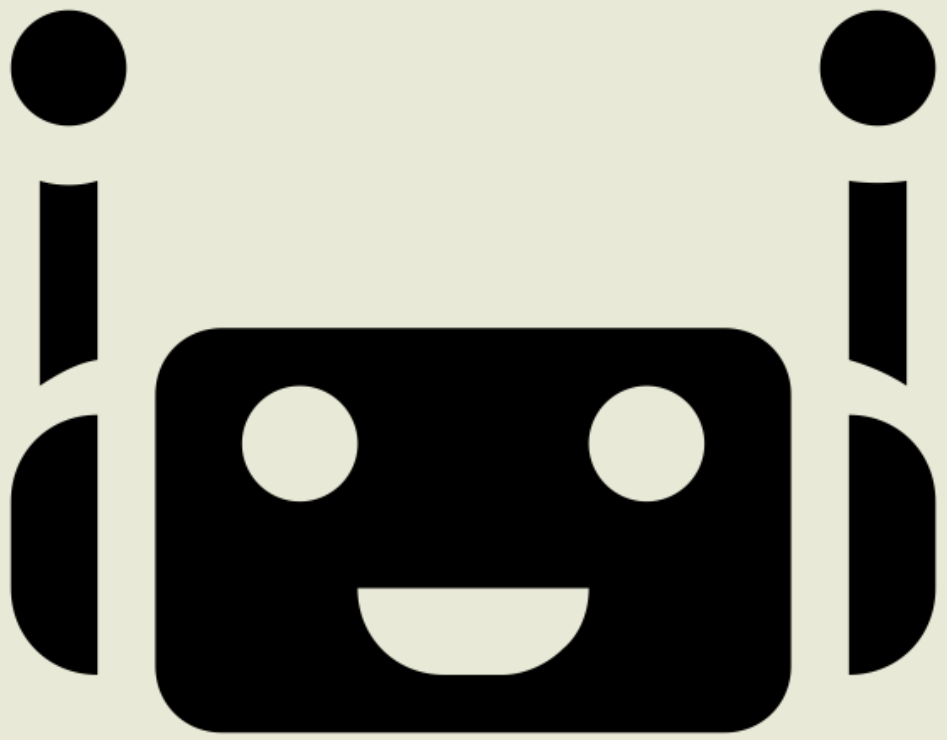
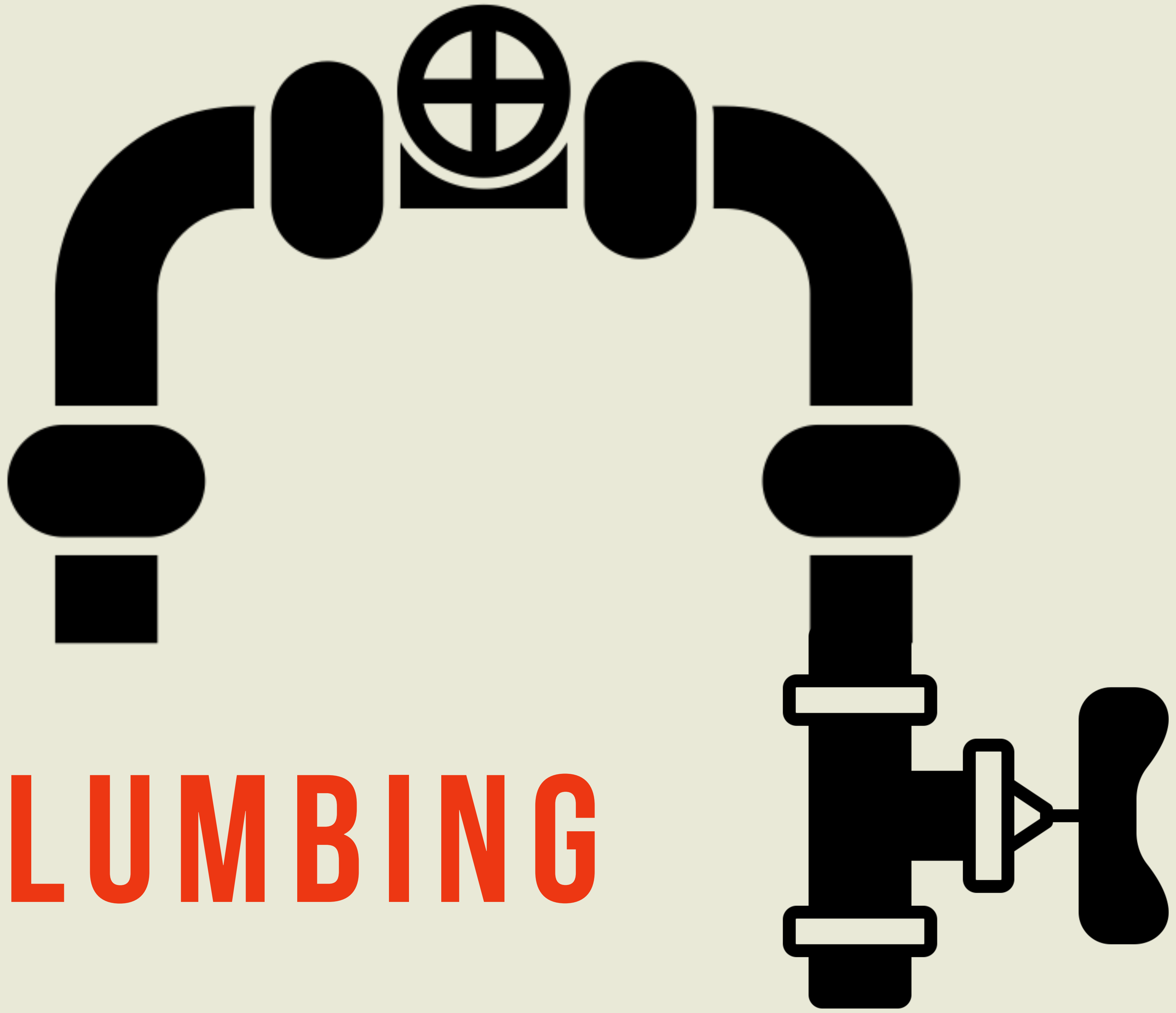


AUTONOMOUS

I'm passionate about building autonomous systems – systems of machines that work together to almost magically improve our lives.



PLUMBING

But I spend most of my days doing what is best described as - digital plumbing.

IF A PERSON ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

To illustrate, let's consider this extremely simple autonomous system.

How do we identify a person?
How do we authenticate them?

IF A PERSON ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

IF A PERSON **ENTERS** A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

How do we know they entered?
With a device?
How do we identify the device?
Can we trust it?

IF A PERSON ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

How do we identify a room?

