Decentralized Identifier WG FF2F Sessions - TPAC Edition

Day 1: November 2, 2020
Chairs: Brent Zundel, Dan Burnett
Location: Cyberspace

Welcome!

- Logistics
- W3C WG IPR Policy
- Agenda
- IRC and Scribes
- Status
- Timeline Reminder

Logistics

- **Zoom call:**
  - See https://lists.w3.org/Archives/Member/member-did-wg/2020Jun/0000.html for dial in information (member only link)
- **Meeting times**:
  - Monday Nov 2: 10:00 - 13:30 EST (16:00 - 19:30 CET, 07:00 - 10:30 PDT, 23:00 - 02:30 JST)
  - Tuesday Nov 3: 12:00 - 15:30 EST (18:00 - 21:30 CET, 09:00 - 12:30 PDT, 01:00 - 04:30 JST)
  - Wednesday Nov 4: 10:00 - 13:30 EST (16:00 - 19:30 CET, 07:00 - 10:30 PDT, 23:00 - 02:30 JST)
  - Thursday Nov 5: 12:00 - 15:30 EST (18:00 - 21:30 CET, 09:00 - 12:30 PDT, 01:00 - 04:30 JST)
- **DID WG Agenda**: https://tinyurl.com/yydapmu3
- **Live slides**: https://tinyurl.com/yyc5fu63 (Google Slides)
- **Breakout Room**: https://zoom.us/j/97932508552?pwd=REFrMXF0NVBreTBhN0IzTVhYYS94Zz09

W3C WG IPR Policy

- This group abides by the W3C patent policy https://www.w3.org/Consortium/Patent-Policy-20040205
- Only people and companies listed at https://www.w3.org/2004/01/pp-impl/117488/status are allowed to make substantive contributions to the specs
- Code of Conduct https://www.w3.org/Consortium/cepc/

Today’s agenda

10:00		
10:00	Welcome, Introductions, Status, and Logistics	Brent
10:30	Steps to CR	Dan Burnett
11:30	Break	
12:00	Avoiding Privacy Violating Properties	Drummond
1:00	Avoiding Privacy Violating Properties - Part 2 OR Open Issues	Drummond / Editors

IRC and Scribes

- Meeting discussions will be documented
  - Text Chat: http://irc.w3.org/?channels=did
  - IRC://irc.w3.org:6665/#did
- Telecon info
  - https://lists.w3.org/Archives/Member/member-did-wg/2020Jun/0000.html

	Monday	Tuesday	Wednesday	Thursday
1	Markus	Drummond	Manu	Drummond
2	Amy	Amy	Wayne (12 pm et onwards)	Amy

<JoeAndrieu> q+ to comment on biometrics
<brent> ack JoeAndrieu
<Zakim> JoeAndrieu, you wanted to comment on biometrics

DID WG Mission and Goals

- “… standardize the DID URI scheme, the data model and syntax of DID Documents, which contain information related to DIDs that enable the aforementioned initial use cases, and the requirements for DID Method specifications.”

