Identity Woman in Business

Self-Sovereign Identity

A Key Piece of the Puzzle to Information Security in an Increasingly Digital Business Environment

Lucy Yang

November 29, 2022

Agenda

- The Missing Identity Layer
- Introduction to Self-Sovereign Identity (SSI)
- SSI for Improved Enterprise Application Security

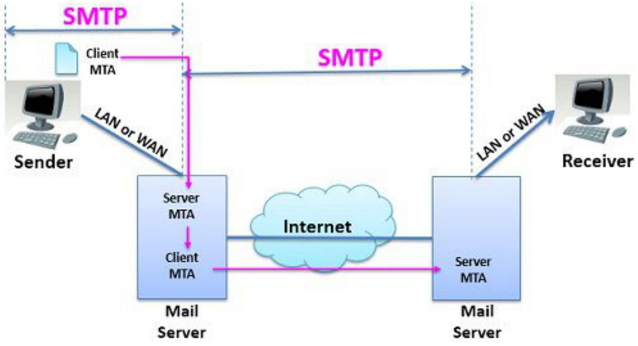
The Missing Identity Layer

Web is built on open protocols

Protocol is

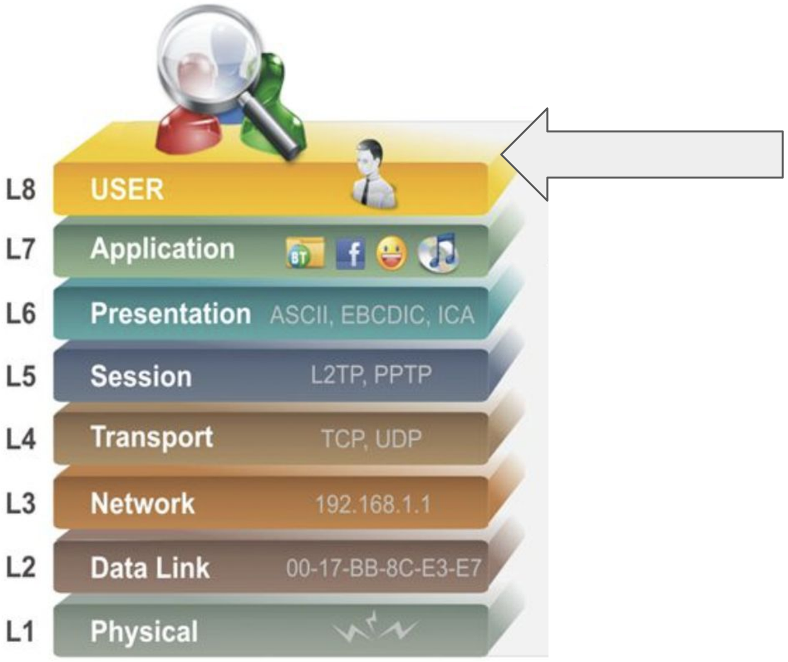
- a system of distributed management that facilitates peer-to-peer relationships between autonomous entities.
- a language that regulates flow, directs netspace, codes relationships, and connects life forms. It is etiquette for autonomous agents.

```
<tr valign="top">
    <td valign="top">
         <!-- table of main content -->
        <table width='100%' cellpadding='0' cellspacing='0' border="0">
            <tr>
                <td style="width:100%; height:400px;" valign="top">
                   <table border='0' width='750' cellpadding="0" cellspacing="0">
                        <tr>
                            <td colspan="7" style="height:10px" class="WelcomeNoteSubTitle" align="left">Help
                            </td>
                        </tr>
                        <tr>
                            <td colspan="7" style="height:15px" class="HelpGrayOption" align="left"><br />Manu
                            </td>
                        </tr>
                        <tr>
                            <td colspan="7" style="height:15px">&nbsp;
                            </td>
                        </tr>
                        <tr valign="top">
                            <td style="height:300px; width:250px;" class="GrayWriting" align="left">
                               <table border='0' style="padding-left:2px; padding-right:2px;" class="ToolBoxIn
                                    <tr>
                                        <td class="BiggerGrayWriting"><b>User Information</b></td>
                                    </tr>
                                    <tr>
                                        <td style="height:1px; background-color:#c8cbd4;"></td>
                                    </tr>
```



Internet protocols allow for inter-operation between computers

Where are we at with the Internet protocols?



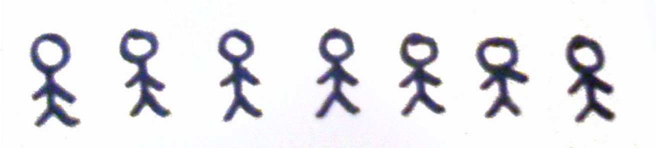
Source:https://moam.info/cyberoams-layer-8-technology-cyberoam_59fa2cd31723dd0a513087ea.html

The Missing Identity Layer: There are no protocols that define user identifiers separate from an application (facebook, twitter) or a particular domain (e-mail). There are also no protocols to express attributes about people that are portable between contexts without pre-existing connection.

identity Woman
in Business

How should users interact on the web?

Organizations



Individuals

There were two answers - neither was good

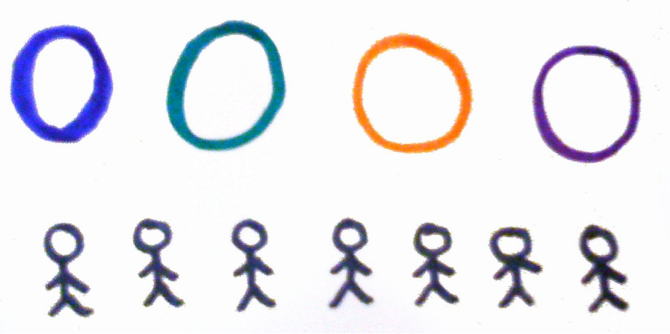
Everyone
JOIN
THE ONE
BIG PORTAL

Stay Isolated

identity Woman
in Business

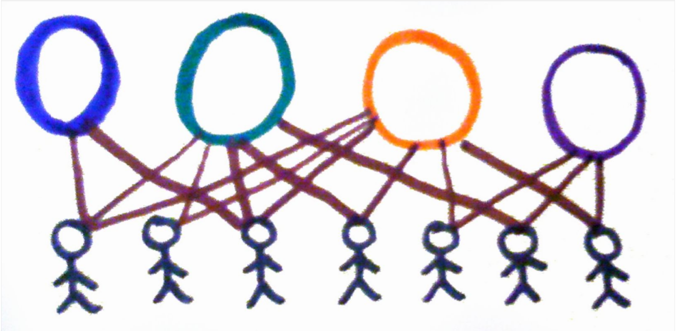
What is the ideal scenario?

