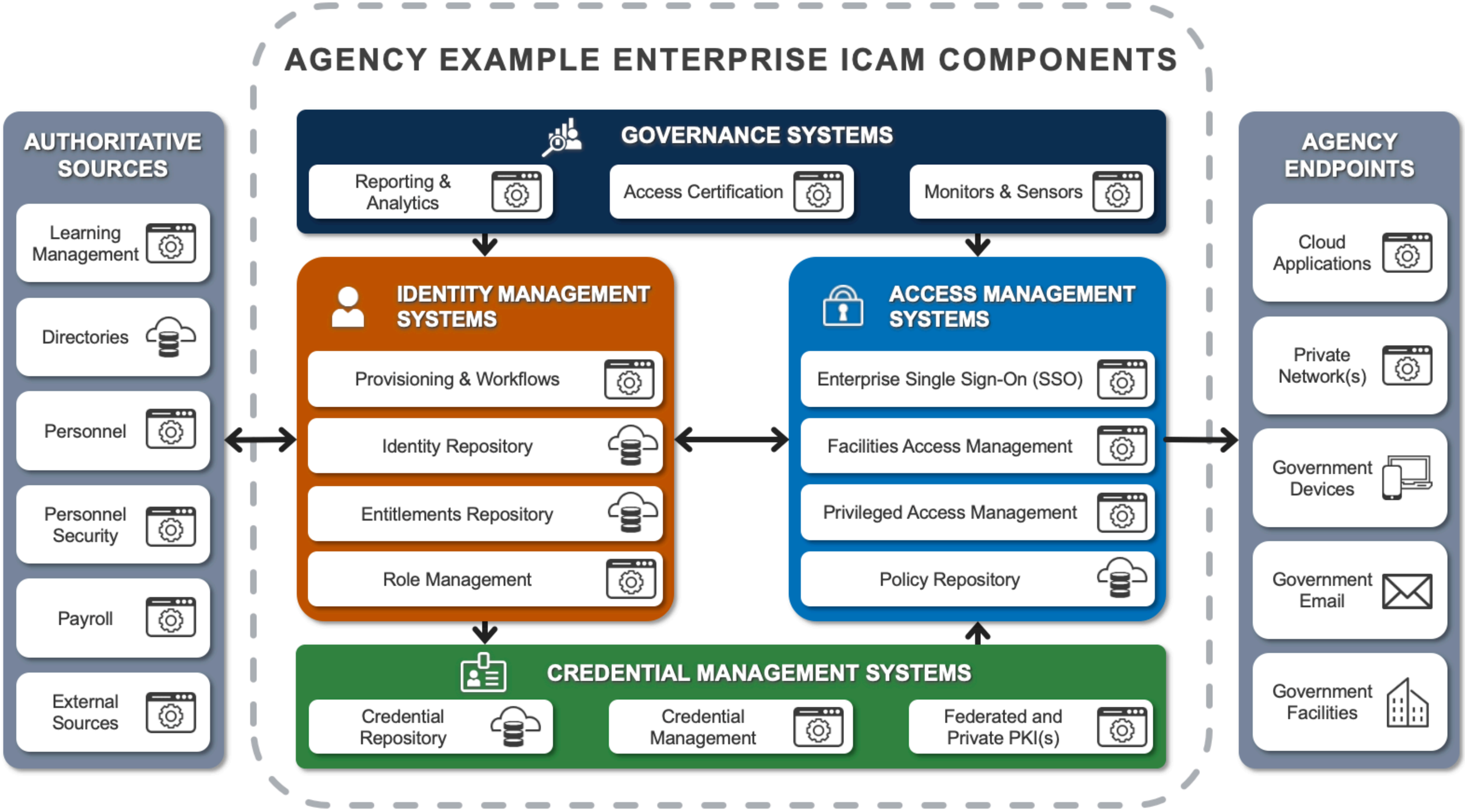
Forgot your password?

We'll help you reset it so you can get back in.