Charter Deliverables and Status

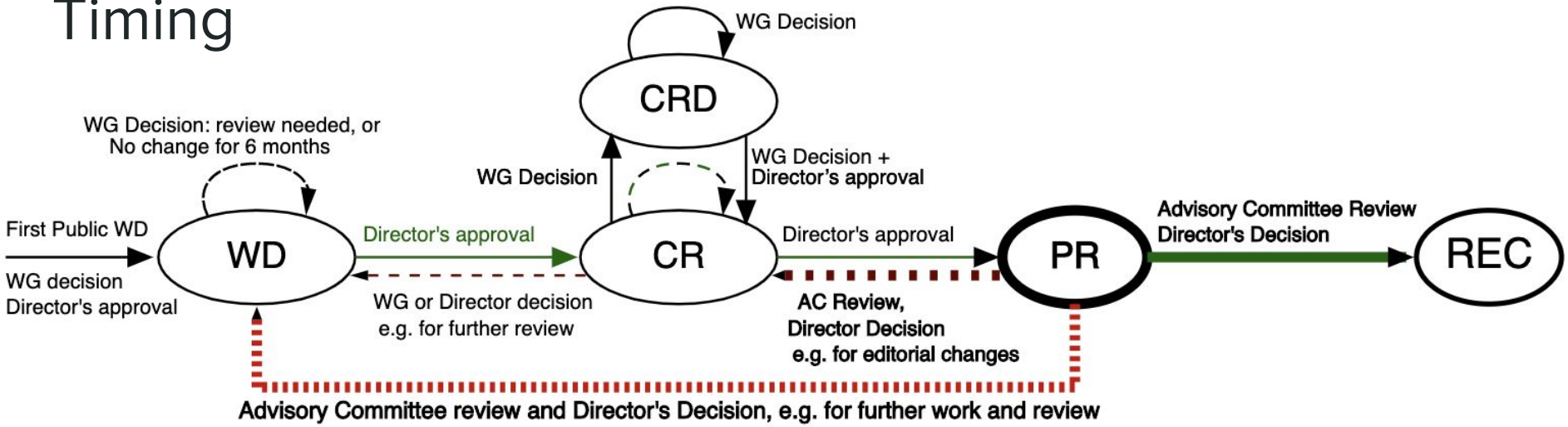
- Recommendation-track Specification
  - Decentralized Identifiers v1.0 (DID Core)
    - A couple of big issues to discuss this week, lots of little stuff to wrap up
- W3C Notes
  - Decentralized Identifier Use Cases v1.0
    - Infinitesimally close to done. Maybe this week?
  - Decentralized Characteristics Rubric v1.0
    - We will discuss Thursday if time permits
- Other Deliverables
  - DID Registries
    - Steady progress; most issues depend on DID Core work
  - Test Suite and Implementation Report
    - There will be a demonstration and work session this week

W3C Technical Report Process

- Working Draft (WD) - does not imply consensus
- Candidate Recommendation (CR)
  - Entry - to publish as CR, the document is expected to be feature complete, have had wide review, and must specify the implementation requirements needed to exit
  - Exit - to exit CR (and move to PR), the document must satisfy the stated implementation requirements; it must also not have made any substantive change not warned about upon entry
- Proposed Recommendation (PR)
  - Basically a one-month sanity check during which the AC is encouraged to have any final review and discussion, but if anything major happens it’s a fail (requiring a move back to CR or earlier)
- Recommendation - Done
  - But errata are possible