IF A PERSON ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

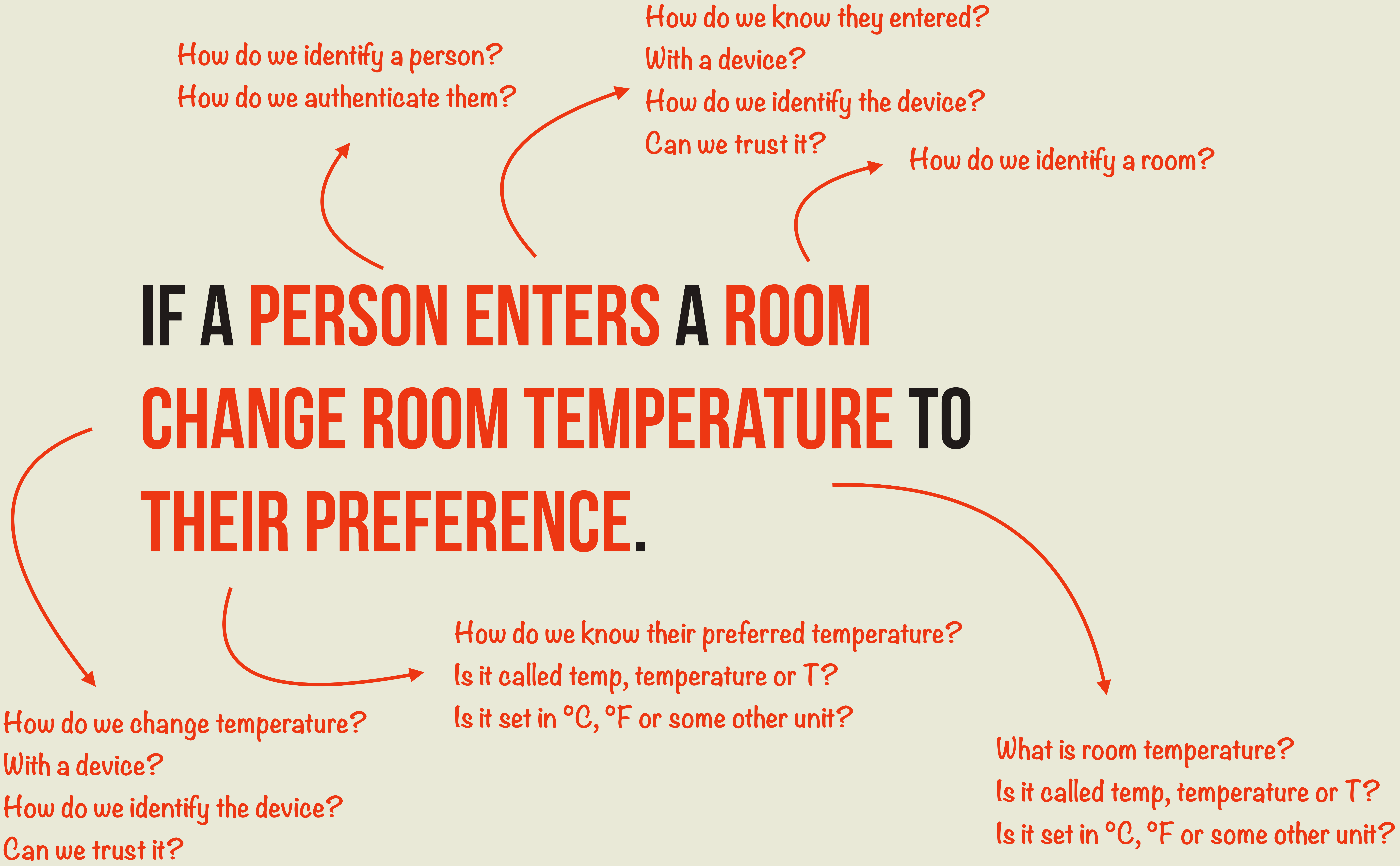
How do we change temperature?
With a device?
How do we identify the device?
Can we trust it?

IF A PERSON ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

What is room temperature?
Is it called temp, temperature or T?
Is it set in °C, °F or some other unit?

IF A PERSON ENTERS A ROOM
CHANGE ROOM TEMPERATURE TO
THEIR PREFERENCE.

How do we know their preferred temperature?
Is it called temp, temperature or T?
Is it set in °C, °F or some other unit?



IF A PERSON ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

How do we identify a person?
How do we authenticate them?

How do we know they entered?
With a device?
How do we identify the device?
Can we trust it?

How do we identify a room?

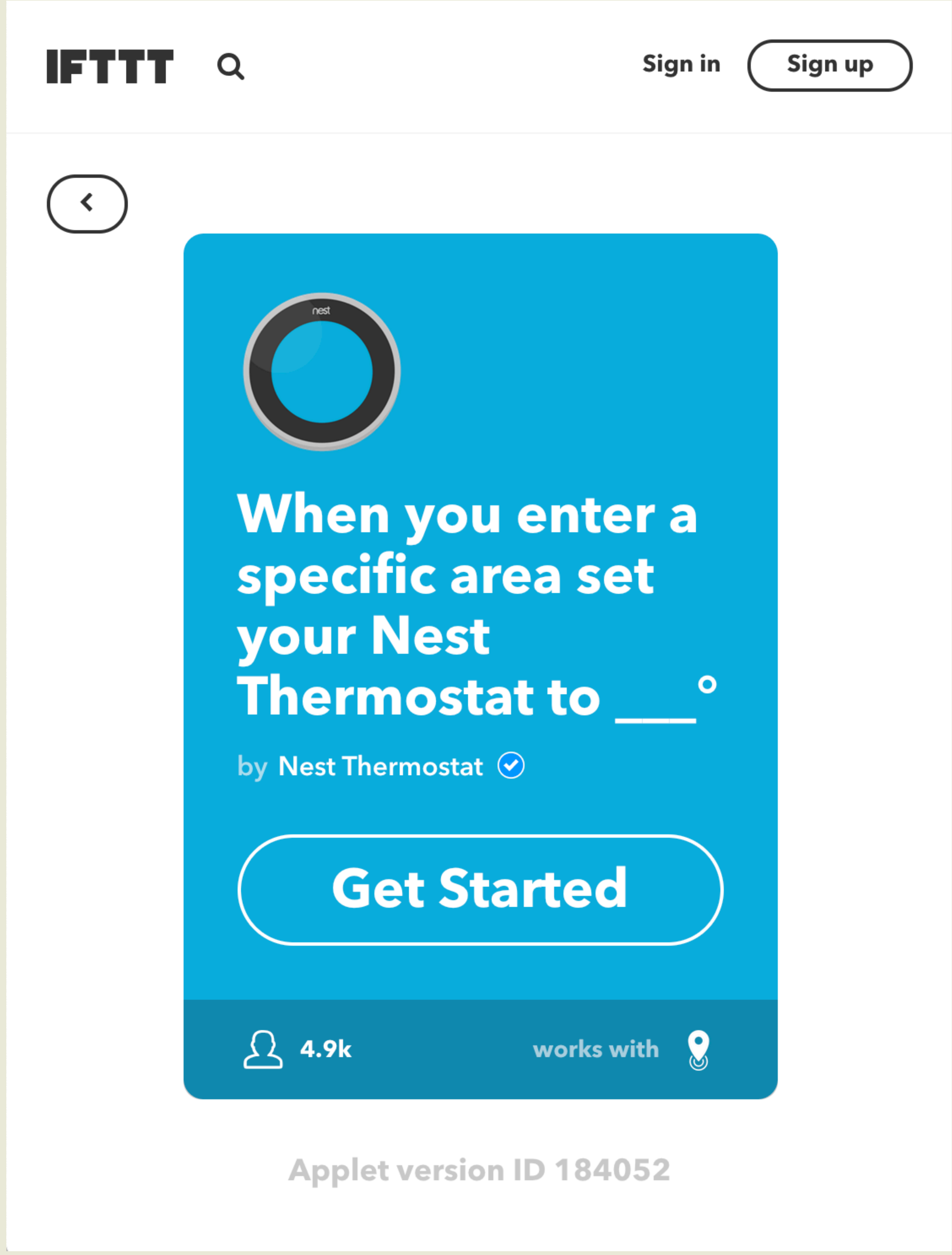
How do we change temperature?
With a device?
How do we identify the device?
Can we trust it?

How do we know their preferred temperature?
Is it called temp, temperature or T?
Is it set in °C, °F or some other unit?

What is room temperature?
Is it called temp, temperature or T?
Is it set in °C, °F or some other unit?

IF A PERSON ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

This seems hard, surely someone else has already built it.



When you enter a specific area set your Nest Thermostat to ___°

by Nest Thermostat ✓

Applet version ID 184052

Found one with a quick google search, but it only works with Nest and IFFTT, my hardware is different :(

1000s of People Identity Systems
Google, Facebook, Apple, Active Directory,
Custom Apps etc.

IF A **PERSON** ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

The problem gets worse if, like any good programmer, I only want to write this program once.

1000s of phones, motion sensors, RFID reader etc.
100s of IoT platforms, proprietary systems etc.

IF A PERSON **ENTERS** A ROOM
CHANGE ROOM TEMPERATURE TO
THEIR PREFERENCE.

100s of building management systems and custom apps etc.