Organizations would have identities



People would have identities

They would be able to connect on their own terms



Each being first class nodes on the network

Self Sovereign Identity is here to make this happen

identity Woman in Business

Introduction to Self Sovereign Identity (SSI)

identity Woman

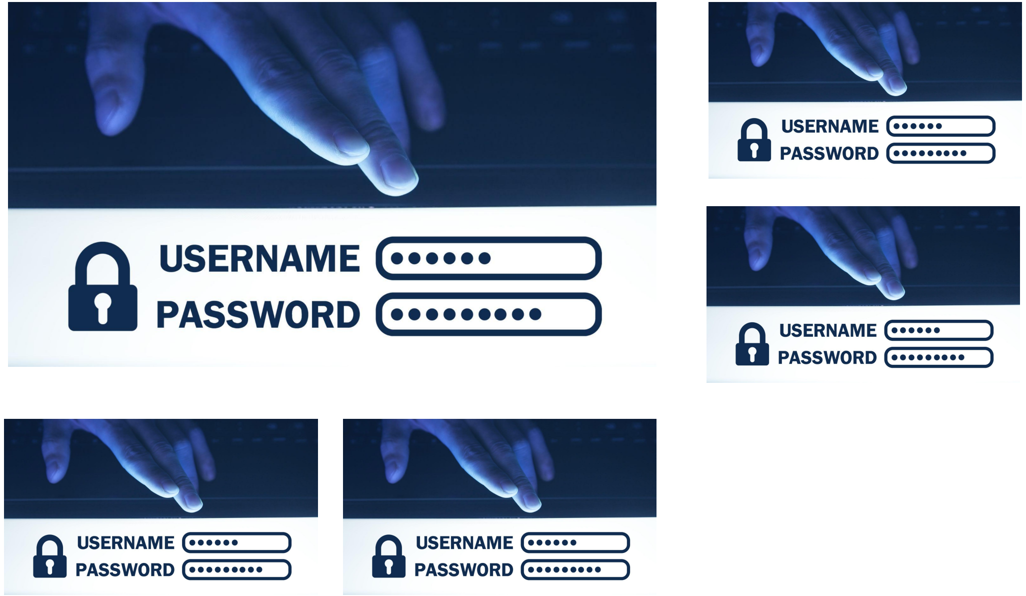
in Business

SSI explained in brief

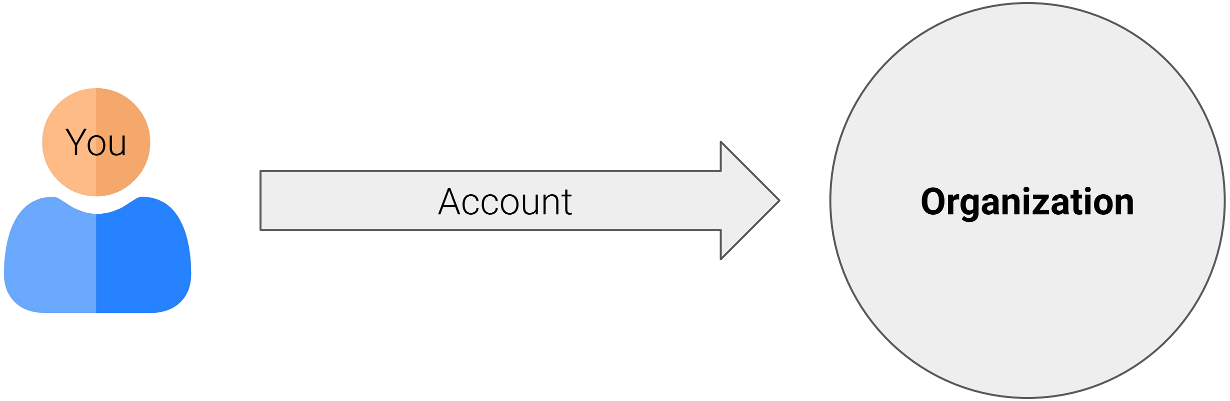
Self-sovereign Identity (SSI) is an emerging digital identity paradigm that can enable secure and trusted online transactions by letting individuals and organizations have control of their digital identity the way they do with their physical identity. With SSI, people can share the minimum required identity information needed for a particular transaction without intermediaries.

Self-sovereign identity falls into a few evolving pillars: 1) the concept of SSI, briefly explained above, 2) the principles of SSI that provide richer meaning than the concept, and 3) the technology that is enabling the realization of the concept and principles.

The SSI journey stop 1: Siloed Identity



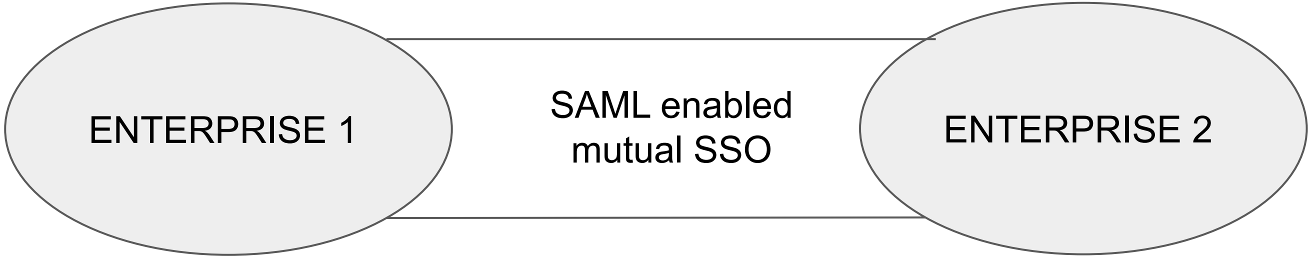
The SSI journey stop 1: Siloed Identity



In the siloed identity model, you need to create an account, typically with a username and password, with each organization in order to interact digitally with it. In this model, the organization becomes a identity provider of yours and you will end up managing countless accounts from countless identity providers who hold your data.