Log in

Continue with Google

Continue with Apple


AGENCY EXAMPLE ENTERPRISE ICAM COMPONENTS
AUTHORITATIVE SOURCES
Learning Management
Directories
Personnel
Personnel Security
Payroll
External Sources
GOVERNANCE SYSTEMS
Reporting & Analytics
Access Certification
Monitors & Sensors
IDENTITY MANAGEMENT SYSTEMS
Provisioning & Workflows
Identity Repository
Entitlements Repository
Role Management
ACCESS MANAGEMENT SYSTEMS
Enterprise Single Sign-On (SSO)
Facilities Access Management
Privileged Access Management
Policy Repository
CREDENTIAL MANAGEMENT SYSTEMS
Credential Repository
Credential Management
Federated and Private PKI(s)
AGENCY ENDPOINTS
Cloud Applications
Private Network(s)
Government Devices
Government Email
Government Facilities

Unique Identifiers

- Emails
- Devices
- Usernames
- UUIDs
- Database IDs

```
37  create_table "users", force: :cascade do |t|
38    t.string   "email",                  default: "", null: false
39    t.string   "encrypted_password",     default: "", null: false
40    t.string   "reset_password_token"
41    t.datetime "reset_password_sent_at"
42    t.datetime "remember_created_at"
43    t.integer  "sign_in_count",          default: 0,  null: false
44    t.datetime "current_sign_in_at"
45    t.datetime "last_sign_in_at"
46    t.string   "current_sign_in_ip"
47    t.string   "last_sign_in_ip"
48    t.datetime "created_at",                          null: false
49    t.datetime "updated_at",                          null: false
50  end
```

Top stories

Fox News

Massive free VPN data breach exposes 360M records

15 hours ago

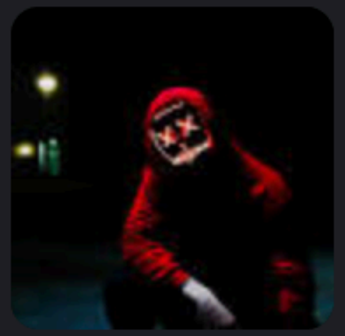
Dark Reading

2.5M Impacted by Enzo Biochem Data Leak After Ransomware Attack

8 hours ago

Bleeping Computer

Clop ransomware claims responsibility for MOVEit extortion attacks



8 hours ago

Financial Times

British Airways, Boots and BBC among companies hit by cyber security attack

11 hours ago

More news →

How can we improve digital identity in web apps?

Unlocking self-sovereign identity for users with Decentralized Identifiers, Verifiable Credentials, and other related protocols.

Self-Sovereign Identity

- Gives individuals control over the information they use to prove who they are to websites
- Often involves a digital credential exchange
- The verifier can verify that the credentials came from an issuer that they trust
- The verifier’s trust in the issuer is transferred to the credential holder