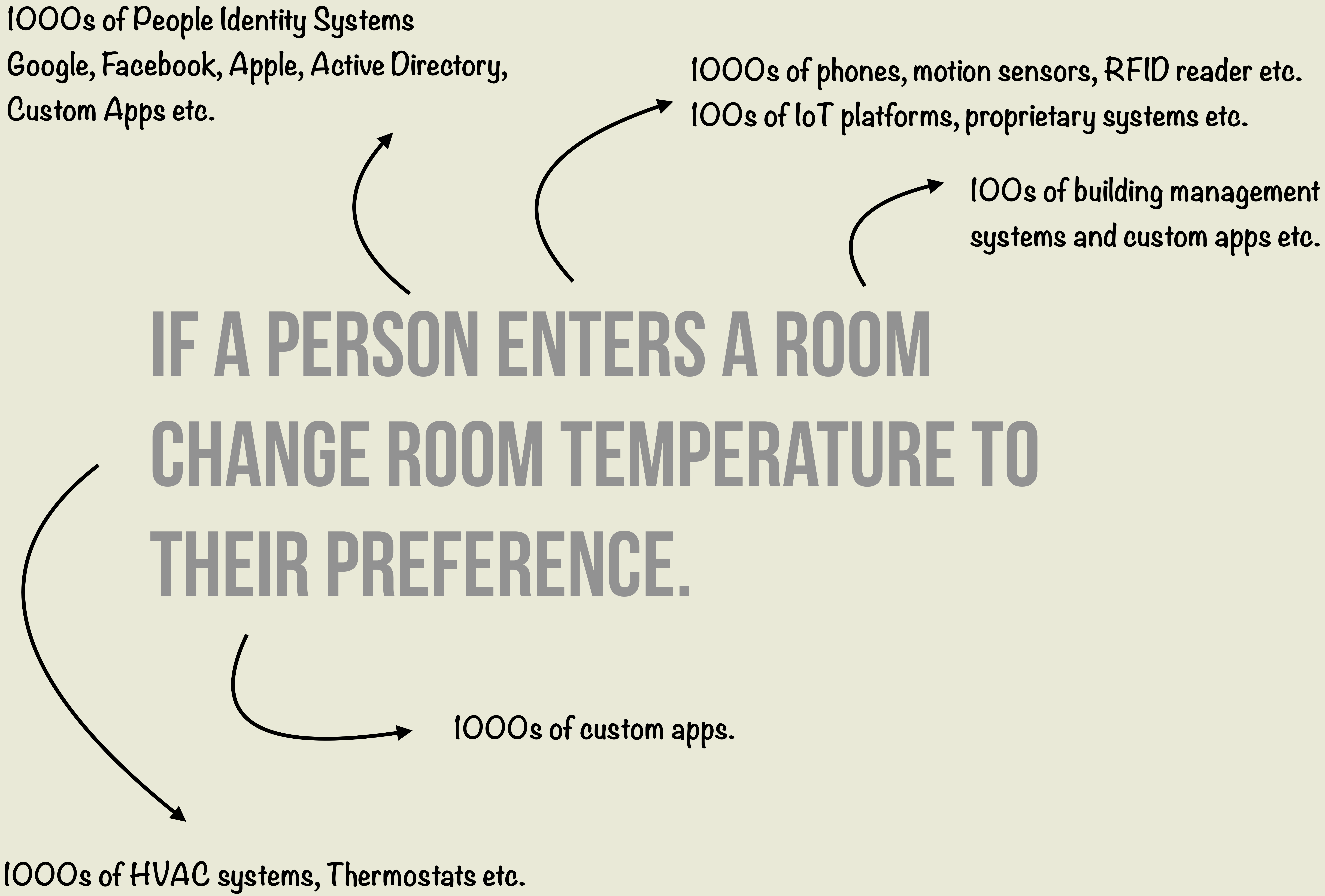
IF A PERSON ENTERS A **ROOM** CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

IF A PERSON ENTERS A ROOM
CHANGE ROOM TEMPERATURE TO
THEIR PREFERENCE.

1000s of HVAC systems, Thermostats etc.

IF A PERSON ENTERS A ROOM
CHANGE ROOM TEMPERATURE TO
THEIR PREFERENCE.

1000s of custom apps.



IF A PERSON ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

1000s of People Identity Systems
Google, Facebook, Apple, Active Directory,
Custom Apps etc.

1000s of phones, motion sensors, RFID reader etc.
100s of IoT platforms, proprietary systems etc.

100s of building management
systems and custom apps etc.

1000s of custom apps.

1000s of HVAC systems, Thermostats etc.

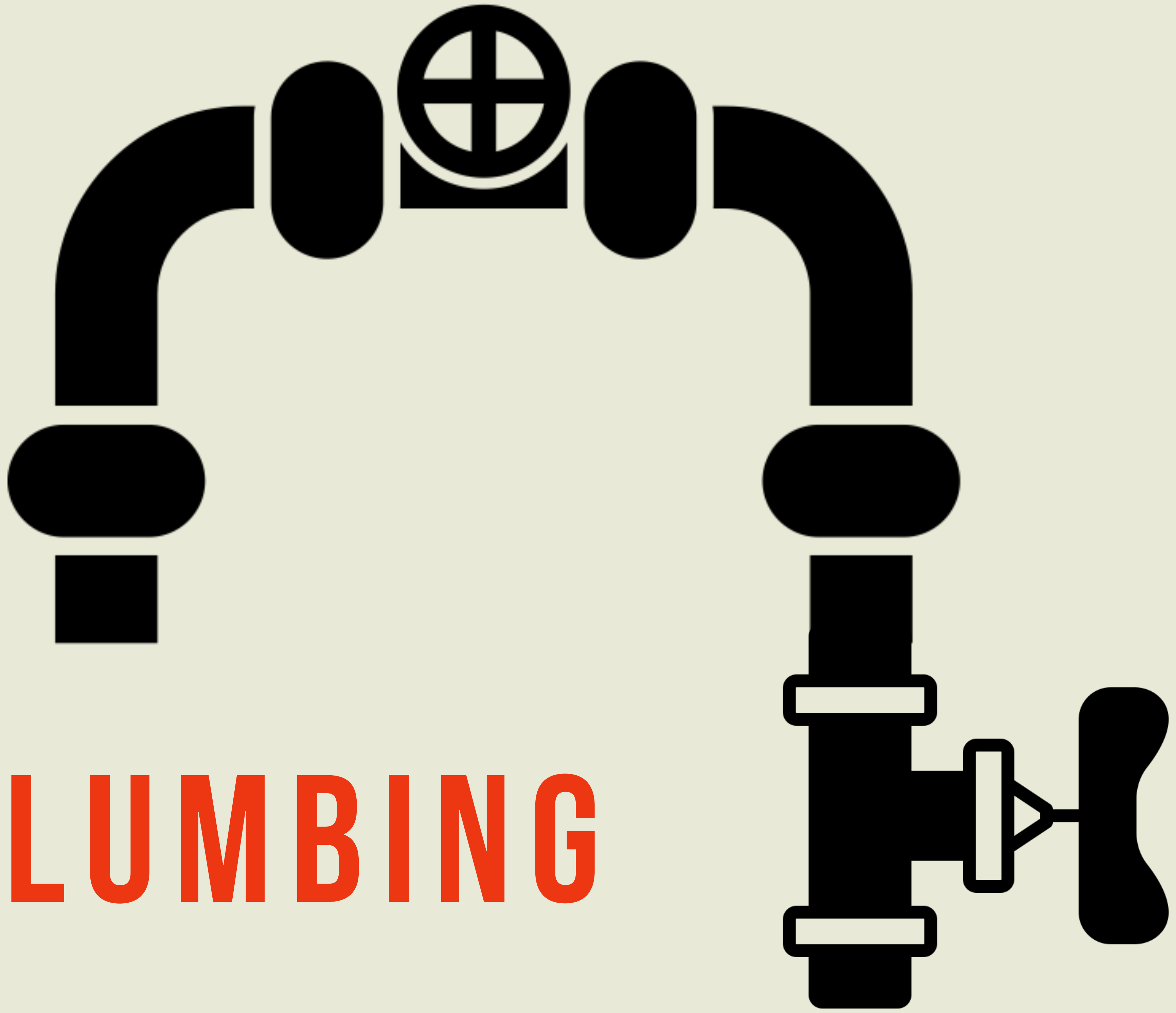
IF A PERSON ENTERS A ROOM CHANGE ROOM TEMPERATURE TO THEIR PREFERENCE.