identity Woman in Business

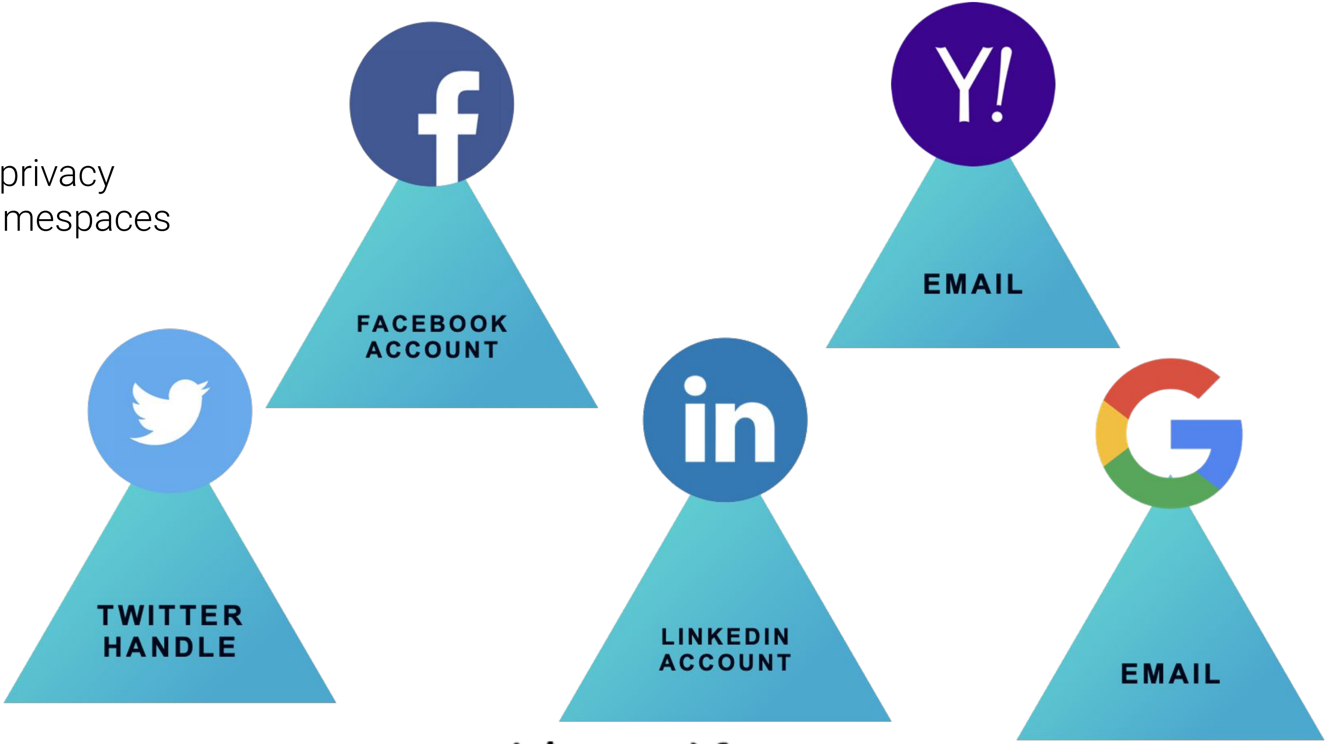
The SSI journey stop 2:
Traditional Federated Enterprise Identity



identity Woman
in Business

The SSI journey stop 2: Federated Identity

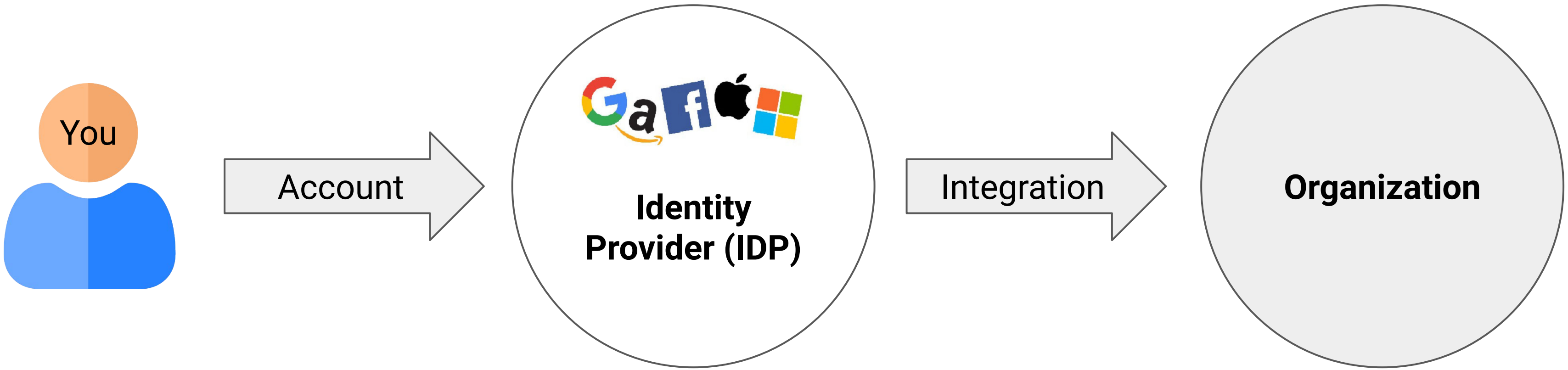
Identifiers in privacy controlled namespaces



identity Woman in Business

Not for Circulation

The SSI journey stop 2: Federated Identity



In the federated identity model, instead of the organization you interact with being your identity provider, you will have a middlemen, usually a big tech company like Facebook and Google, provide the identity data needed for the organization to authenticate you. In this model, the middlemen will know about your every single interaction with the organization that they are involved in.

