Lessons Learned: Implementing a Decentralized Identity Platform

Daniel McGrogan

Principal Distributed Systems Software Engineer

Workday

Overview

Act 1

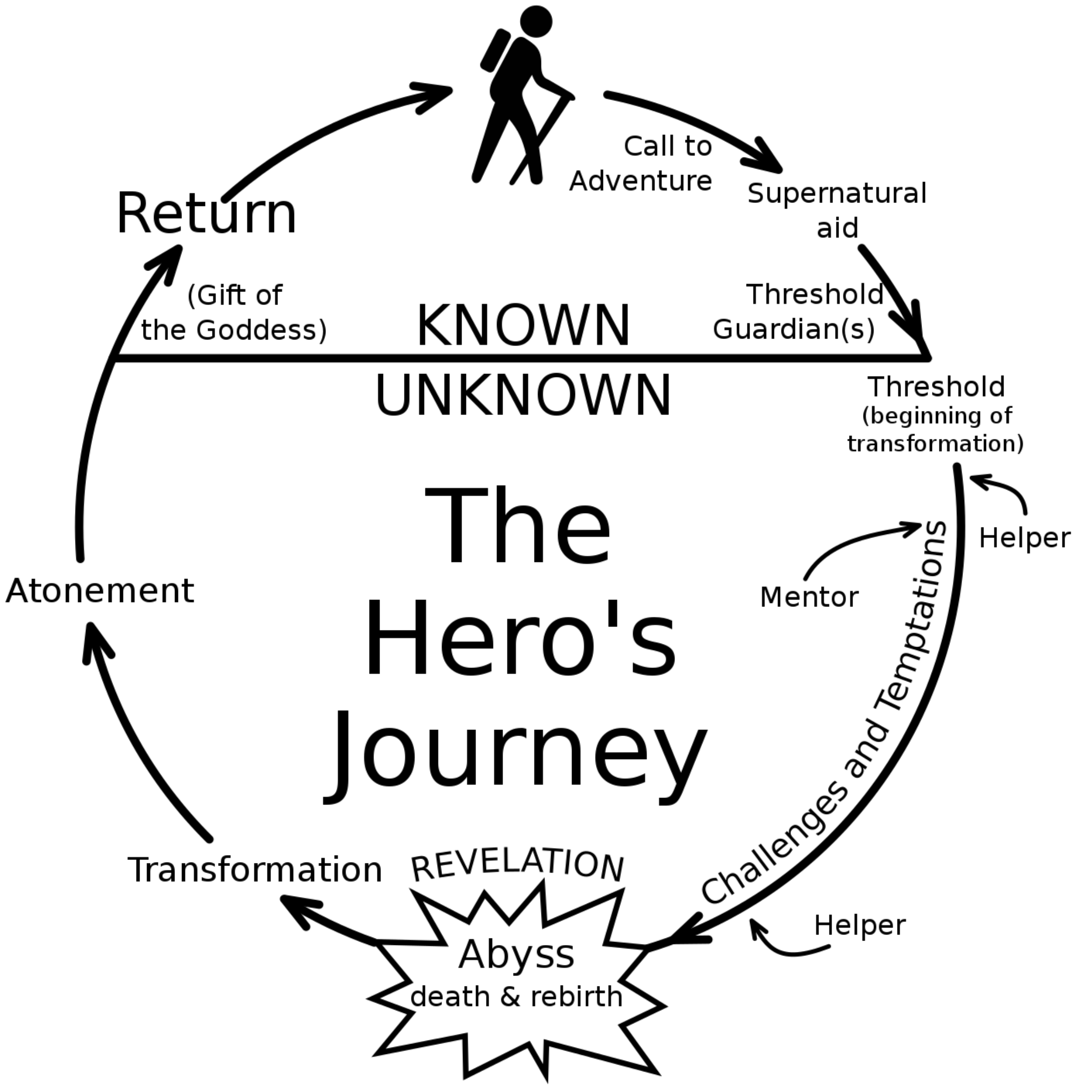
- Introduction
- What We Built

Act 2

- Lessons
- What We Built Next

Act 3

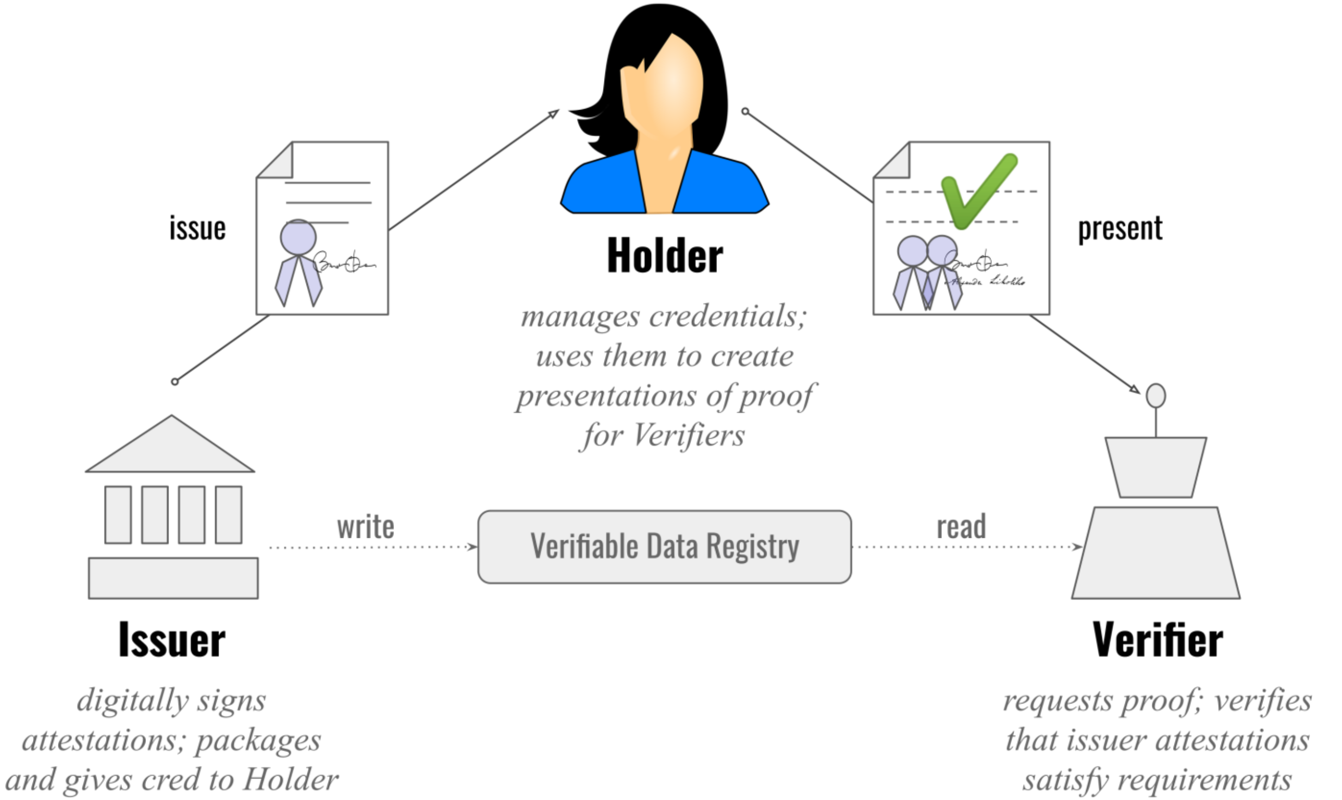
- Future



Act 1:
Call to Adventure

Verifiable Credentials
&
Distributed Identity

Actors



issue

Holder

manages credentials; uses them to create presentations of proof for Verifiers