Also, this problem statement isn't general enough, I like to write reusable code.

IF A SHIPMENT ENTERS A CONTAINER CHANGE CONTAINER TEMPERATURE TO IDEAL TEMPERATURE OF SHIPMENT.

Also, this new problem statement isn’t that different, lets generalize …

IF AN ENTITY THAT HAS PREFERENCES,
IS DETECTED AS HAVING ENTERED AN AREA THAT CAN APPLY PREFERENCES
APPLY ALL ENTITY PREFERENCES THAT THE AREA CAN APPLY
THAT THIS ENTITY IS AUTHORIZED TO APPLY TO THIS AREA.



PLUMBING

Most IoT developers spend most of their time dealing with this complicated plumbing, the magic is rare.

SCALABILITY

SECURITY

PRIVACY

TRUST

RELIABILITY

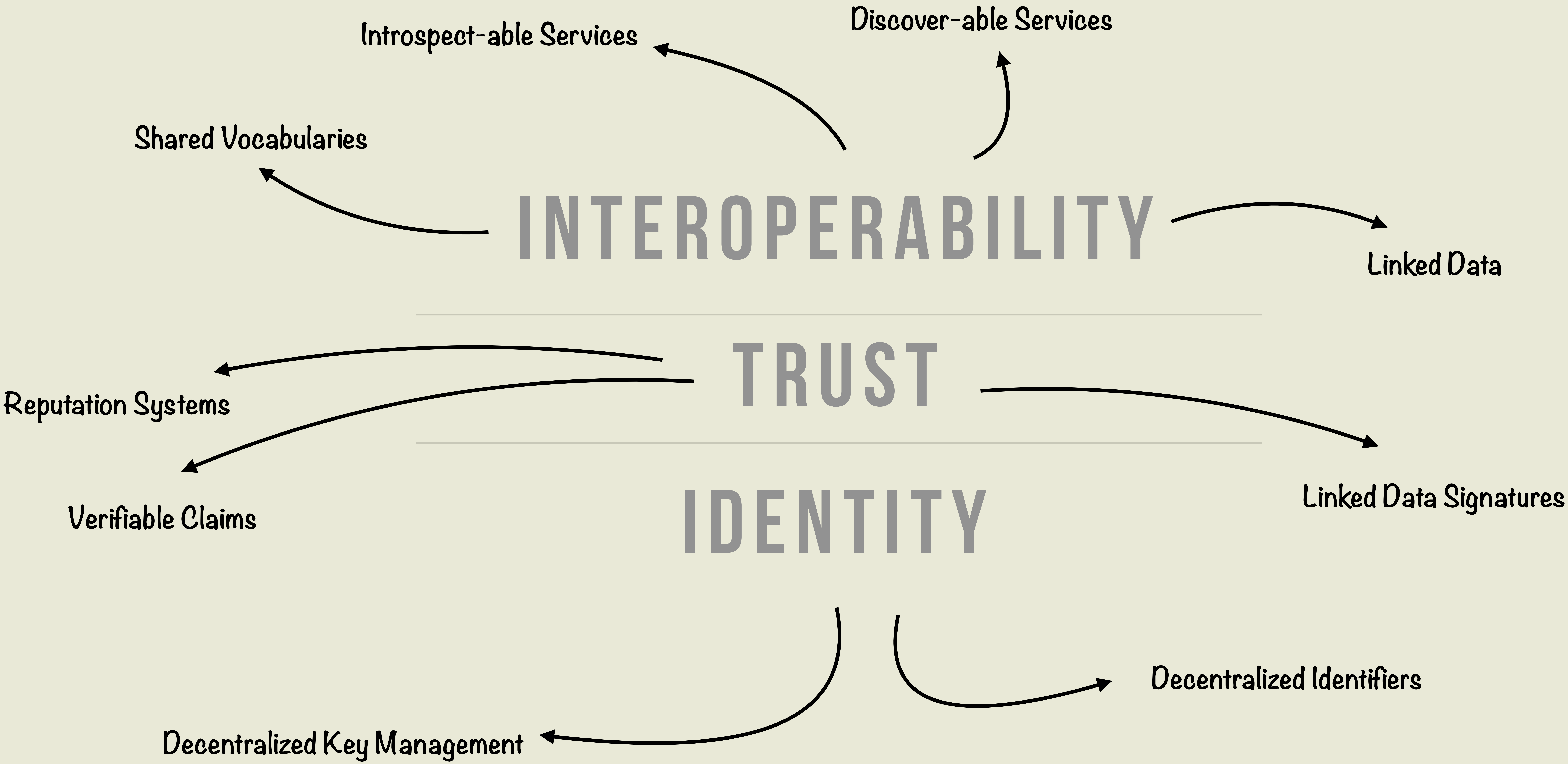
All of these plumbing complications also manifest as weaknesses in other key architectural requirements.

INTEROPERABILITY

TRUST

IDENTITY

We’re applying several open standards and building open source tools to address these challenges.
Our thinking is organized in the above three layers.