identity Woman
in Business

The SSI journey stop 2: Federated Identity

some identifiers we can pick…

MYURL.COM

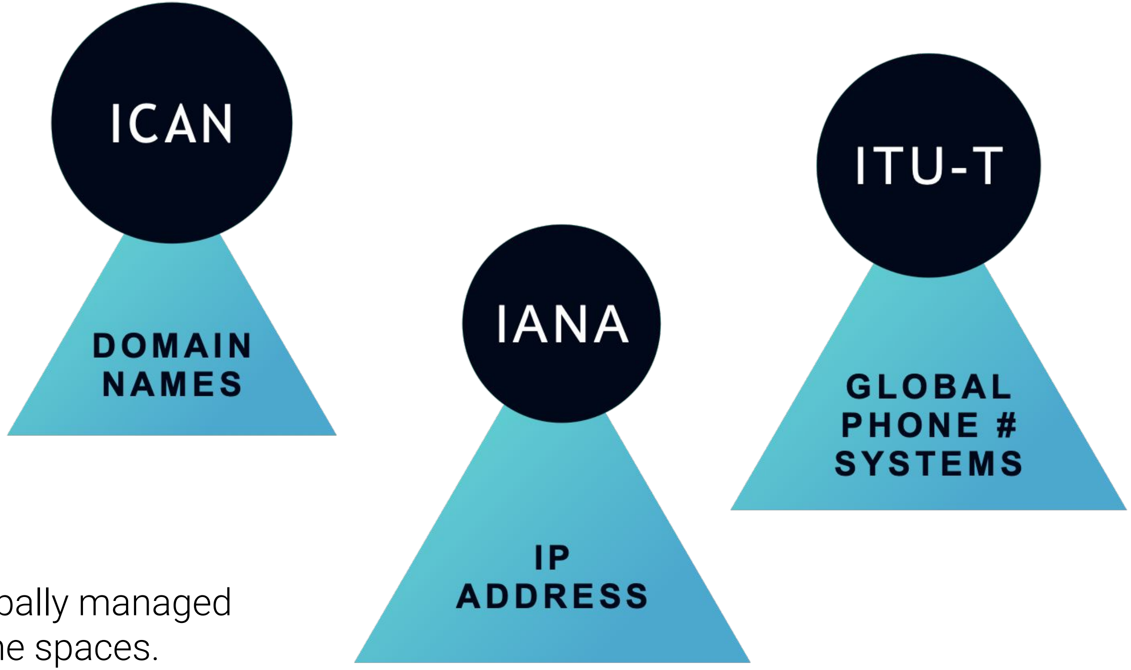
…but we really rent them…

identity Woman in Business

The SSI journey stop 2: Federated Identity

...and we rent our phone numbers

The SSI journey stop 2: Federated Identity



ICAN

DOMAIN NAMES

IANA

IP ADDRESS

ITU-T

GLOBAL PHONE # SYSTEMS

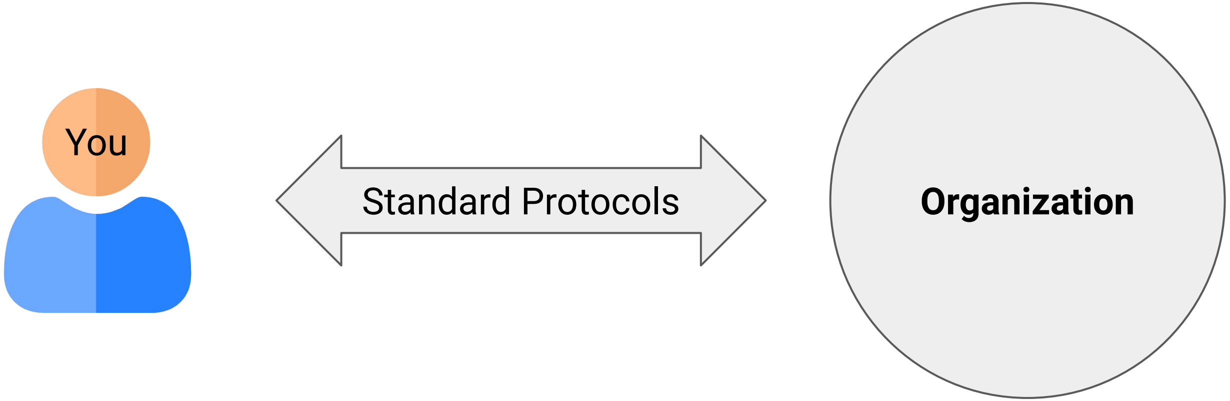
Identifiers in globally managed
hierarchical name spaces.

identity Woman
in Business

The SSI journey stop 3: Self Sovereign Identity

There are no digital
identifiers
we really own.

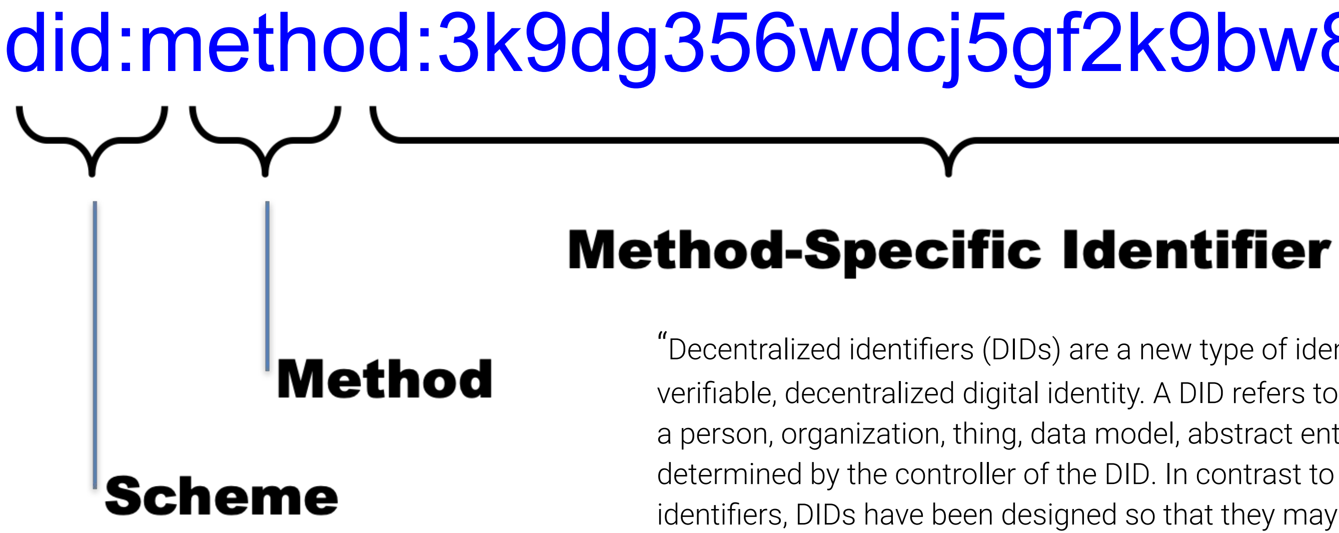
The SSI journey stop 3: Self Sovereign Identity



The self-sovereign identity model enable peer-to-peer interactions that allow you to be your own identity provider when interacting with an organization digitally. You control the data that makes up your identity information as well with whom you share that information with. This is made possible by a set of emerging open standards and technology.

identity Woman in Business

Core SSI Standard 1: Decentralized Identifier (DID)