present

Issuer

digitally signs attestations; packages and gives cred to Holder

write

Verifiable Data Registry

read

Verifier

requests proof; verifies that issuer attestations satisfy requirements

https://en.wikipedia.org/wiki/Verifiable_credentials

Decentralized Digital Identity

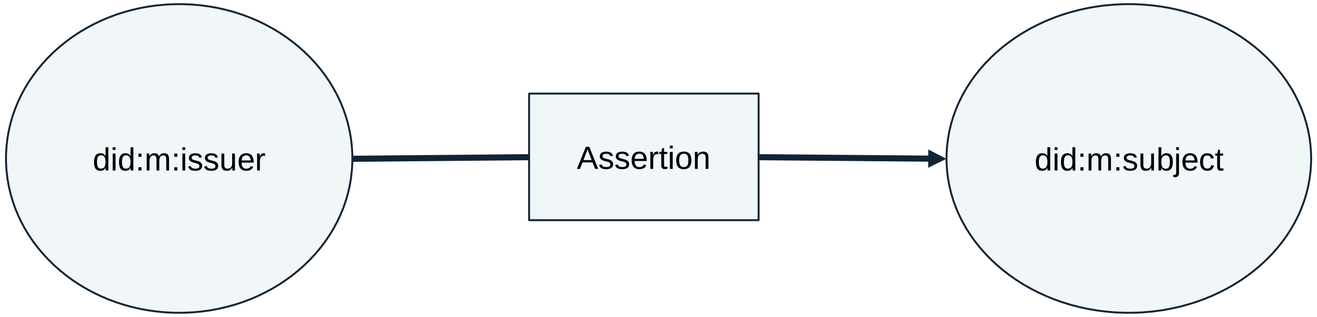
Decentralized Identifier (DID)

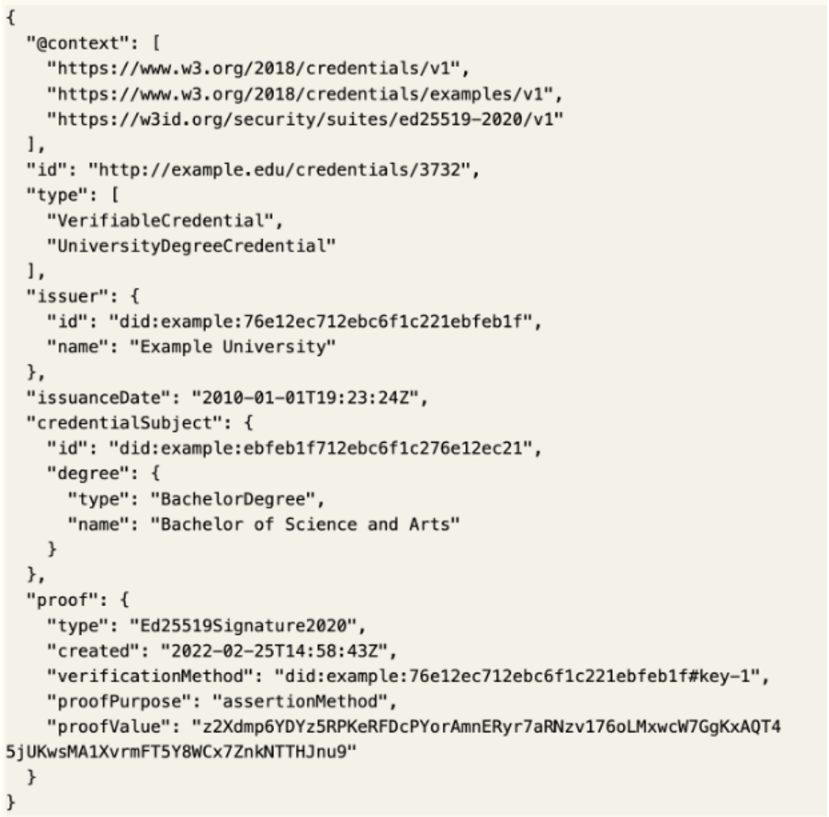
- PKI Mechanism
- Control of the ID without centralised permission
- https://www.w3.org/TR/did-core