Verifiable Credentials

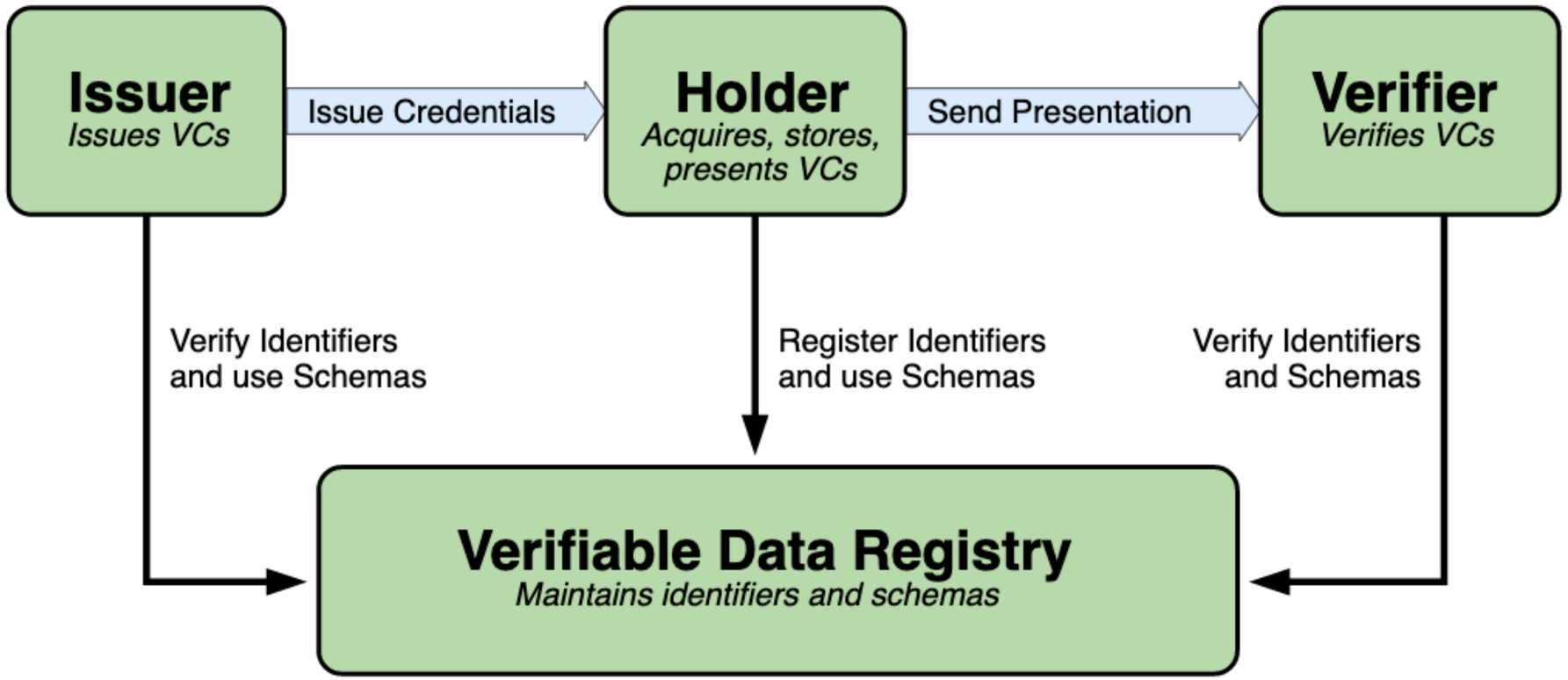
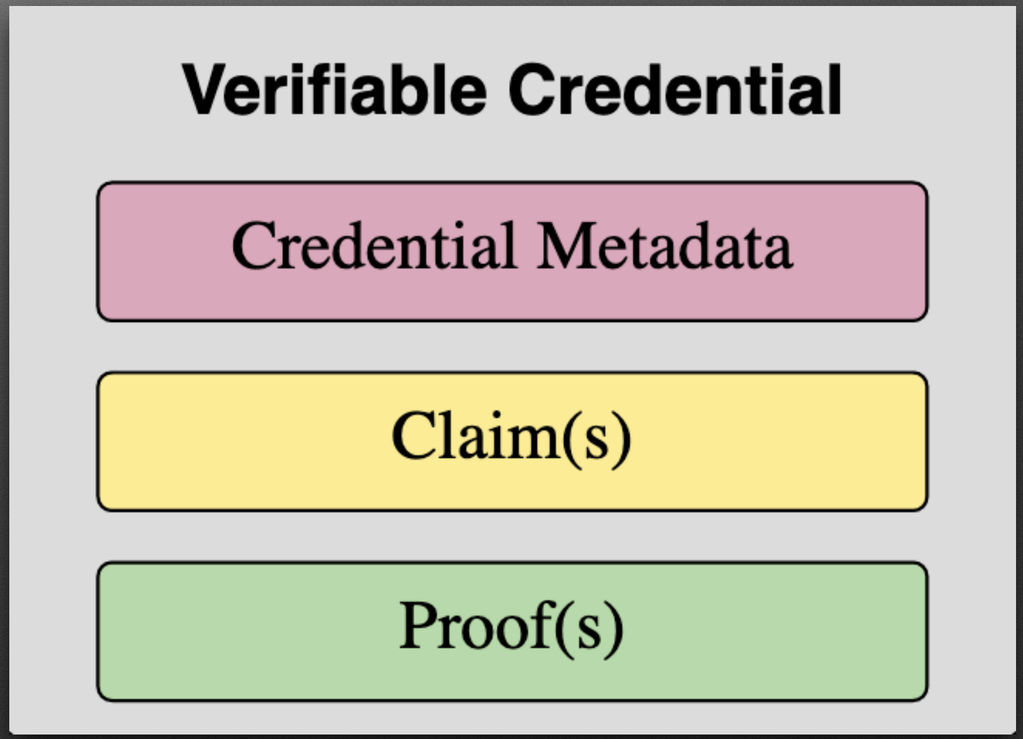


Figure 1 The roles and information flows forming the basis for this specification.