https://www.w3.org/2020/Process-20200915/

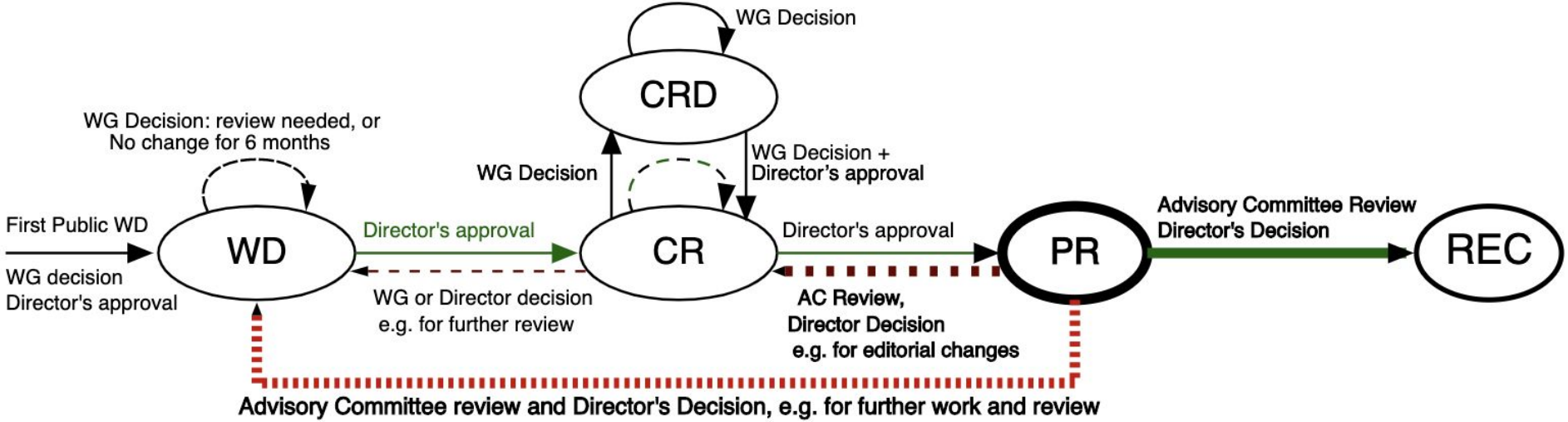
Timing

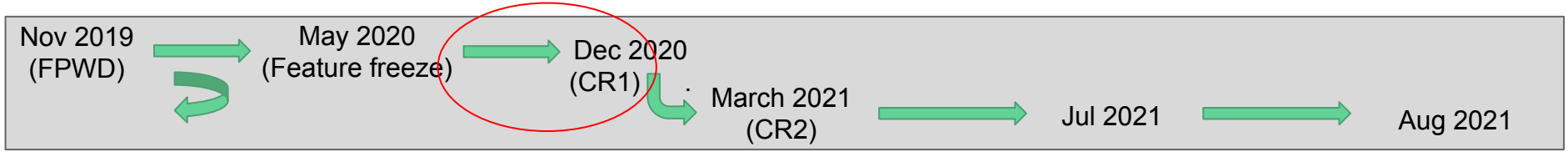


2.3 Timeline

Specification	FPWD	CR	PR	Rec
Decentralized Identifier Use Cases & Requirements (NOTE)	November 2019			August 2021
Decentralized Characteristics Rubric (NOTE)	December 2019			September 2021
Decentralized Identifiers Data Model and Syntax(es)	November 2019	November 2020	July 2021	August 2021
Note: The group will document significant changes from this initial schedule on the group home page.				

Timing of our primary spec





Decentralized Identifiers Data Model and Syntax(es)	November 2019	November 2020	July 2021	August 2021

https://www.w3.org/2019/Process-20190301/

Goals for this meeting

- Make clear what work remains before we can go to CR
- Resolve all major outstanding issues (ADM and privacy concerns)
- Resolve 25% of remaining issues

Steps to CR (Chairs, 60 min)

Steps to CR

- CR requirements described in
  - Process 2020 (https://www.w3.org/2020/Process-20200915/)
  - Pubrules (https://www.w3.org/pubrules/)
  - Guide (https://www.w3.org/Guide/transitions?profile=CR&cr=new)
- From https://www.w3.org/2020/Process-20200915/
  - *Advancing to Candidate Recommendation indicates that the document is considered complete and fit for purpose, and that no further refinement to the text is expected without additional implementation experience and testing; additional features in a later revision may however be expected. A Candidate Recommendation is expected to be as well-written, detailed, self-consistent, and technically complete as a Recommendation, and acceptable as such if and when the requirements for further advancement are met.*
  - *The first Candidate Recommendation publication after approval of a Transition Request is always a Candidate Recommendation Snapshot.*

Requirements for CR (Part I - Group)

- Document prep
  - * Complete Wide Review (incl. Horizontal Review)
  - * Formally address all issues raised about the document since the previous maturity level.
  - Publicly document all new features (class 4 changes) to the technical report since the previous publication.
  - Publicly document any other substantive changes (class 3 changes).
  - Optionally publicly document if editorial changes have been made.
  - Optionally identify features in the document as at risk. These features may be removed before advancement to Proposed Recommendation without a requirement to publish a new Candidate Recommendation.
  - Document how adequate implementation experience will be demonstrated
  - Specify the deadline for comments, which must be at least 28 days after publication, and should be longer for complex documents
- Group decision to request advancement.