INTEROPERABILITY

Shared Vocabularies

Introspect-able Services

Discover-able Services

Linked Data

TRUST

Reputation Systems

Verifiable Claims

Linked Data Signatures

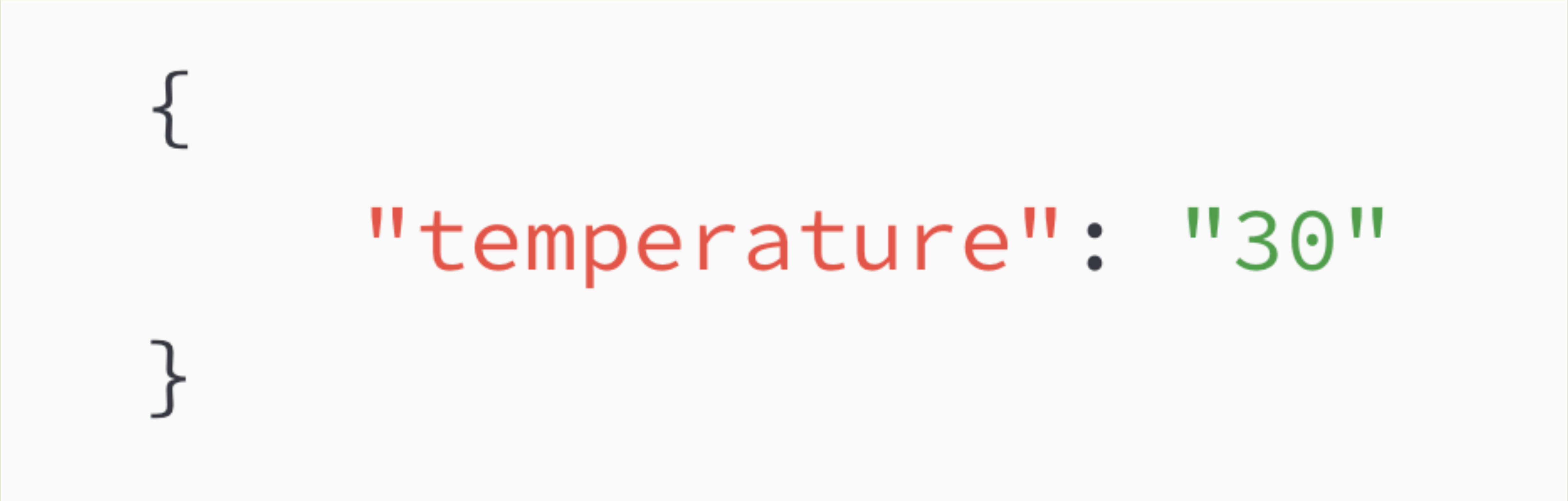
IDENTITY

Decentralized Key Management

Decentralized Identifiers

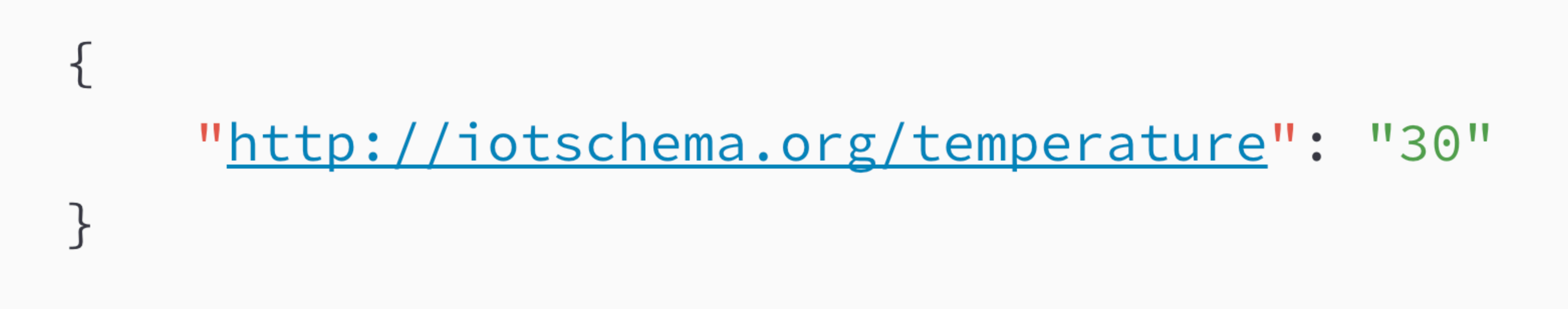
LINKED DATA & JSON-LD

The progress made by the open web community around Linked Data can be applied to IoT,
this brings semantic meaning and relationships to IoT data ...



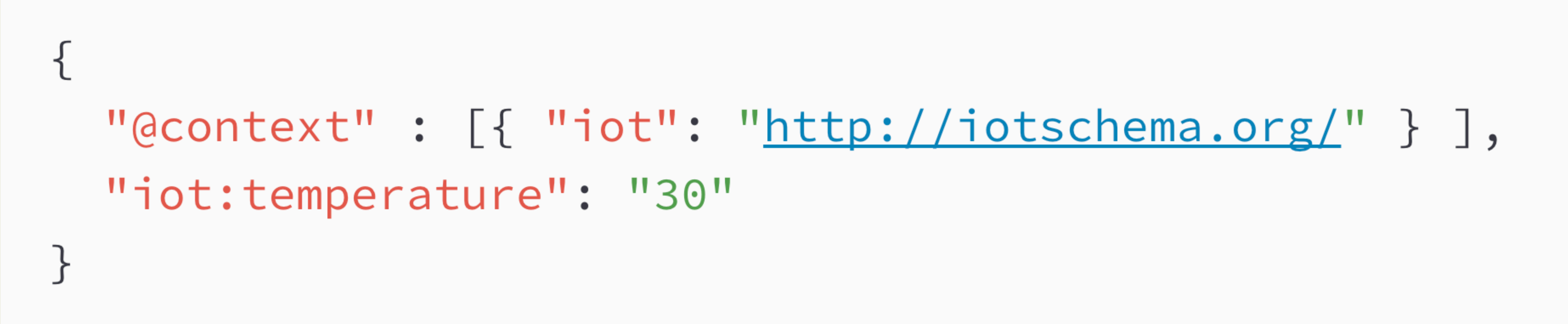
```
{
    "temperature": "30"
}
```

Instead of describing temperature as a key of my choosing “temperature”, “temp” or “T” ...



```
{
      "http://iotschema.org/temperature": "30"
}
```

Let’s describe it with well defined semantics.



```
{
  "@context" : [{ "iot": "http://iotschema.org/" } ],
  "iot:temperature": "30"
}
```

Now, two developers who have never met or coordinated can independently build a temperature sensor and a controller that can work with each other.

SHARED VOCABULARIES

Shared vocabularies enable us to break down the n-squared integration problem that causes a lot of the plumbing we discussed.

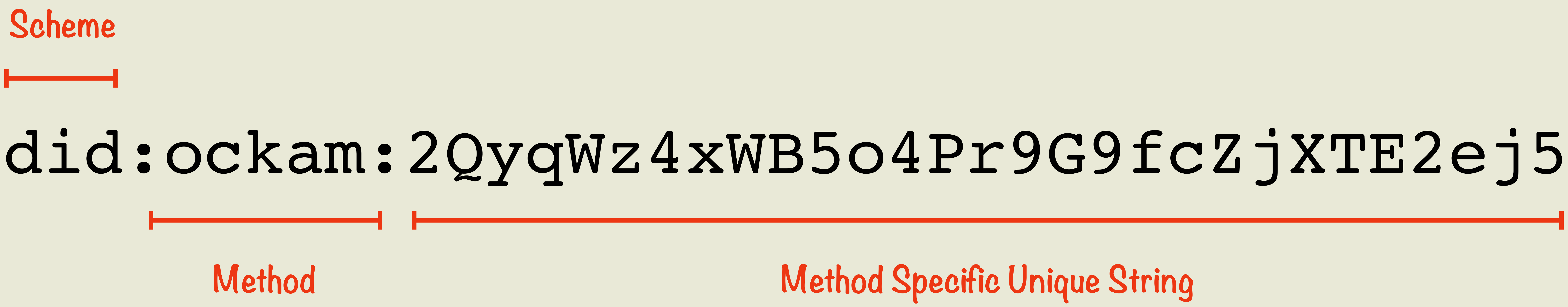
RELATIONSHIPS

Linked Data also enables us to build a relationship graph within our data ...

```
{
  "@context" : [{ "iot": "http://iotschema.org/" } ],
  "iot:temperature": "30",
  "iot:isPropertyOf": "did:ockam:2PZPT7LfPzJjyrTzEjjYhzjq7NX5v"
}
```

Now this data is about an entity (room) described by the above DID.

DECENTRALIZED IDENTIFIERS



Scheme

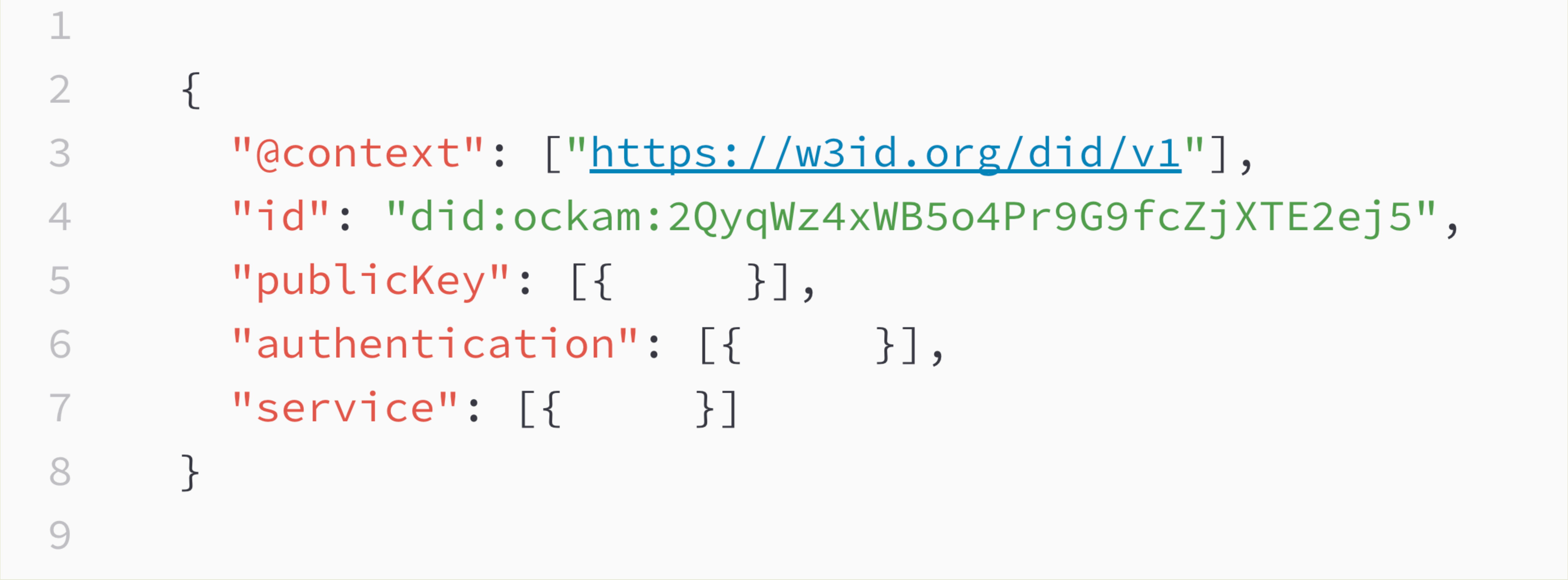
```
did:ockam:2QyqWz4xWB5o4Pr9G9fcZjXTE2ej5
```

Method

Method Specific Unique String

DIDs or Decentralized Identifiers leverage blockchains to enable cryptographically secured IDs that are not locked in silos and can easily interoperate with other entities.