Verifiable Credentials (VC)

- Cryptographically verifiable
- Assertion about a Subject made by the Issuer (signer)
- https://www.w3.org/TR/vc-data-model

What are Verifiable Credentials?





```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "http://example.edu/credentials/3732",
  "type": [
    "VerifiableCredential",
    "UniversityDegreeCredential"
  ],
  "issuer": {
    "id": "did:example:76e12ec712ebc6f1c221ebfeb1f",
    "name": "Example University"
  },
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-02-25T14:58:43Z",
    "verificationMethod": "did:example:76e12ec712ebc6f1c221ebfeb1f#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z2Xdmp6YDYz5RPKeRFDcPYorAmnERyr7aRNzv176oLMxwcW7GgKxAQT4
5jUKwsMA1XvrmFT5Y8WCx7ZnkNTTHJnu9"
  }
}
```

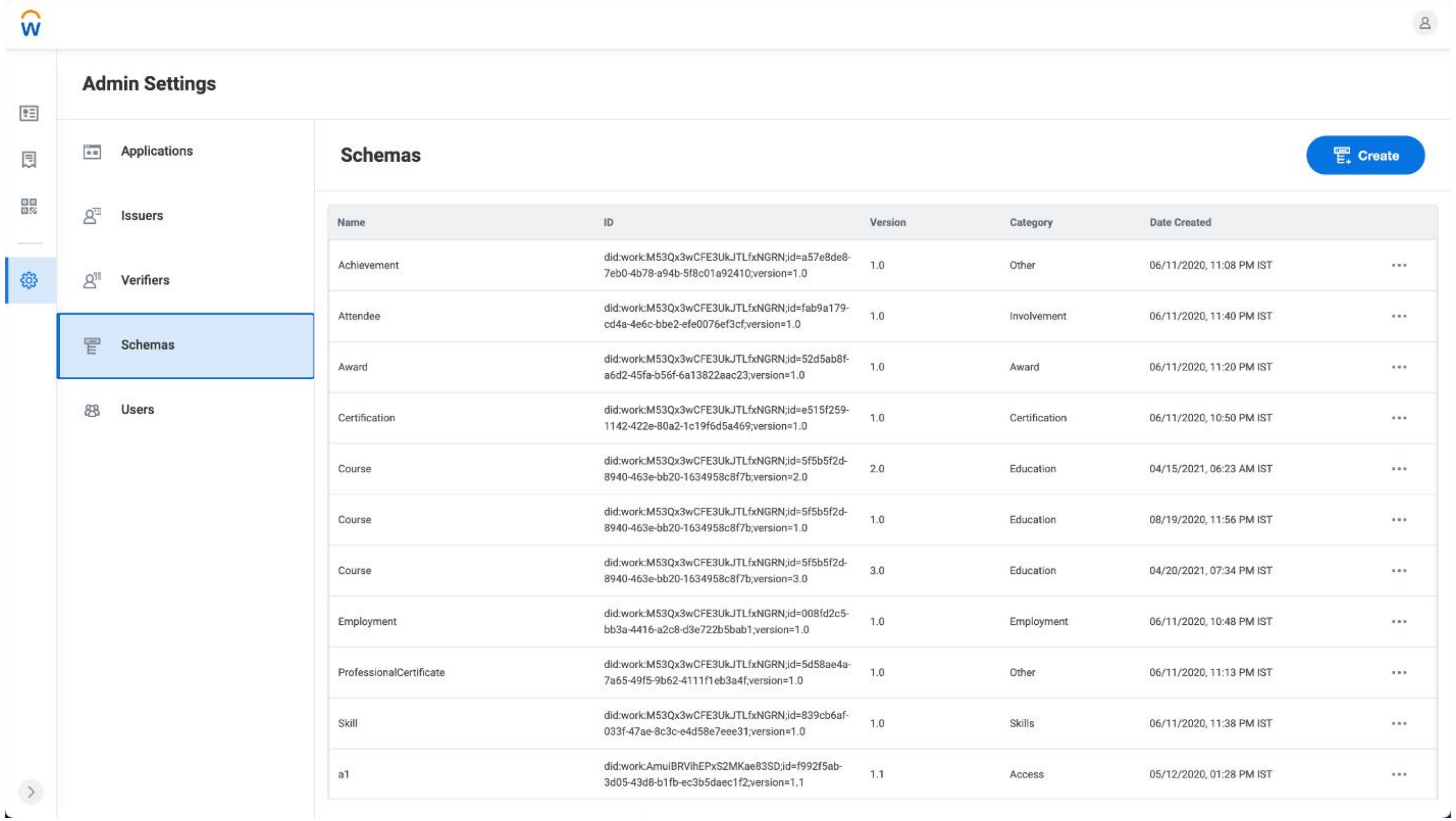
What We Built

Credentialing SAAS & Wallet

Solution for …

- Registering Issuer and Verifier DIDs
- Defining VC schemas
- Requesting VCs from users
- Issuing VCs
- Revoking VC
- Mobile Wallets for End Users
  - iOS
  - Android