Requirements for CR (Part II - Editors and Chairs)

- Request transition
  - Publicly document any Formal Objections.
  - Show that the specification has received wide review
  - Report which, if any, of the Working Group's requirements for this document have changed since the previous step.
  - Show that the specification has met all Working Group requirements, or explain why the requirements have changed or been deferred
  - Report any changes in dependencies with other groups.
  - Provide information about implementations known to the Working Group.
- Approvals (Min. 1-2 weeks after group decision)
  - If needed, schedule and hold a formal review meeting with Director to ensure the requirements have been met before Director's approval is given.
  - Director approval.
- Publication (Min. 1-2 weeks after approvals)

Break (30 min)

Avoiding Privacy-Violating Properties (Drummond, 60-90 mins)

Motivation for this session

- The editors believe there is general WG consensus that privacy is a paramount consideration for the DID Core spec
- Thus we propose to apply the following general principle throughout the spec:

DID method specifications and DID controllers SHOULD NOT use privacy-violating properties in publicly available DID documents

Structure of this session

1. Part One
    a. Discuss any concerns about this overall privacy stance
    b. Seek consensus on specific proposed wording in the spec
    c. Assign action items
2. Part Two (assuming there is time)
    a. Discuss several other privacy issues
    b. Work on wording (if there is time)
    c. Assign action items

Part One: Privacy-Violating Properties

What this would mean for the ‘type’ property

1. We would no longer specify a ‘type’ property in DID Core
2. Since DID documents use an open world data model, any DID method specification or DID controller has the ability add any property they want
3. So the issue is larger than just the ‘type’ property—it applies to any privacy-violating property
4. Amy has proposed the following language in PR 444 (including a few enhancements from Brent and Drummond)

10.x Avoiding Privacy-Violating Properties in Public DID Documents

It is dangerous to add properties to a publicly-accessible DID document that can be used to indicate, explicitly or through inference, what type or nature of thing the DID subject is, particularly if the DID subject is a person.

Not only do such properties potentially result in personally identifiable information or correlatable data being present in the DID document, but they can be used for grouping particular DIDs in such a way that they could be included in or excluded from certain operations or functionalities.

Including information about the type or nature of a DID subject in a public DID document could result in personal privacy harms even if the DID subject is a non-person entity (NPE), such as an IoT device. The aggregation of such information around a DID controller could serve as a form of digital fingerprint and so is best avoided.

To minimize these risks, properties in a public DID document should only be used for expressing cryptographic material, services, or verification methods related to using the DID.

Decisions & Action Items - Part One

- Do we have closure on this wording (modulo review of the revised PR)? Yes
- Should we include this text as its own subsection under Privacy Considerations?
  - Currently there are 4 subsections, this will be a 5th
- Action items:
  - Amy: update her PR 444
  - Consider how we would also cover service endpoints in more depth in this PR or elsewhere in the Privacy Considerations section
  - Consider providing guidance about how DID methods can be designed to incorporate policies to restrict the properties they allow in a DID document

Part Two: Other Privacy Issues

Current List of Other Privacy Issues

1. PII (personally-identifiable information) in DID documents
2. GDPR and the “right to be forgotten”
3. Persistence
4. Biometrics
5. Notarization—moving from pseudonymous to identifiable
6. Definition of publicly-available DID documents & potential privacy risks of VCs based on that DID
7. Others?

#1: PII in DID documents

- We already have text in the Privacy Considerations section for this
- The issues are:
  - Is this text still accurate?
  - Does it need to be revised based on our other decisions about privacy?

10.1 Keep Personally-Identifiable Information (PII) Private

If a DID method specification is written for a public verifiable data registry where all DIDs and DID documents are publicly available, it is *critical* that DID documents contain no personal data. All personal data should be kept behind service endpoints under the control of the DID subject. Additional due diligence should be taken around the use of URLs in service endpoints as well to prevent leakage of unintentional personal data or correlation within a URL of a service endpoint. For example, a URL that contains a username is likely dangerous to include in a DID Document because the username is likely to be human-meaningful in a way that can unintentionally reveal information that the DID subject did not consent to sharing. With this privacy architecture, personal data can be exchanged on a private, peer-to-peer basis using communications channels identified and secured by public key descriptions in DID documents. This also enables DID subjects and requesting parties to implement the GDPR right to be forgotten, because no personal data is written to an immutable distributed ledger.

#2: The GDPR “right to be forgotten” issue

- The definition of personal data under GDPR is very broad

  ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The question at the heart of the issue

- Can <u>any</u> DID whose DID subject is a natural person be written to an immutable ledger, i.e., a distributed database whose cryptographic security depends on the immutability of all of the transactions written to the database—and still satisfy the GDPR right of erasure?