Verifiable Credentials (W3C)

- An open specification
- A set of one or more claims by an issuer
- Tamper-evident
- Authorship is cryptographically verifiable
- Context and linked data can be provided
- Selective disclosure and Zero Knowledge Proofs are possible



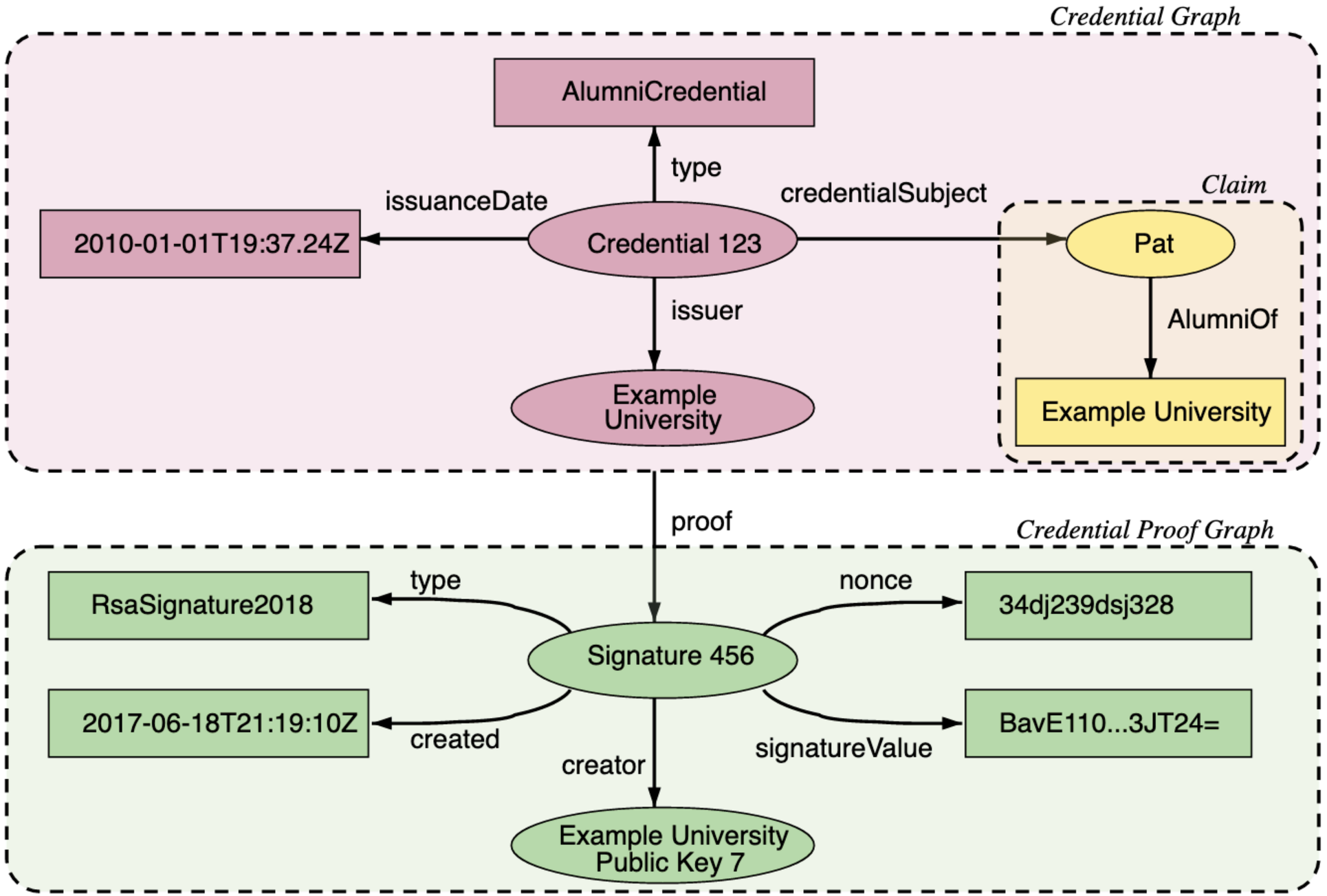


Figure 6 Information graphs associated with a basic verifiable credential.