DID DOCUMENTS

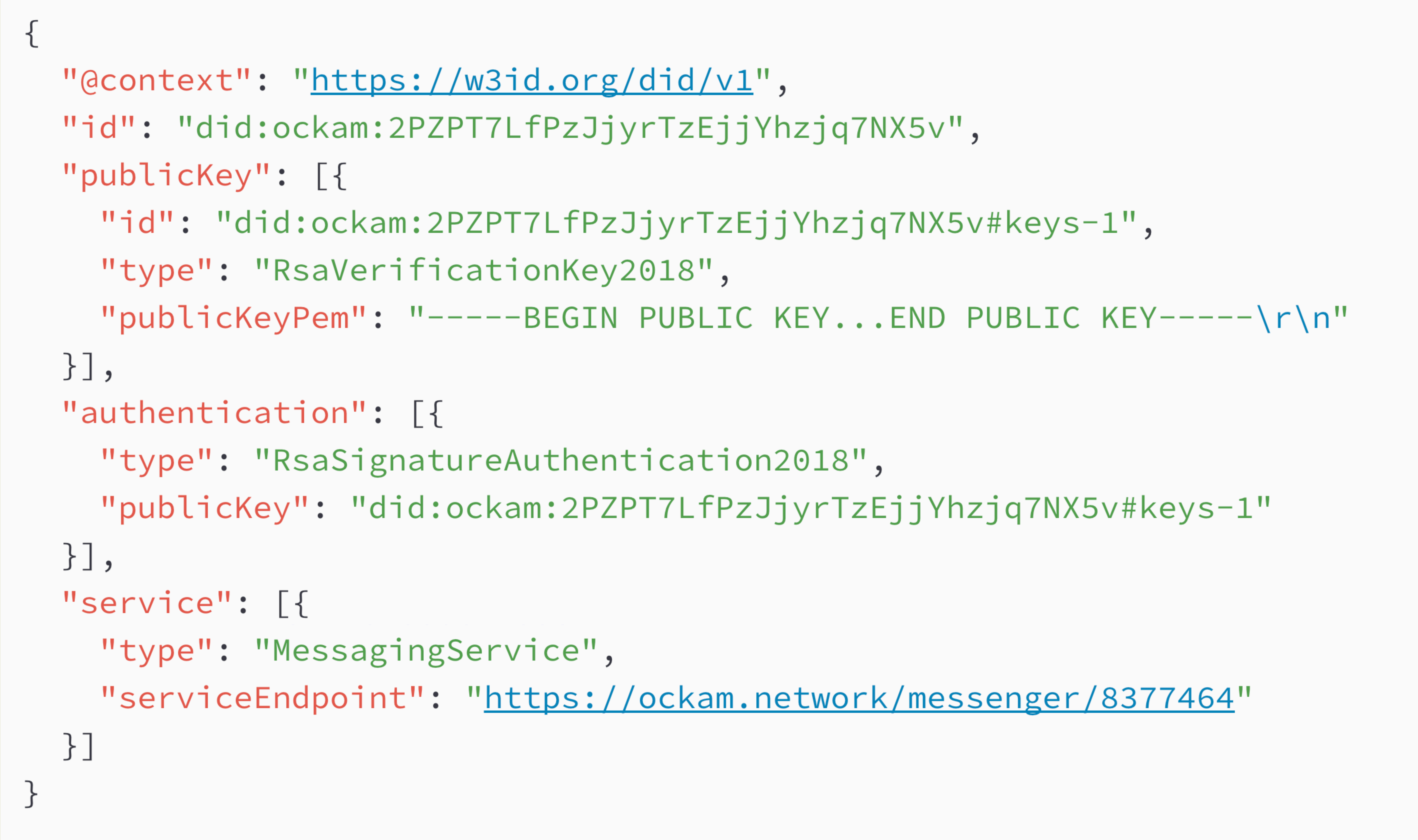


```

{
  "@context": ["https://w3id.org/did/v1"],
  "id": "did:ockam:2QyqWz4xWB5o4Pr9G9fcZjXTE2ej5",
  "publicKey": [{     }],
  "authentication": [{     }],
  "service": [{     }]
}

```

DID Documents are Linked Data documents that describe the DID, they contain the public keys of the DID, authentication methods, services etc...



```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:ockam:2PZPT7LfPzJjyrTzEjjYhzjq7NX5v",
  "publicKey": [{
    "id": "did:ockam:2PZPT7LfPzJjyrTzEjjYhzjq7NX5v#keys-1",
    "type": "RsaVerificationKey2018",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "authentication": [{
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:ockam:2PZPT7LfPzJjyrTzEjjYhzjq7NX5v#keys-1"
  }],
  "service": [{
    "type": "MessagingService",
    "serviceEndpoint": "https://ockam.network/messenger/8377464"
  }]
}
```

GLOBALLY RESOLVABLE

If you have a DID string, you can resolve it to its DID Document via its Method.
We did not have this property of global uniqueness/resolvability **across systems** with old ID schemes like UUID etc.
This breaks silos.

CRYPTOGRAPHICALLY VERIFIABLE OWNERSHIP

DIDs are tied to public keys, you can prove ownership of an ID if you have the corresponding private key.
This enables cryptographically secure identities.

DECENTRALIZED KEY MANAGEMENT

The public keys tied to a DID can be rotated, revoked etc. DID on a blockchain enable a decentralized public key infrastructure.
IOT companies no longer need to spend millions on centralized PKIs that are often single points of failure.

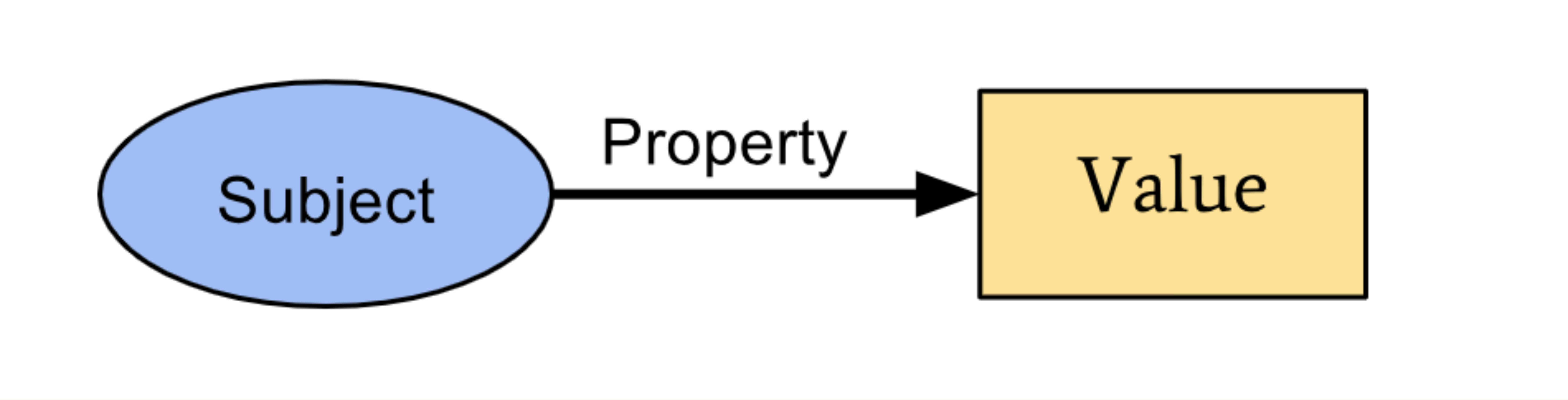
PRIVACY BY DESIGN

DIDs enable privacy in several ways, for example one device can easily generate lots of pair-wise-unique DIDs