did:method:3k9dg356wdcj5gf2k9bw8kfg7a

Method-Specific Identifier

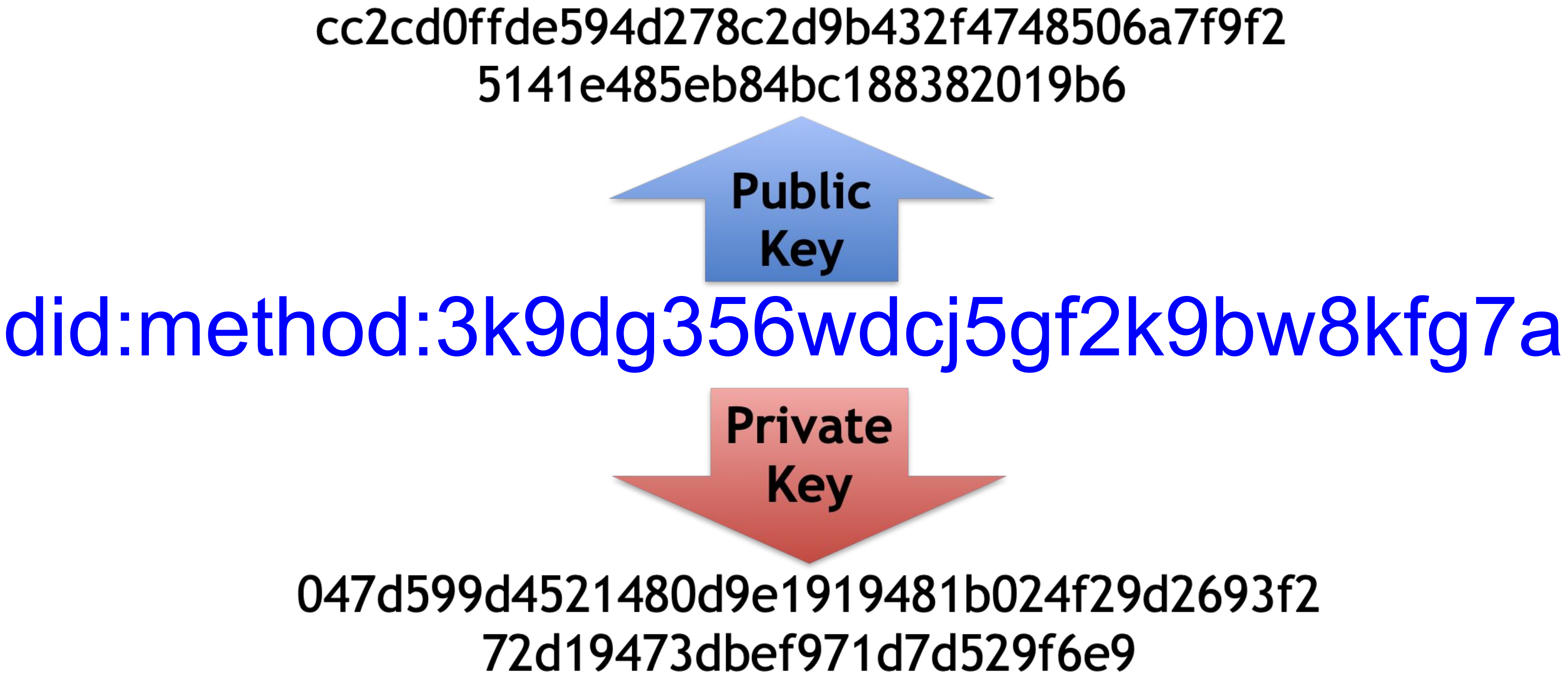
Method

Scheme

“Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities.”
(Source: https://www.w3.org/TR/did-core/)

Identity Woman
in Business

Core SSI Standard 1: Decentralized Identifier (DID)



cc2cd0ffde594d278c2d9b432f4748506a7f9f2
5141e485eb84bc188382019b6

Public Key

did:method:3k9dg356wdcj5gf2k9bw8kfg7a

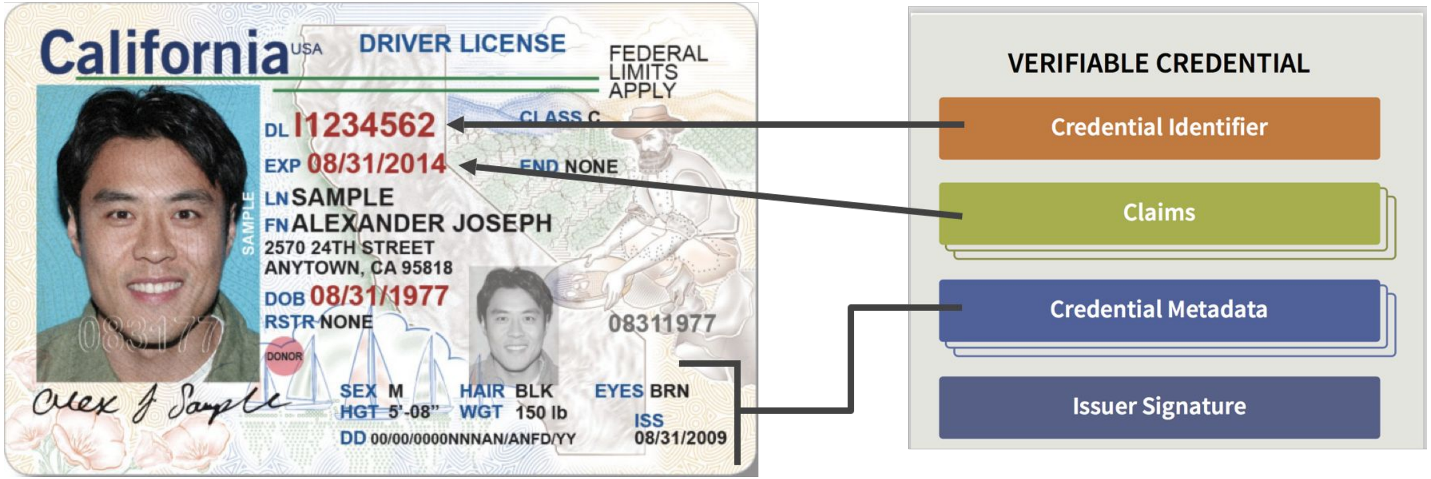
Private Key

047d599d4521480d9e1919481b024f29d2693f2
72d19473dbef971d7d529f6e9

identity Woman
in Business

Core SSI Standard 2: Verifiable Credential (VC)

“A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.” (Source: https://www.w3.org/TR/vc-data-model/)