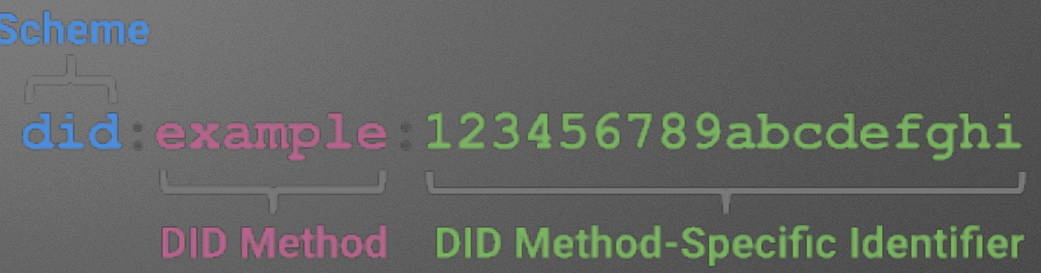
JSON-LD

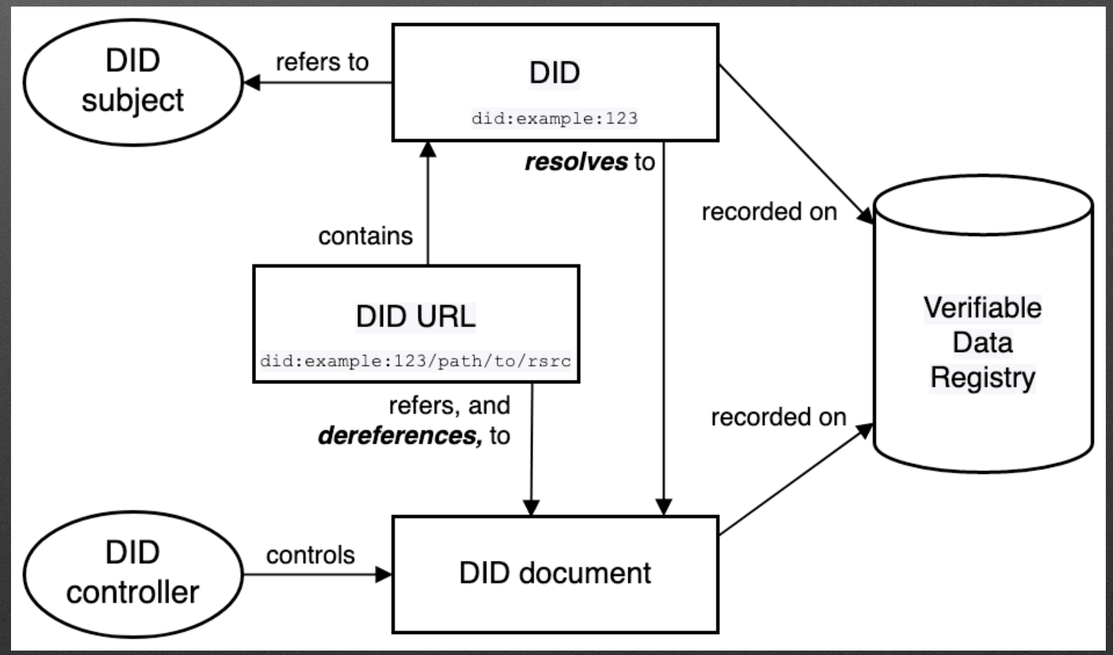
```
{
  // set the context, which establishes the special terms we will be using
  // such as 'issuer' and 'alumniOf'.
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  // specify the identifier for the credential
  "id": "http://example.edu/credentials/1872",
  // the credential types, which declare what data to expect in the credential
  "type": ["VerifiableCredential", "AlumniCredential"],
  // the entity that issued the credential
  "issuer": "https://example.edu/issuers/565049",
  // when the credential was issued
  "issuanceDate": "2010-01-01T19:23:24Z",
  // claims about the subjects of the credential
  "credentialSubject": {
    // identifier for the only subject of the credential
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    // assertion about the only subject of the credential
    "alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
        "value": "Example University",
        "lang": "en"
      }, {
        "value": "Exemple d'Université",
        "lang": "fr"
      }]
    }
  },
```

```
  "alumniOf": {
    "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
    "name": [{
      "value": "Example University",
      "lang": "en"
    }, {
      "value": "Exemple d'Université",
      "lang": "fr"
    }]
  }
},
// digital proof that makes the credential tamper-evident
// see the NOTE at end of this section for more detail
"proof": {
  // the cryptographic signature suite that was used to generate the signature
  "type": "RsaSignature2018",
  // the date the signature was created
  "created": "2017-06-18T21:19:10Z",
  // purpose of this proof
  "proofPurpose": "assertionMethod",
  // the identifier of the public key that can verify the signature
  "verificationMethod": "https://example.edu/issuers/565049#key-1",
  // the digital signature value
  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
    sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc
    X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
    PAYuNzVBAh4vGHSrQyHUdBBPM"
}
```