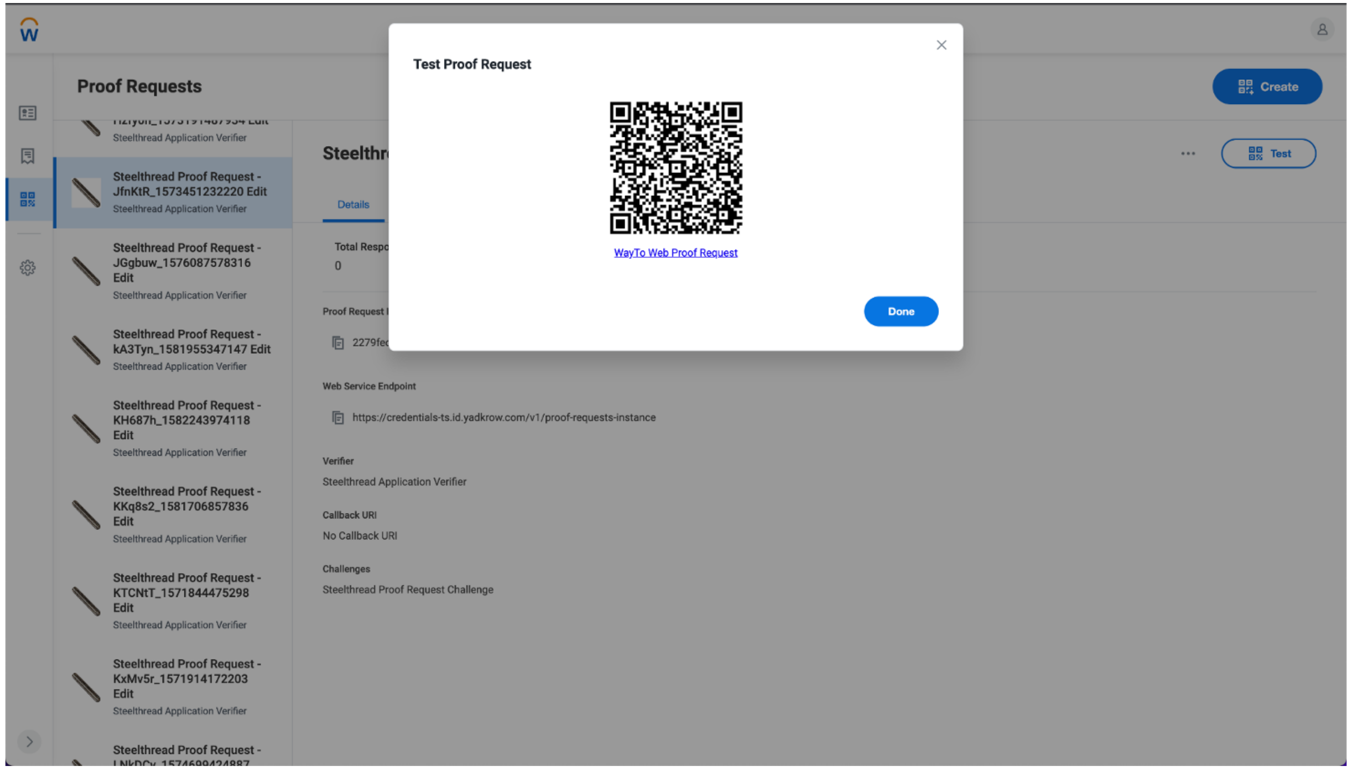
Define and Issue VC



Schemas

Name	ID	Version	Category	Date Created
Achievement	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=a57e8de8-7eb0-4b78-a94b-5f8c01a92410;version=1.0	1.0	Other	06/11/2020, 11:08 PM IST
Attendee	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=fab9a179-cd4a-4e6c-bbe2-efe0076ef3cf;version=1.0	1.0	Involvement	06/11/2020, 11:40 PM IST
Award	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=52d5ab8f-a6d2-45fa-b56f-6a13822aac23;version=1.0	1.0	Award	06/11/2020, 11:20 PM IST
Certification	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=e515f259-1142-422e-80a2-1c19f6d5a469;version=1.0	1.0	Certification	06/11/2020, 10:50 PM IST
Course	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=5f5b5f2d-8940-463e-bb20-1634958c8f7b;version=2.0	2.0	Education	04/15/2021, 06:23 AM IST
Course	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=5f5b5f2d-8940-463e-bb20-1634958c8f7b;version=1.0	1.0	Education	08/19/2020, 11:56 PM IST
Course	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=5f5b5f2d-8940-463e-bb20-1634958c8f7b;version=3.0	3.0	Education	04/20/2021, 07:34 PM IST
Employment	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=008fd2c5-bb3a-4416-a2c8-d3e722b5bab1;version=1.0	1.0	Employment	06/11/2020, 10:48 PM IST
ProfessionalCertificate	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=5d58ae4a-7a65-49f5-9b62-4111f1eb3a4f;version=1.0	1.0	Other	06/11/2020, 11:13 PM IST
Skill	did:work:M53Qx3wCFE3UkJTLfxNGRN;id=839cb6af-033f-47ae-8c3c-e4d58e7eee31;version=1.0	1.0	Skills	06/11/2020, 11:38 PM IST
a1	did:work:AmuiBRVihEPxS2MKae83SD;id=f992f5ab-3d05-43d8-b1fb-ec3b5daec1f2;version=1.1	1.1	Access	05/12/2020, 01:28 PM IST