Options for resolving this issue

1. Warn against recording any DID whose subject is a natural person (“NP DID”) on an immutable ledger
2. Recommend that any DID method specification that supports recording an NP DID on an immutable ledger seek regulatory approval first
3. Specify how a natural person controlling their own NP DID has “an effective right of erasure” - could be by dissociating a DID from the person - make the point that the DID spec fundamentally supports people having more control over their data - we can follow the pattern of VCs with proof of control
4. Treat DIDs linked to a VDR the way we treat Bitcoin addresses.
5. Other options?

#3: Persistence

- The spec currently states all DIDs are persistent identifiers (effectively URNs—Uniform Resource Names)
- However in practice all DIDs are only as persistent as:
  - Their DID controller chooses
  - The underlying DID method is able to support
- Therefore should we revise our language wrt persistence?

Persistence—current language from section 3.1

A DID is expected to be persistent and immutable. That is, a DID is bound exclusively and permanently to its one and only subject. Even after a DID is deactivated, it is intended that it never be repurposed.

Ideally, a DID would be a completely abstract decentralized identifier (like a UUID) that could be bound to multiple underlying verifiable data registries over time, thus maintaining its persistence independent of any particular system. However, registering the same identifier on multiple verifiable data registries makes it extremely difficult to identify the authoritative version of a DID document if the contents diverge between the different verifiable data registries. It also greatly increases implementation complexity for developers.

To avoid these issues, developers should refer to the Decentralized Characteristics Rubric [DID-RUBRIC] to decide which DID method best addresses the needs of the use case.

Persistence—possible new language

The persistence of a DID, i.e., the ability for it to continue to identify the same DID subject over time, is a function of: a) the DID controller, and b) the DID method. While DID architecture is designed to enable a DID to be permanently bound to one DID subject for all time, there are two important caveats: 1) the DID controller may wish to terminate this binding—or possibly even bind the DID to a different DID subject, and 2) even if a permanent binding is desired, maintaining this binding is dependent on the infrastructure required by the DID method.

With regard to (1), requesting parties are advised not to make assumptions about the permanence of the binding of a DID to a DID subject in the absence of DID assignment policies specified by the DID controller and consistent with the DID method.

With regard to (2), DID controllers should refer to the Decentralized Characteristics Rubric [DID-RUBRIC] to decide which DID method best addresses their needs for persistence.

Decisions & Action Items - Part Two

- Decisions wrt PII in DID documents text?
  - More explanation of service endpoint types—decide normatively first
  - Update “DID subject to DID controller”
  - Add a separate PR about migration of DID docs from private to public
  - Ensure strong warning about encrypted data in a public DID doc
- Decision wrt GDPR right to be forgotten issue?
  - No resolution yet but great suggestions
- Decision wrt persistence text?
  - Identifiers are contextual
  - Proposal to use language on slide 34 as a starting point for revision
- Action items:
  - Drummond to prepare PR

End of Day 1

Decentralized Identifier WG Virtual Face-to-Face meeting

Day 2: November 3, 2020
Chairs: Brent Zundel, Dan Burnett
Location: The World Wide Web

Today’s agenda

12:00		
12:00	Review and Agenda	Brent
12:15	Unregistered properties and the ADM	Manu / Markus
13:30	Break	
14:00	DIDs in use today - DIDcomm	D. Hardman
14:30	Meeting with TAG	Chairs
15:00	Prep for Horizontal Review - Privacy and Security	Editors

The Abstract Data Model

Unregistered Properties

(Manu and Markus, 75 min)

Why are we having this session?

It is now clear that the Amsterdam Face-to-Face meeting, where we decided to create the DID Spec Registries, led to a number of hand waves and miscommunications on the purpose of the registry and what it is capable of doing. There are similar issues with the Abstract Data Model.

Resolution from the last F2F [Markus]

1. The DID Core specification will define an **abstract data model** that can be **cleanly represented** in at least JSON, JSON-LD, and CBOR. There will also be a graphical depiction of the abstract data model. **There must be lossless conversion between multiple syntaxes** (modulo signatures and verification).
2. In general, the registry mechanism is the one that will be used for globally interoperable extensions.
3. The governance of the registry mechanism will be defined by the W3C DID Working Group.
4. Extension authors must provide references to specifications for new entries and **a valid JSON-LD Context to be associated with each entry to ensure lossless conversion between serializations** for both producers and consumers. This is partly being done to ensure semantic interoperability.