California USA DRIVER LICENSE

FEDERAL LIMITS APPLY

DL I1234562 CLASS C

EXP 08/31/2014 END NONE

LN SAMPLE

FN ALEXANDER JOSEPH

2570 24TH STREET
ANYTOWN, CA 95818

DOB 08/31/1977

RSTR NONE

08311977

DONOR

Alex J Sample

SEX M HAIR BLK EYES BRN

HGT 5'-08" WGT 150 lb

DD 00/00/0000NNNAN/ANFD/YY

ISS 08/31/2009

VERIFIABLE CREDENTIAL

Credential Identifier

Claims

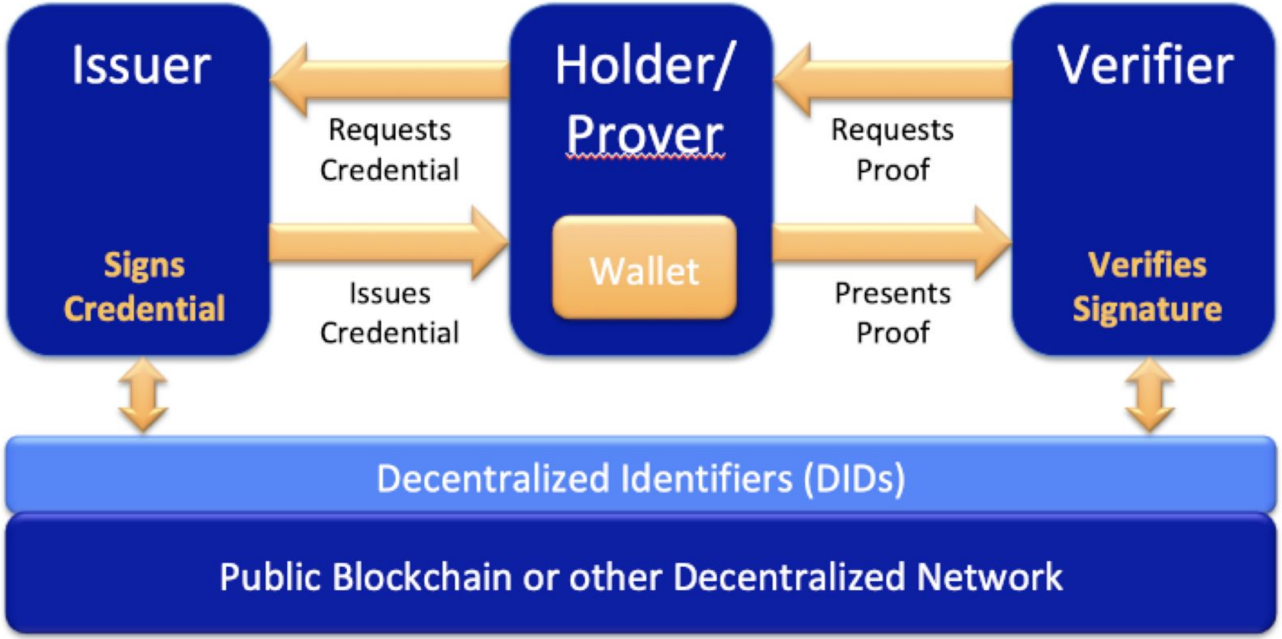
Credential Metadata

Issuer Signature

Source: https://livebook.manning.com/book/self-sovereign-identity/chapter-2/v-7/36

identity Woman in Business

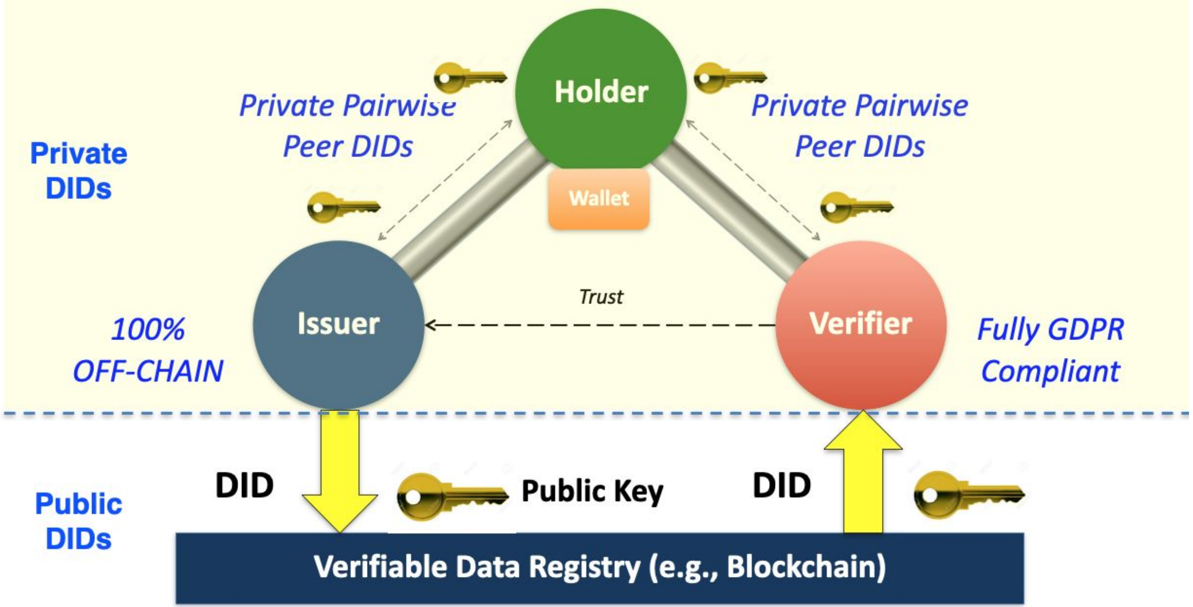
Core SSI Standard 2: Verifiable Credential (VC)



Source: https://www.slideshare.net/SSIMeetup/decentralized-identifiers-dids-the-fundamental-building-block-of-selfsovereign-identity-ssi

identity Woman in Business

Core SSI Standard 3: DIDComm Messaging



Source: https://trustoverip.github.io/WP0010-toip-foundation-whitepaper/trust/vcred_trust_triangle/

The purpose of DIDComm Messaging is to provide a secure, private communication methodology built atop the decentralized design of DIDs

(Source:https://identity.foundation/didcomm-messaging/spec/)