Decentralized Identifiers (DIDs)

- Globally unique URI-like scheme
- Verifiable, persistent, and does not require a central registry
- Resolves (points) do a DID Document
- Did method specifies how to CRUD the DID Document






```
# Parse a did:web DID
did_string = 'did:web:identity.foundation'

did = DIDX(did_string)
=> #<DIDX::Web:0x000000010bb1ad30 @id="did:web:identity.foundation", @method="web",

# Resolve to a did:web's DID Document
did.document
=> #<DIDX::Document:0x000000010aa597d0 @assertion_method=nil, @authentication=nil,
```

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "did:example:123",
  "authentication": [
    {
      "id": "did:example:123#z6MkecaLyHuYWkayBDLw5ihndj3T1m6zKTGqau3A51G7RBf3",
      "type": "Ed25519VerificationKey2020", // external (property value)
      "controller": "did:example:123",
      "publicKeyMultibase": "zAKJP3f7BD6W4iWEQ9jwndVTCBq8ua2Utt8EEjJ6Vxsf"
    }
  ],
  "capabilityInvocation": [
    {
      "id": "did:example:123#z6MkhdmzFu659ZJ4XKj31vtEDmjvsi5yDZG5L7Caz63oP39k",
      "type": "Ed25519VerificationKey2020", // external (property value)
      "controller": "did:example:123",
      "publicKeyMultibase": "z4BWwfeqdp1obQptLLMvPNgBw48p7og1ie6Hf9p5nTpNN"
    }
  ],
  "capabilityDelegation": [
    {
      "id": "did:example:123#z6Mkw94ByR26zMSkNdCUi6FNRsWnc2DFEeDXyBGJ5KTzSWyi",
      "type": "Ed25519VerificationKey2020", // external (property value)
      "controller": "did:example:123",
      "publicKeyMultibase": "zHgo9PAmfeoxHG8Mn2XHXamxnnSwPpkyBHAMNF3VyXJCL"
    }
  ],
  "assertionMethod": [
    {
      "id": "did:example:123#z6MkiukuAuQAE8ozxvmahnQGzApvtW7KT5XXKfojjwbdEomY",
      "type": "Ed25519VerificationKey2020", // external (property value)
      "controller": "did:example:123",
      "publicKeyMultibase": "z5TVraf9itbKXrRvt2DSS95Gw4vqU3CHAdetoufdcKazA"
    }
  ]
}
```

Use Cases

- Cross-domain data exchanges
  - Digital Identity
  - Documents
  - Supply Chains
- Privacy-preserving identification over the internet
  - Human — Human
  - Human — Machine
  - Machine — Machine
- Verifiable data provenance
- Reusable background checks
- Personal data vaults
- Certifications
- Decentralized data catalog
- Digital marketplaces
- P2P Communication
- Zero Trust Architectures

verdafy.com

Verdafy

Ruby Gems for Decentralized Identifiers,

Verifiable Credentials & SSI protocols

Decentralized Identifiers

DIDX

Verifiable Data

Verda

verdafy.com/brr

Blue Ridge Ruby

Verifiable Credential Issuer and Verifier

GET Rubyist ID

VERIFY Rubyist ID

Digital Identity or:

How I Learned to Stop Worrying and Love Web3

An introduction to Self-Sovereign Identity, Decentralized Identifiers & Verifiable Credentials

@htcarr3
htcarr.com

Thomas Carr
Consultant, Software Developer
CGI Federal, Emerging Technologies Practice
June 9, 2023

"On the Internet, nobody knows you're a dog."