Request a VC



Proof Requests

hZlyun_1573191487934 Edit
Steelthread Application Verifier

Steelthread Proof Request - JfnKtR_1573451232220 Edit
Steelthread Application Verifier

Steelthread Proof Request - JGgbuw_1576087578316 Edit
Steelthread Application Verifier

Steelthread Proof Request - kA3Tyn_1581955347147 Edit
Steelthread Application Verifier

Steelthread Proof Request - KH687h_1582243974118 Edit
Steelthread Application Verifier

Steelthread Proof Request - KKq8s2_1581706857836 Edit
Steelthread Application Verifier

Steelthread Proof Request - KTCNtT_1571844475298 Edit
Steelthread Application Verifier

Steelthread Proof Request - KxMv5r_1571914172203 Edit
Steelthread Application Verifier

Steelthread Proof Request - LNkDCv_1574699424887

Steelthr

Total Respo
0

Proof Request I
2279fec

Web Service Endpoint
https://credentials-ts.id.yadkrow.com/v1/proof-requests-instance

Verifier
Steelthread Application Verifier

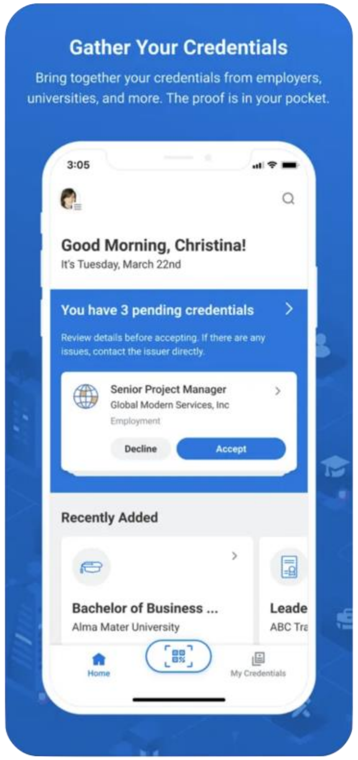
Callback URI
No Callback URI

Challenges
Steelthread Proof Request Challenge

Test Proof Request

WayTo Web Proof Request

User Wallet



Gather Your Credentials

Bring together your credentials from employers, universities, and more. The proof is in your pocket.

Good Morning, Christina!

It's Tuesday, March 22nd

You have 3 pending credentials

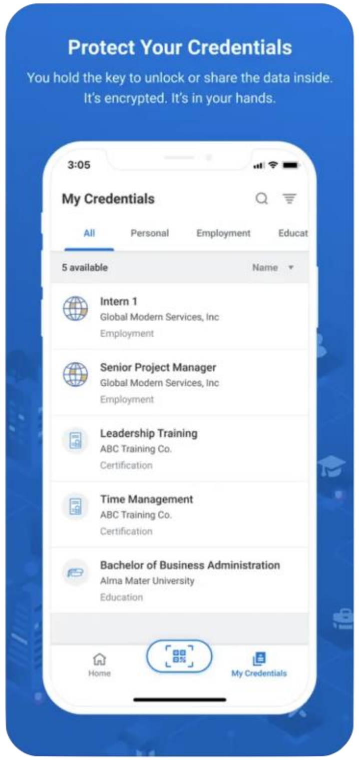
Review details before accepting. If there are any issues, contact the issuer directly.

Senior Project Manager
Global Modern Services, Inc
Employment

Recently Added

Bachelor of Business ...
Alma Mater University

Leade
ABC Tra



Protect Your Credentials

You hold the key to unlock or share the data inside. It's encrypted. It's in your hands.

My Credentials

5 available

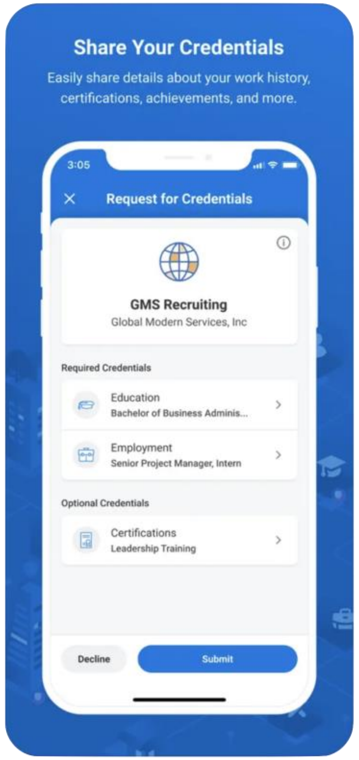
Intern 1
Global Modern Services, Inc
Employment

Senior Project Manager
Global Modern Services, Inc
Employment

Leadership Training
ABC Training Co.
Certification

Time Management
ABC Training Co.
Certification

Bachelor of Business Administration
Alma Mater University
Education



Share Your Credentials

Easily share details about your work history, certifications, achievements, and more.