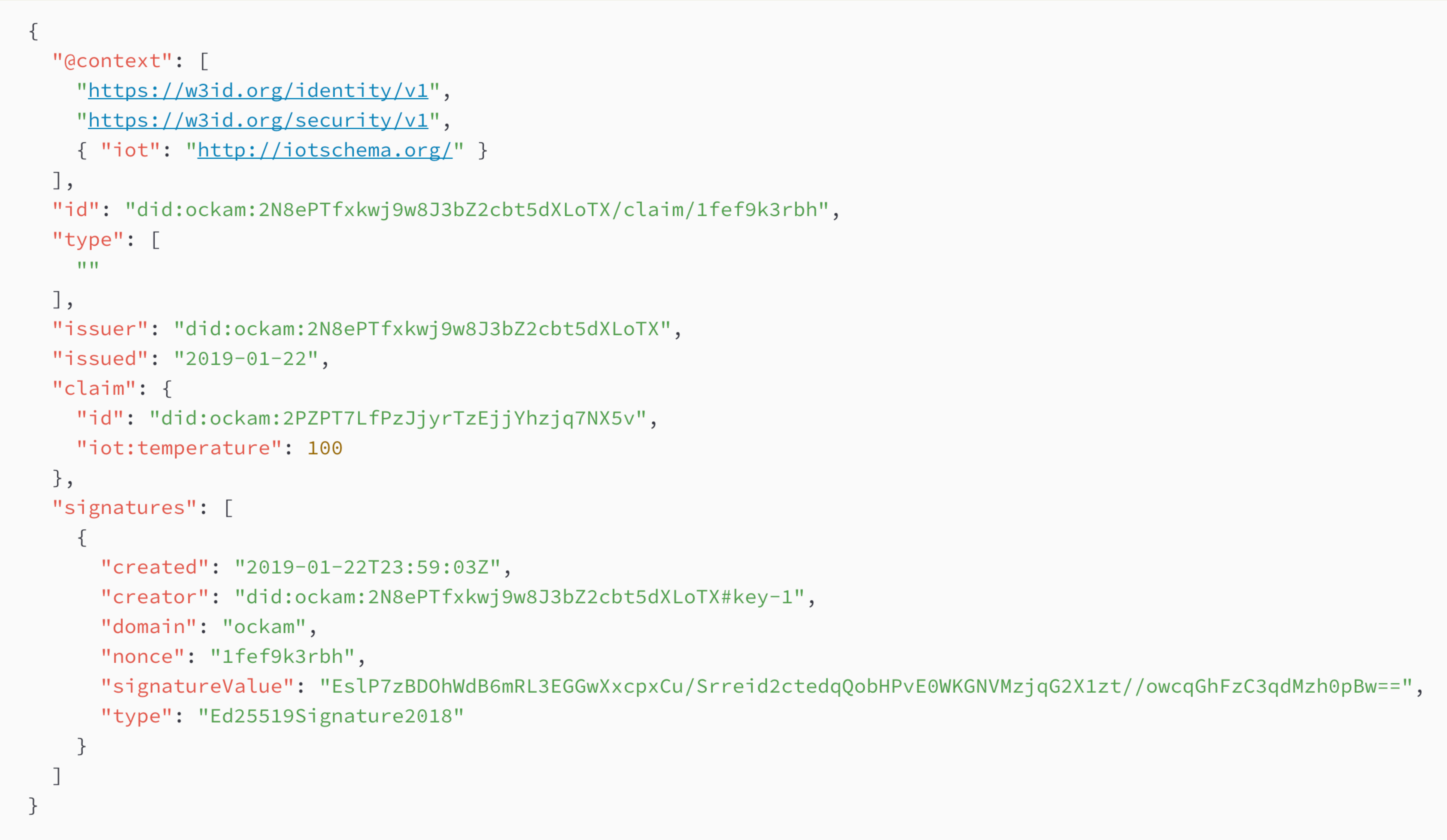
SERVICE DISCOVERY

The service section of the DID document enables de-coupling of systems.