Lossless conversion [Markus]

```
{
  "@context": ["https://www.w3.org/ns/did/v1",
  "https://identity.foundation/EcdsaSecp256k1RecoverySignature2020"],
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "EcdsaSecp256k1RecoveryMethod2020",
    "ethereumAddress": "0xF3beAC30C498D"
  }],
  "service": [{
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "AgentService",
    "serviceEndpoint": "https://test.com/a/"
  }]
}
```

application/did+ld+json

```
{
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "EcdsaSecp256k1RecoveryMethod2020",
    "ethereumAddress": "0xF3beAC30C498D"
  }],
  "service": [{
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "AgentService",
    "serviceEndpoint": "https://test.com/a/"
  }]
}
```

application/did+json

§ **4.4.1 ethereumAddress**

Normative Definition	JSON-LD	CBOR
ESRS2020		esrs2020

EXAMPLE 12: Example of ethereumAddress property

```
{
```

```
{
  "@context": {
    "@version": 1.1,
    "esrs2020": "https://identity.foundation/EcdsaSecp256k1RecoverySignature2020#",
    "publicKeyHex": "esrs2020:publicKeyHex",
    "privateKeyHex": "esrs2020:privateKeyHex",
    "ethereumAddress": "esrs2020:ethereumAddress"
  }
}
```

Lossless conversion [Markus]

produce

consume

```
62a2 6469 646f 6469 653a 6178 706d 656c
313a 3332 7672 7265 6669 6369 7461 6f69
4d6e 7465 6f68 8164 62a4 6469 2366 656b
2d79 6430 7974 6570 1a78 6445 3532 3135
5639 7265 6669 6369 7461 6f69 4b6e 7965
3032 3831 636a 6e6f 7274 6c6f 656c 6f72
```

application/did+cbor

produce

consume

```
{
  "@context": ["https://www.w3.org/ns/did/v1",
    "https://identity.foundation/EcdsaSecp256k1RecoverySignature2020"],
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2018",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVA"
  }, {
    "id": "did:example:123456789abcdefghi#keys-2",
    "type": "EcdsaSecp256k1RecoveryMethod2020",
    "ethereumAddress": "0xF3beAC30C498D"
  }],
  "service": [{
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "AgentService",
    "serviceEndpoint": "https://test.com/a/"
  }]
}
```

application/did+ld+json

produce

consume

```
{
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2018",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVA"
  }, {
    "id": "did:example:123456789abcdefghi#keys-2",
    "type": "EcdsaSecp256k1RecoveryMethod2020",
    "ethereumAddress": "0xF3beAC30C498D"
  }],
  "service": [{
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "AgentService",
    "serviceEndpoint": "https://test.com/a/"
  }]
}
```

application/did+json

Goals for this session

1. Come to consensus on the revised purpose of the registry now that it can be proven that it can't do what some in the group wanted it to do (e.g., under certain scenarios, it is mathematically impossible to use it to construct certain properties like @context).

2. Come to consensus on whether properties are solely about the DID Subject, or if they can be about other things (e.g., the proof property).

3. Come to consensus on whether preserve-by-default applies to all properties in the abstract data model.

4. Come to consensus on whether implementers are allowed to "clean up" the abstract data model before an application uses it to "perform further processing higher up the stack".

Oversight: Add Representations to DID Spec Registries

The specification currently does not tell you how to add a new representation. This means that you have to modify DID Core to add a new representation, which will be difficult to do once DID Core is a standard.

Oops.

PROPOSAL: The DID Spec Registries MUST contain a section on Representations to enable future representations to be registered in an extensible manner. The DID Core specification MUST specify how this extensibility mechanism works as well as the requirements on representation specifications.

Clarify: The definition of a Property

Are properties solely about the DID Subject or can they be about other things (e.g., the proof property, the unknown foo property)?