Request for Credentials

GMS Recruiting
Global Modern Services, Inc

Required Credentials

Education
Bachelor of Business Adminis...

Employment
Senior Project Manager, Intern

Optional Credentials

Certifications
Leadership Training

Act 2:
Setbacks &
Transformation

Lessons:
People and Product

Restrictions & Challenges

Verifiable Credentials only have value if they can be exchanged freely between parties

Distributed Identity technology is a terrible solution for monetizing people’s identity

Most identity-based business models monetize over the exchange of information about a subject.

Restrictions & Challenges

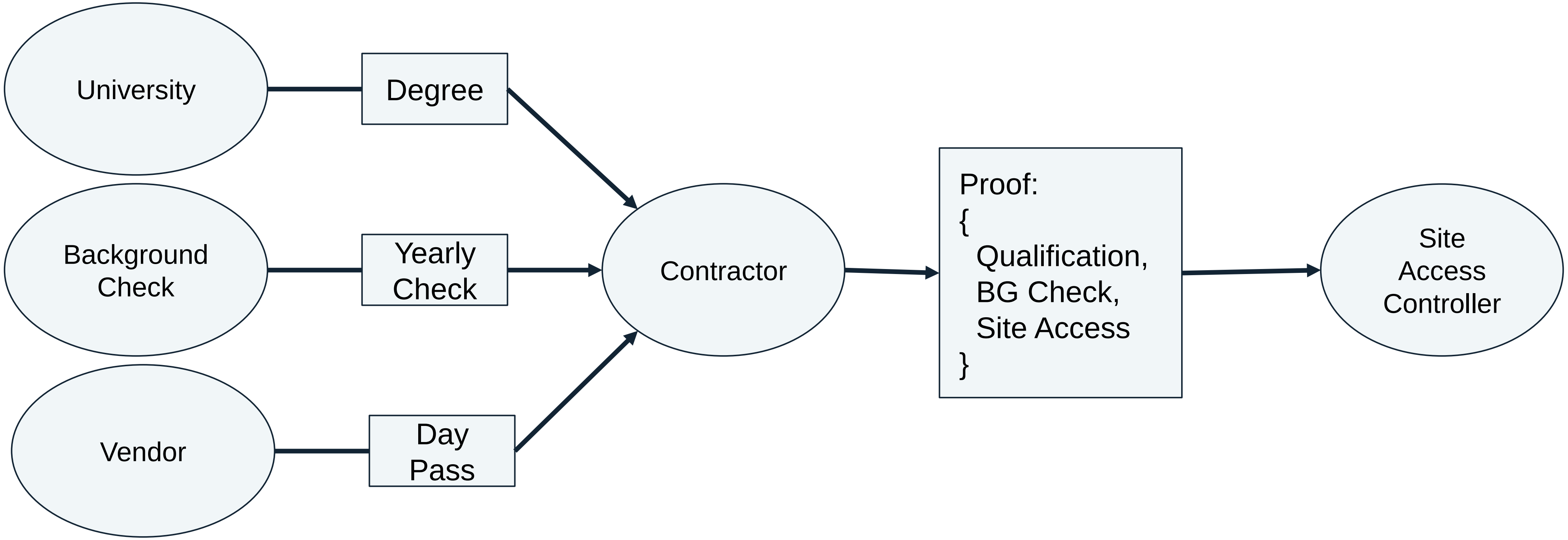
Difficult to propagate negative assertions

Verifiers are waiting for Issuers. Issuers are waiting for Verifiers.

End users are reluctant to pay for anything

You can’t sell technology, only solutions it enables

Power Use Case



Types of Trust

Delegated Trust

- Hierarchical Trust

Compounding Relationship Trust

- Weight of numbers (wisdom of crowds)

Relationship trust is affected by familiarity

- Awareness
  - Proof of age with an unfamiliar ID
- Reputational
  - Ivy League Colleges