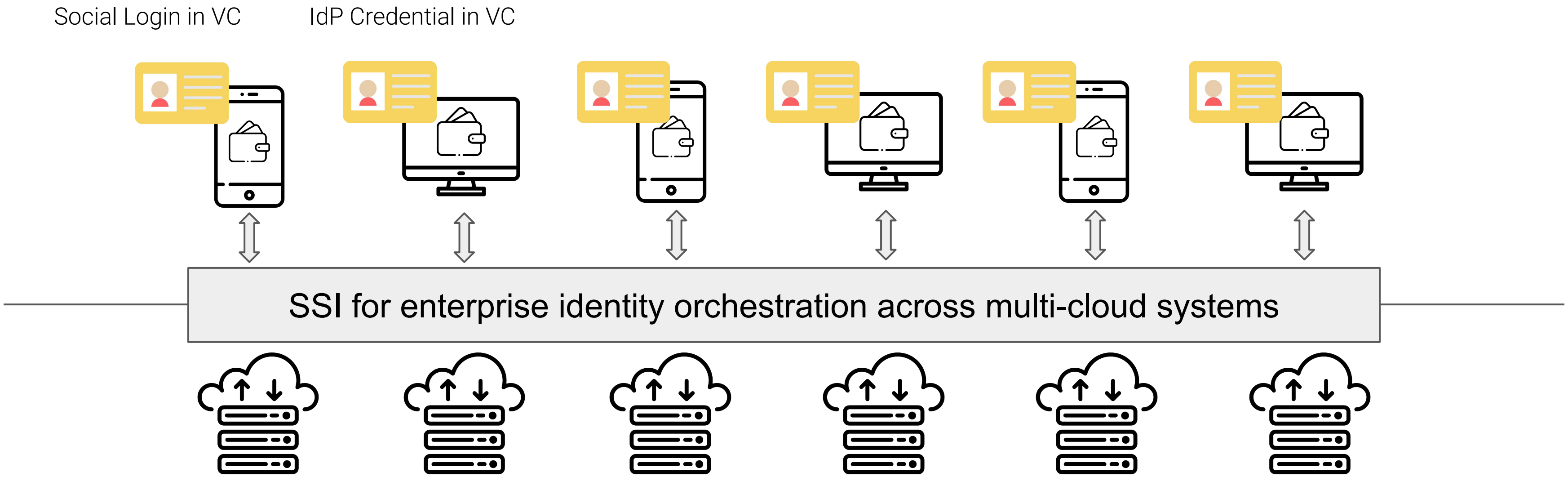
identity Woman in Business

SSI for Improved Information Security

IAM Across Multiple Cloud Environments

identity Woman
in Business

Passwordless Login Across Platforms



Social Login in VC

IdP Credential in VC

SSI for enterprise identity orchestration across multi-cloud systems

identity Woman

in Business

SSI for Improved Information Security

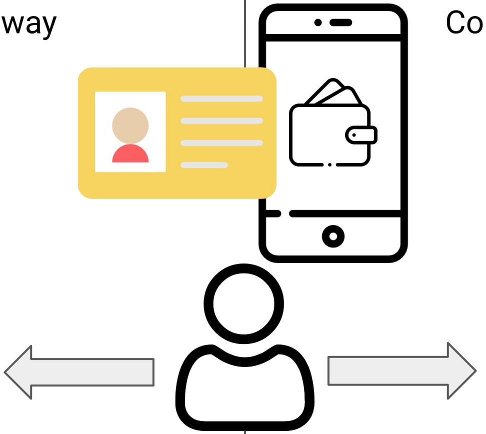
Workforce and Customer IAM

identity Woman
in Business

People-Centric Identity Management

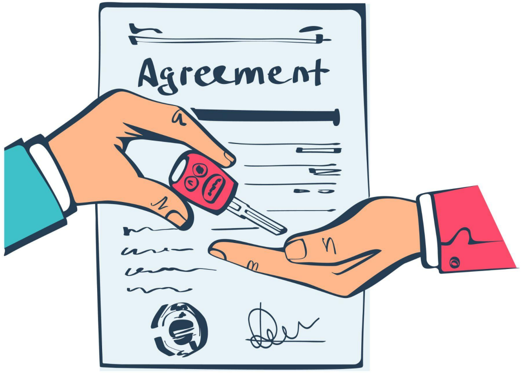
Workforce

Passing through office building gateway



Customer

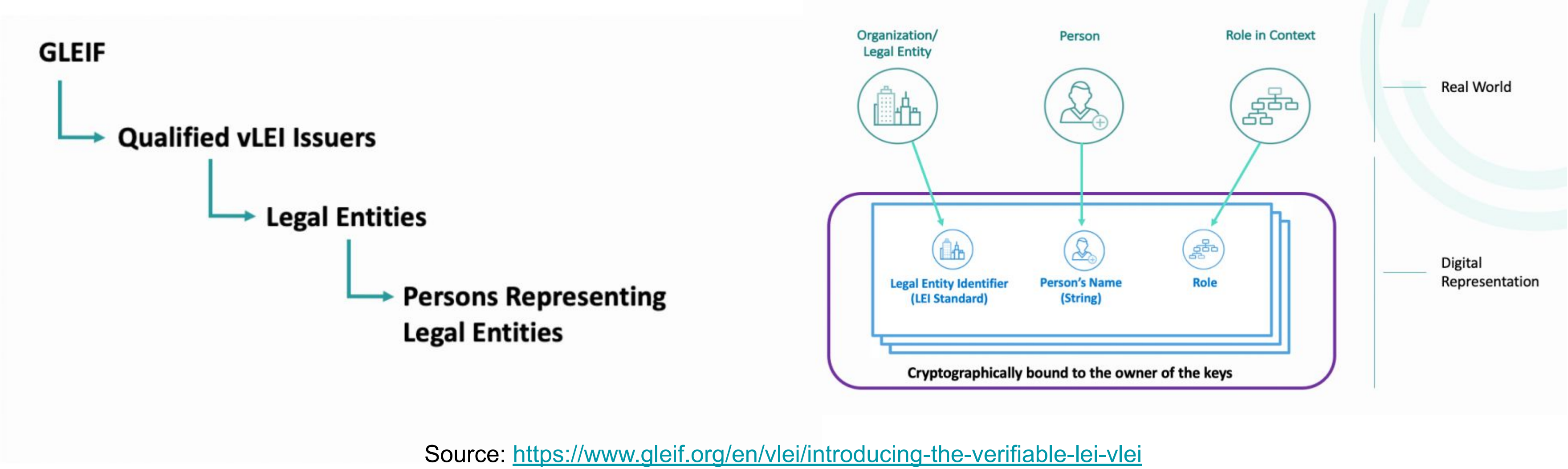
Corporate employee discount at car rental



Identity Woman
in Business

Verifiable Legal Entity Identifier (vLEI)

Much harder for attackers to fake identities as an employee/representative of your company



GLEIF

Qualified vLEI Issuers

Legal Entities

Persons Representing Legal Entities

Source: https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei

identity Woman
in Business

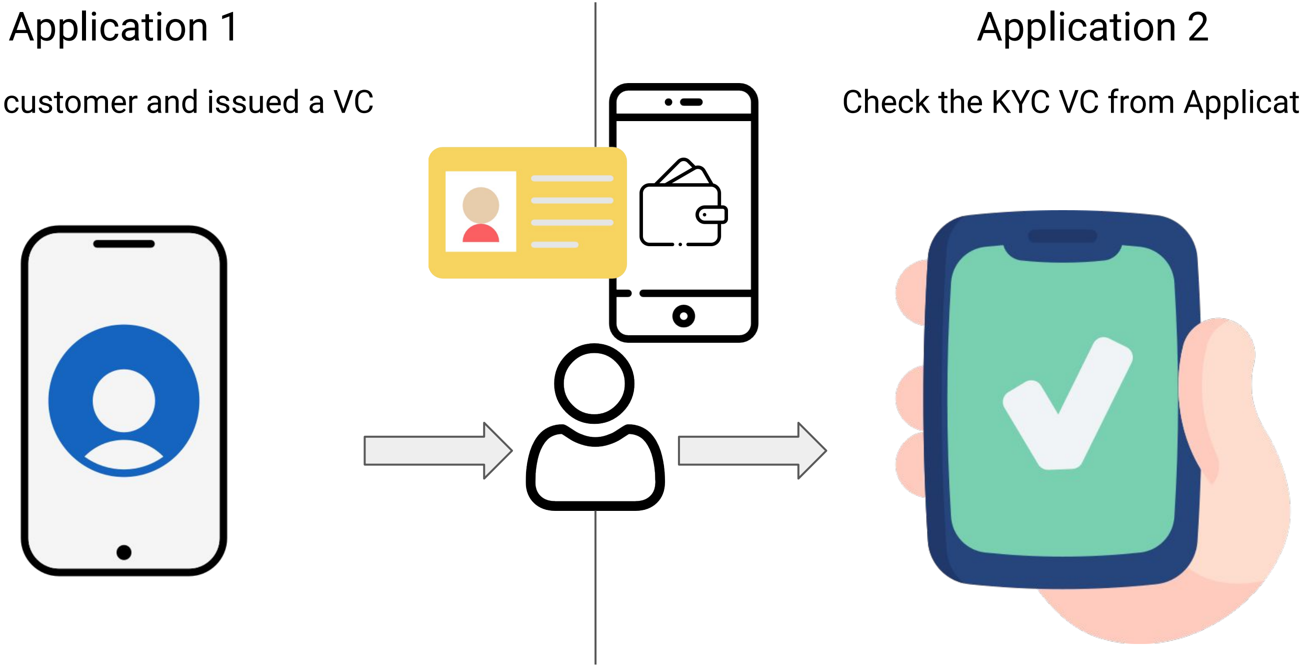
Leverage KYC conducted by trusted parties