PROPOSAL: A property in the Abstract Data Model can be any information expressed in the DID Document. Properties are often, but not exclusively, about the DID Subject.

"Properties" [Markus]

- From the metadata discussion:
  - "Data **about the DID subject**" -> "DID document"
  - "Metadata **about the DID and DID document**" -> "DID document metadata"
  - "Metadata **about a DID resolution process**" -> "DID resolution metadata"
- From various issues and PRs:
  - "The DID document is a collection of properties describing the DID subject".
  - "The DID document is just the name for a set of properties about the DID subject."
  - "These properties have the DID subject as their subject".
- From the spec:
  - § 4.1 Definition. A DID document consists of a **map of properties** [...] The definitions of each of these properties are specified in section § 5. Core Properties.
  - § 5. Core Properties. **These properties describe relationships between the DID subject and the value of the property.**

"Properties" [Markus]

```
«[
  "id" → `did:example:123`,
  "verificationMethod" → «[
    "id" → `#key-0`,
    "type" → `EcdsaSecp256k1RecoveryMethod2020`,
    "controller" → `EcdsaSecp256k1RecoveryMethod2020`,
    "ethereumAddress" → `0xF3beAC`
  ]»
]»
```

Are these "properties" of the "Abstract Data Model" that should be "preserved"?

```
{
  "@context":[
    "https://www.w3.org/ns/did/v1",
    "https://identity.foundation/EcdsaSecp256k1...#"
  ],
  "id": "did:example:123",
  "verificationMethod":[{
    "id": "#key-0",
    "type": "EcdsaSecp256k1RecoveryMethod2020",
    "controller": "did:example:123",
    "ethereumAddress": "0xF3beAC"
  }]
}
```

application/did+ld+json

```
%YAML 1.2
---
  id: "did:example:123"
  verificationMethod:
    -
      id: "#key-0"
      type: "EcdsaSecp256k1RecoveryMethod2020"
      controller: "did:example:123"
      ethereumAddress: "0xF3beAC"
```

text/did+yaml

```
{
  "xmlns": "https://www.w3.org/ns/did/v1",
  "xmlns:sec="https://w3id.org/security#",
"xmlns:esrs2020="https://identity.foundation/Ecd#"
  "id": "did:example:123",
  "sec:verificationMethod": [{
    "id": "#key-0",
    "type": "EcdsaSecp256k1RecoveryMethod2020",
    "sec:controller": "did:example:123",
    "esrs2020:ethereumAddress": "0xF3beAC"
  }]
}
```

application/did+xml

Break (30 min)

DIDs in use today - DIDComm (Daniel Hardman, 30 min)

What is DIDComm?

https://github.com/decentralized-identity/didcomm-messaging

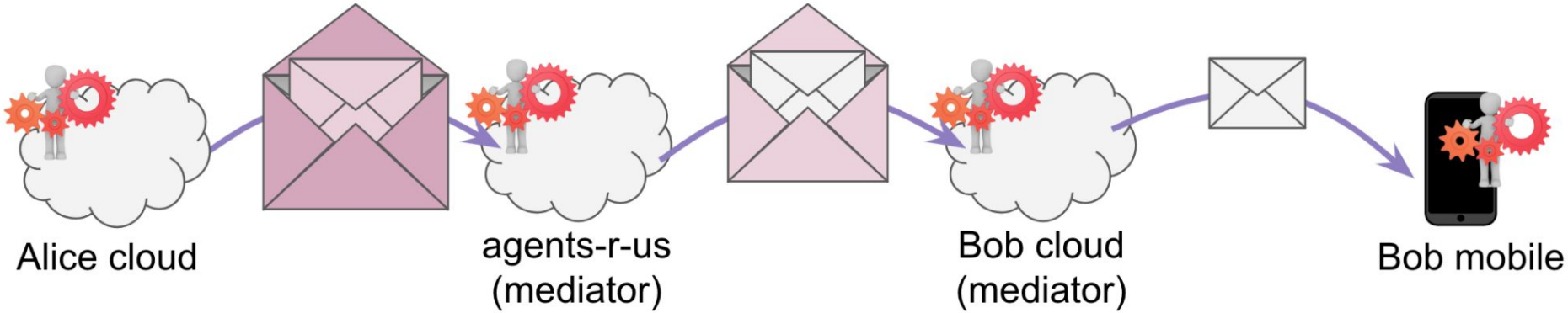
- Method to leverage DIDs into secure comm channels
- V1 production since late 2018; V2 under dev at DIF
- Any DID method
- Any transport: HTTP, file system, email, BlueTooth, CHAPI, AMQP, Kafka, etc
- Think s/mime but with DIDs instead of certs
- Uses JOSE tech:
  - JWM (JWT-like but for arbitrary messages instead of just tokens) — IETF RFC proposal
  - Signs with JWS
  - Authenticated encryption with JWE
- Peer-to-peer: use your DID for authenticated pairwise or n-wise encr
- Broadcast: use your DID to sign a message to the world (QR, mailers, etc)
- Web: client/server with RESTful or similar