Opportunities

Efficiency: Agency staff being given dynamic access to resources

Productivity: A consortium of banks may choose issue KYC VCs

Security: High security and high trust environments

Risk: Reduce identity and temporal threat

Lessons: Technical

Speaking The Same Language

Government

Community & Standards Organizations

- Interoperable
- Standard Implementations

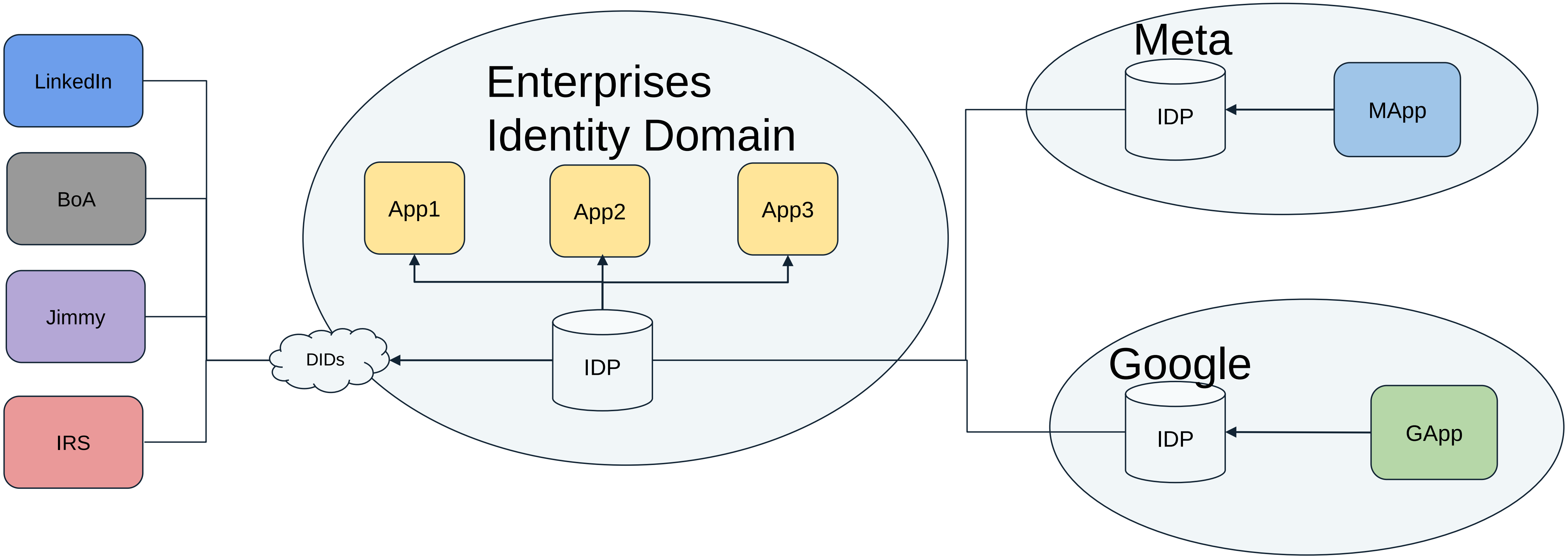
Monopoly/Monopsony

- iPhone
- Android

Enterprise Abstraction

If we consider the Holder Application to be the system of record, for a given subject’s assertions, for any number of Issuers (companies), then Verifiable Credentials can be thought of as an Integration Solution between any number of systems, bridged across the user plane.

Model for Enterprise



Applying Lessons Learned

Guiding Stars

- Empower Workday Applications to leverage identity and trust technologies, for integrating with enterprises and individuals
- Enable Workday Applications and Services to issue and revoke Verifiable Credentials to externally created identities and externally controlled holder resources (Wallets/IDHubs)
- Enable Workday Applications and Services to ingest & verify Verifiable Credentials as shared by other decentralised identities, both individual and enterprises
- Leverage existing Workday technologies and solutions
- Cost effective

SAAS to PAAS

Existing offering was impressive

Over featured for our customer needs

Want to allow Apps and Service to leverage VCs (domain experts)

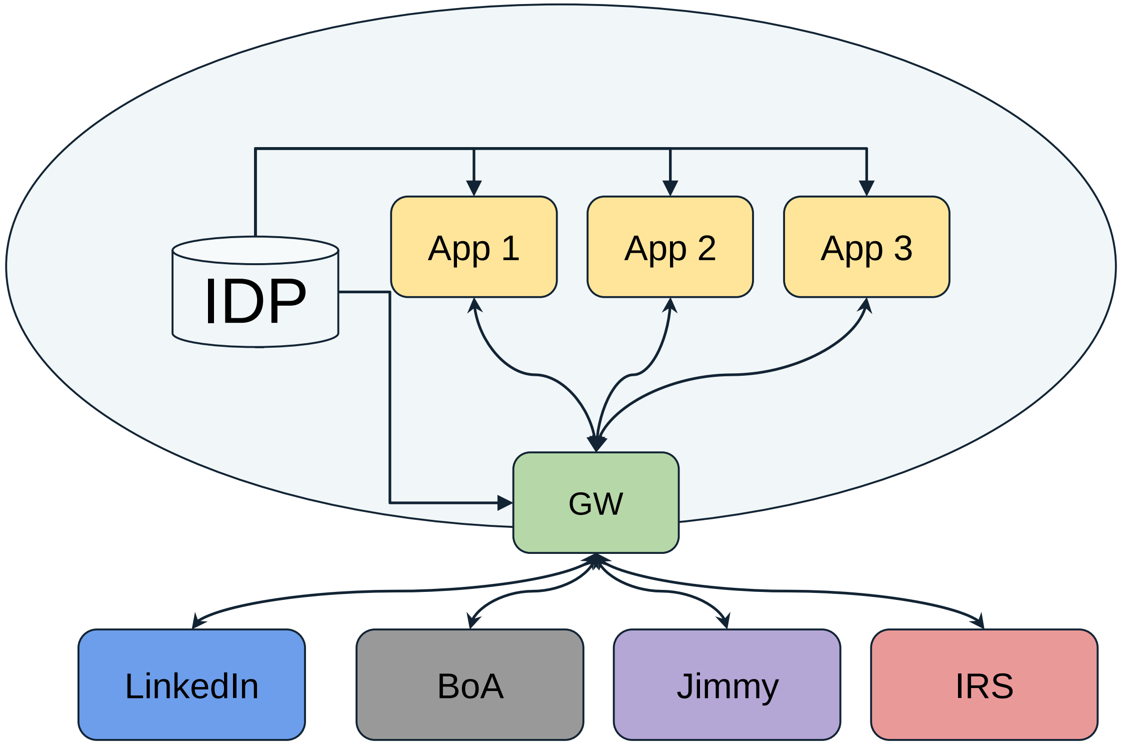
API to match tooling

Robust but easy to iterate

Verifiable Credentials Gateway

"I use a gateway whenever I access some external software and there is any awkwardness in that external element. Rather than let the awkwardness spread through my code, I contain to a single place in the gateway." - Martin Fowler