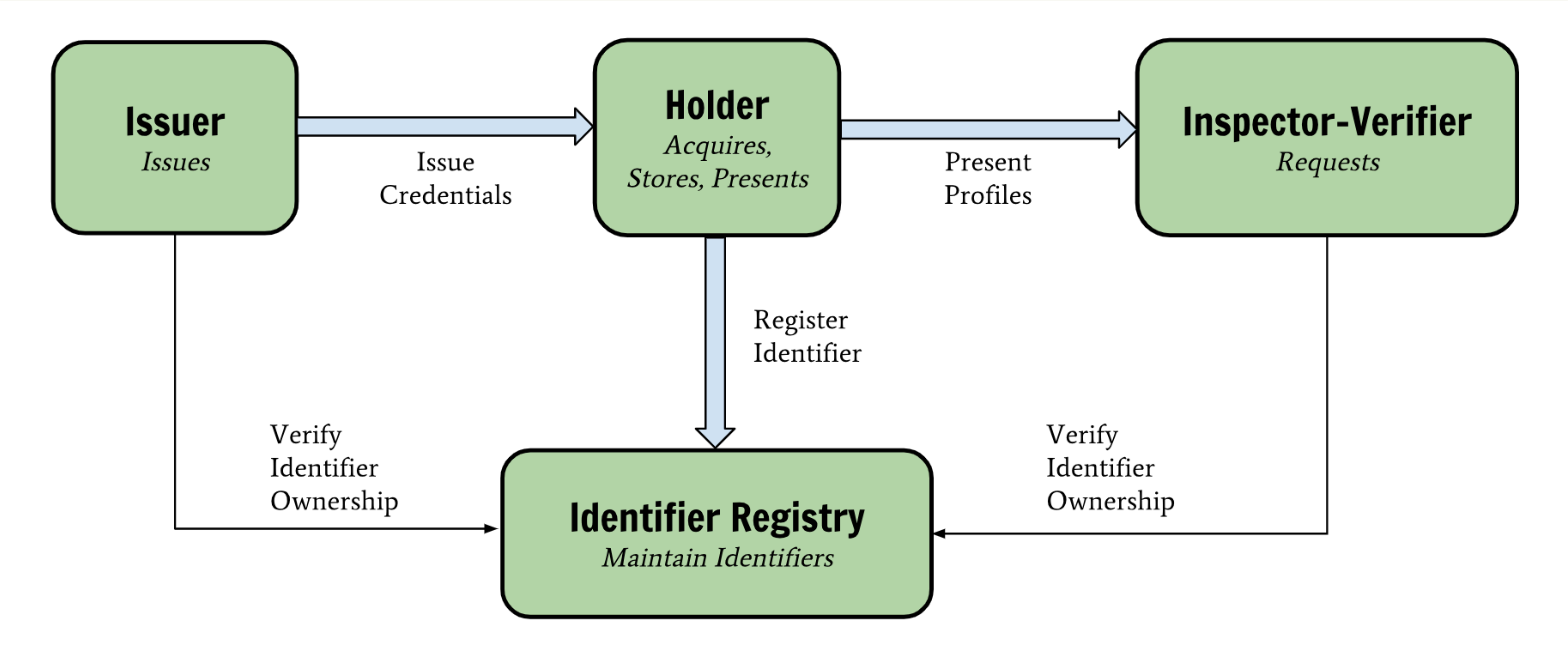
VERIFIABLE CLAIMS



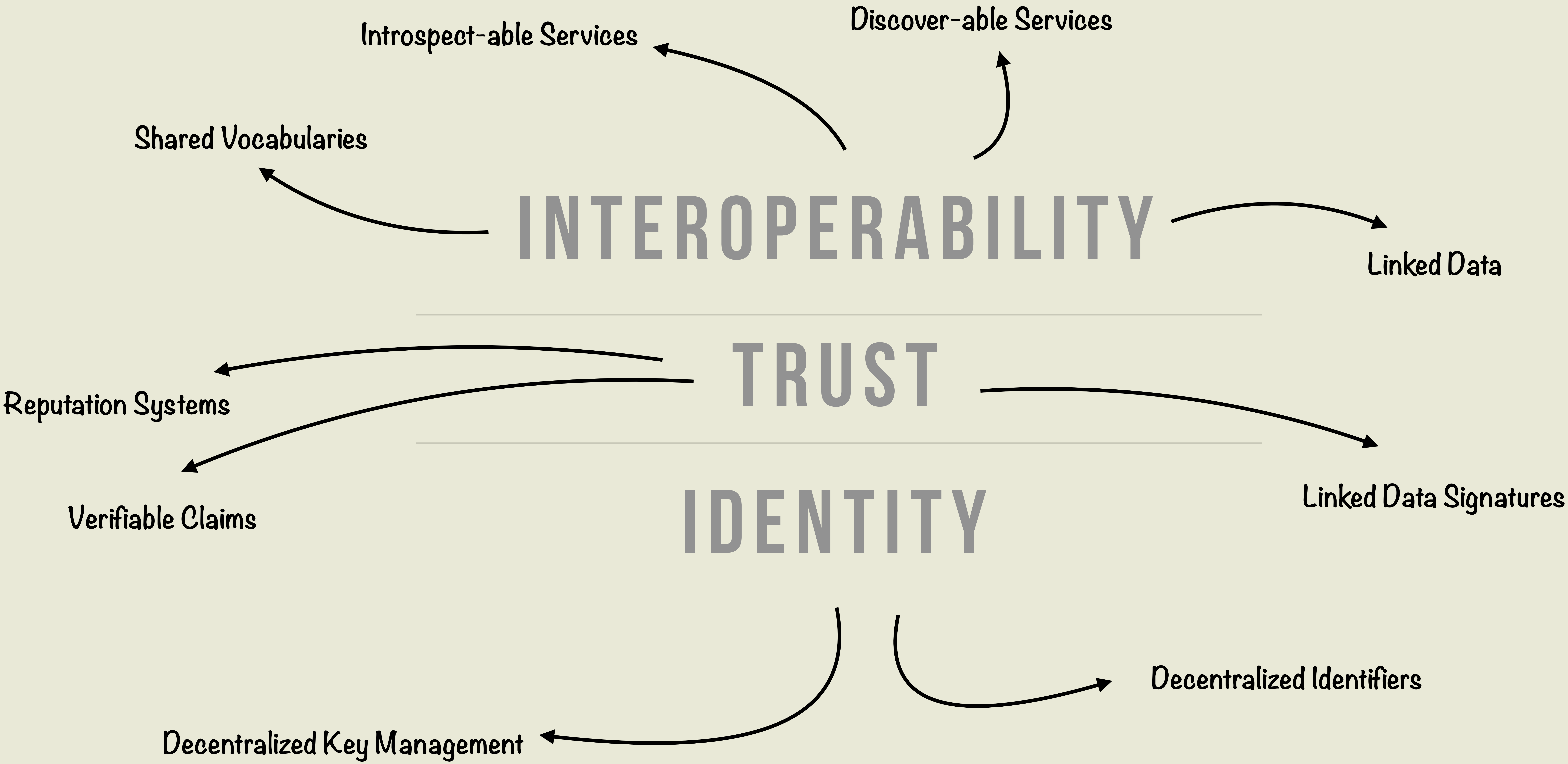
An Issuer can **cryptographically sign** claims about a subject.



```json
{
  "@context": [
    "https://w3id.org/identity/v1",
    "https://w3id.org/security/v1",
    { "iot": "http://iotschema.org/" }
  ],
  "id": "did:ockam:2N8ePTfxkwj9w8J3bZ2cbt5dXLoTX/claim/1fef9k3rbh",
  "type": [
    ""
  ],
  "issuer": "did:ockam:2N8ePTfxkwj9w8J3bZ2cbt5dXLoTX",
  "issued": "2019-01-22",
  "claim": {
    "id": "did:ockam:2PZPT7LfPzJjyrTzEjjYhzjq7NX5v",
    "iot:temperature": 100
  },
  "signatures": [
    {
      "created": "2019-01-22T23:59:03Z",
      "creator": "did:ockam:2N8ePTfxkwj9w8J3bZ2cbt5dXLoTX#key-1",
      "domain": "ockam",
      "nonce": "1fef9k3rbh",
      "signatureValue": "EslP7zBDOhWdB6mRL3EGGwXxcpxCu/Srreid2ctedqQobHPvE0WKGNVMzjqG2X1zt//owcqGhFzC3qdMzh0pBw==",
      "type": "Ed25519Signature2018"
    }
  ]
}
```



DIDs + Verifiable Claims + Blockchain gives cryptographically signed IoT data that cannot be tampered with in motion or at rest.



INTEROPERABILITY

TRUST

IDENTITY

Introspect-able Services

Discover-able Services

Shared Vocabularies

Linked Data

Reputation Systems

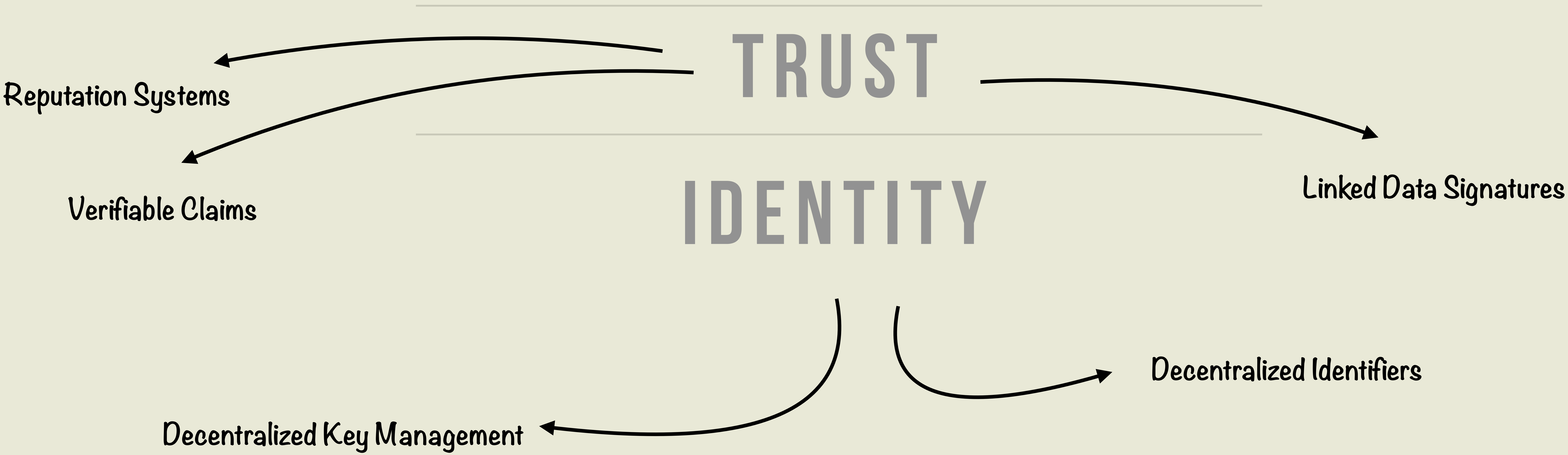
Verifiable Claims

Linked Data Signatures

Decentralized Identifiers

Decentralized Key Management

Blockchains are a new way to implement identity and trust, in IoT systems, that unlocks interoperability in powerful ways.



TRUST

IDENTITY

Reputation Systems

Verifiable Claims

Linked Data Signatures

Decentralized Key Management

Decentralized Identifiers

Code: github.com/ockam-network/ockam

Slack: bit.ly/2CXw4PD

Come contribute to Ockam on Github or Slack w3.org/community/credentials

Shout out to the w3c credentials group that is developing many of these powerful standards.

Ockam

Mrinal Wadhwa
CTO & Co-Founder

@mrinal

Attributions for the images used in this deck:

- pipes by Aleksandr Vector from the Noun Project
- valve by Ben Davis from the Noun Project
- Robot by Vectors Market from the Noun Project