Application 1

KYCed a customer and issued a VC

Application 2

Check the KYC VC from Application



identity Woman

in Business

SSI for Improved Information Security

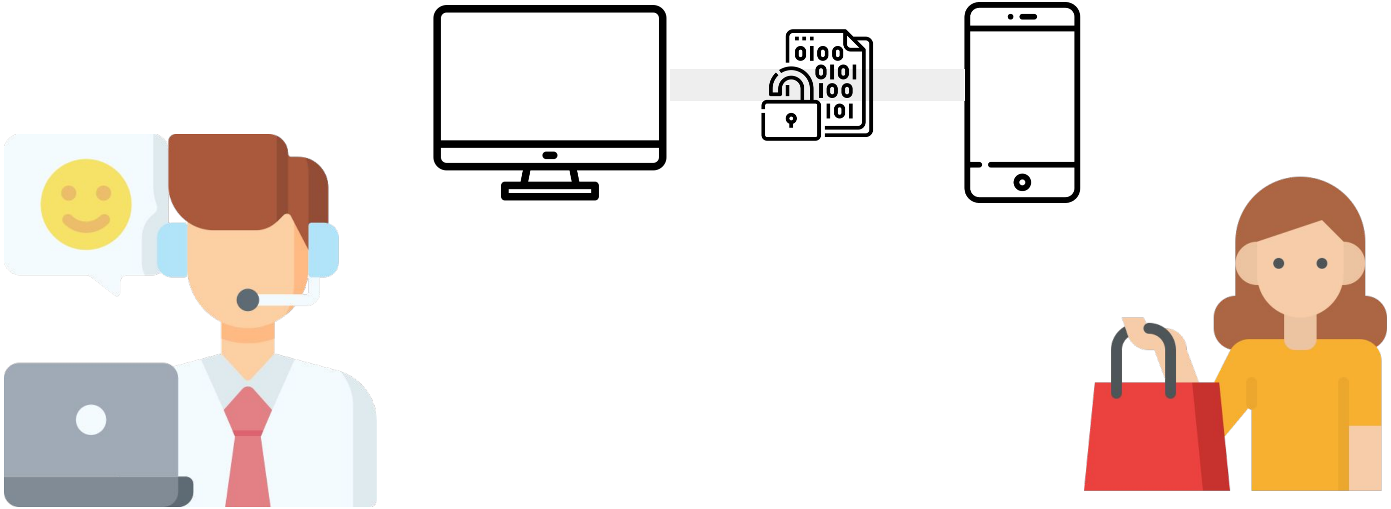
Information / Data Security Management

identity Woman
in Business

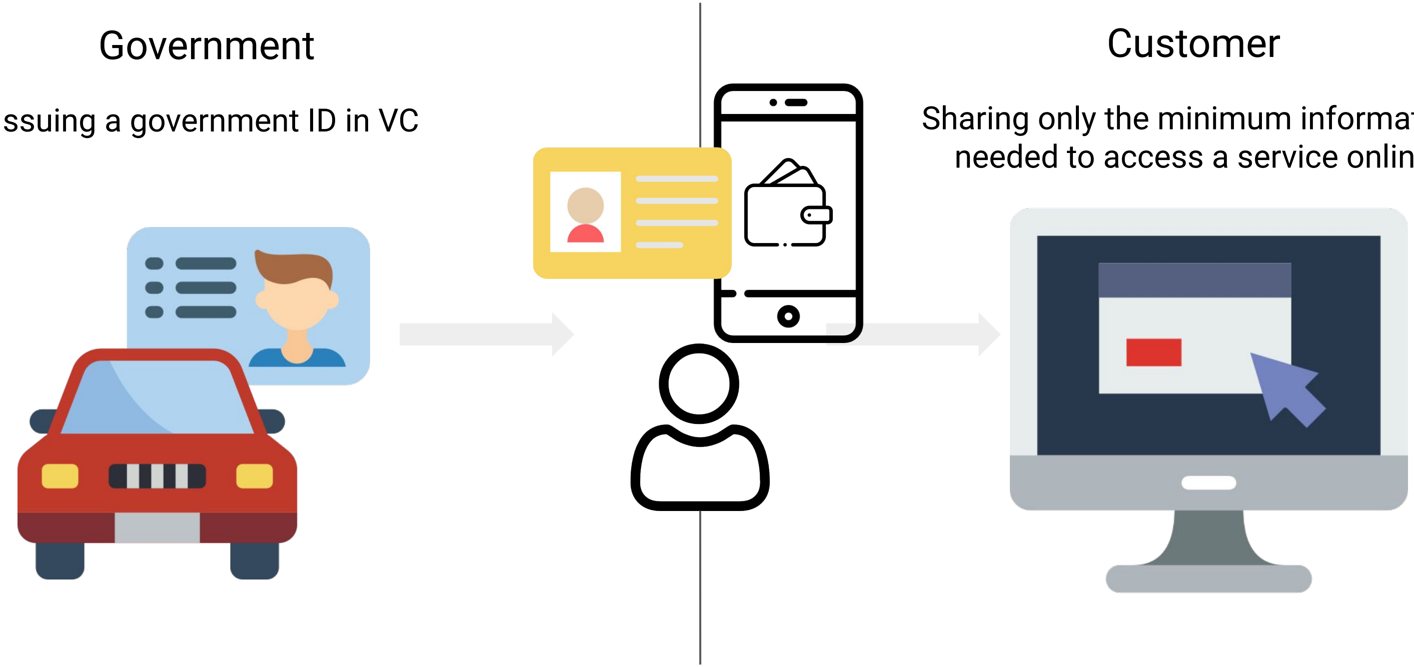
Secure and Peer-to-Peer Communication

Organization

Customer



Minimal data exposure, sharing and storage



Government

Issuing a government ID in VC

Customer

Sharing only the minimum information needed to access a service online

Q&A

Further Resources and Contact

Free edX Course: Getting Started with Self Sovereign Identity

Identosphere Newsletter: https://newsletter.identosphere.net/

lucy@identitywoman.net

identity Woman
in Business