- Akin to an API Gateway
- Abstracts away sophisticated concerns
- Easier client uptake
- Encapsulates the Identity Space



Community Approach

Interoperability Profile

Compromise & Move Forward

Microsoft, Ping Identity, MATTR, IBM

No new IP or solutions

Strip optionality

Work through OIDF & Decentralized Identity Foundation

Good Now > Perfect in the Future

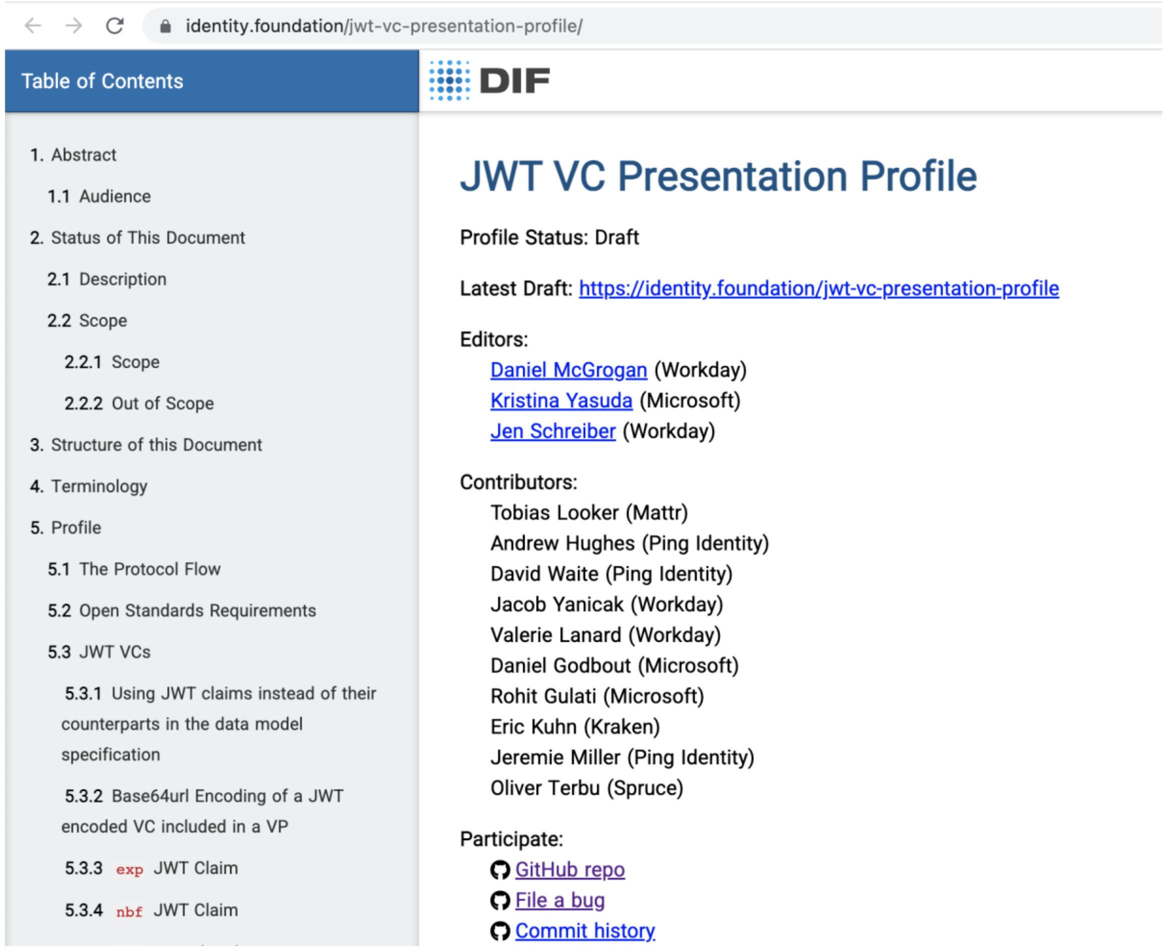


Table of Contents

JWT VC Presentation Profile

Profile Status: Draft

Latest Draft: https://identity.foundation/jwt-vc-presentation-profile

Editors:
Daniel McGrogan (Workday)
Kristina Yasuda (Microsoft)
Jen Schreiber (Workday)

Contributors:
Tobias Looker (Mattr)
Andrew Hughes (Ping Identity)
David Waite (Ping Identity)
Jacob Yanicak (Workday)
Valerie Lanard (Workday)
Daniel Godbout (Microsoft)
Rohit Gulati (Microsoft)
Eric Kuhn (Kraken)
Jeremie Miller (Ping Identity)
Oliver Terbu (Spruce)

Participate:
GitHub repo
File a bug
Commit history

Act 3:
To Be Written

Future

May 2023 Workday took a step back from active research

Customer driven use cases

Platform is primed

Waiting for the flywheel

THANK YOU!

Lessons Learned: Implementing a Distributed Identity Platform