How DIDComm Works

service endpoints

routing

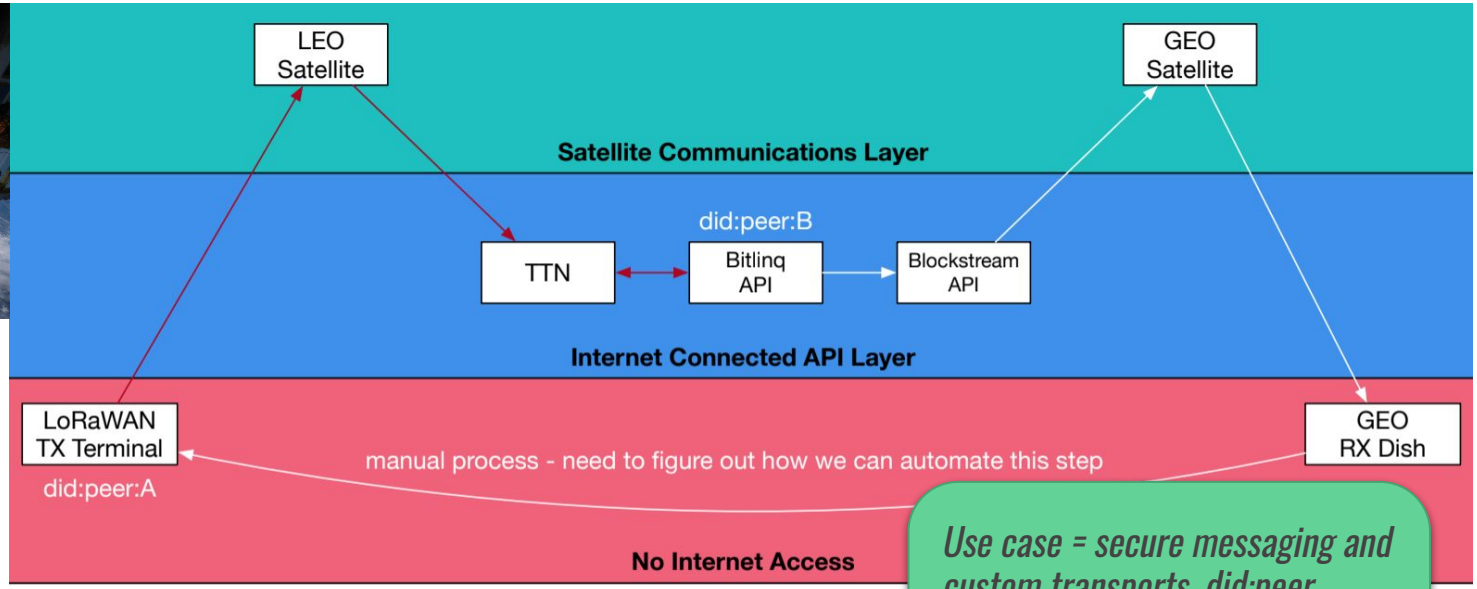
authenticated encryption



Research highlight: DIDx and Low-Earth Orbit Satellites

diddoc = {"@context": "https://w3id.org/did/v1", "publicKey": "5f1f0b987f...d5b553dc6d54", "service": [{"id": "default", "type": "didcomm", "serviceEndpoint": "leogeo:A"}]}

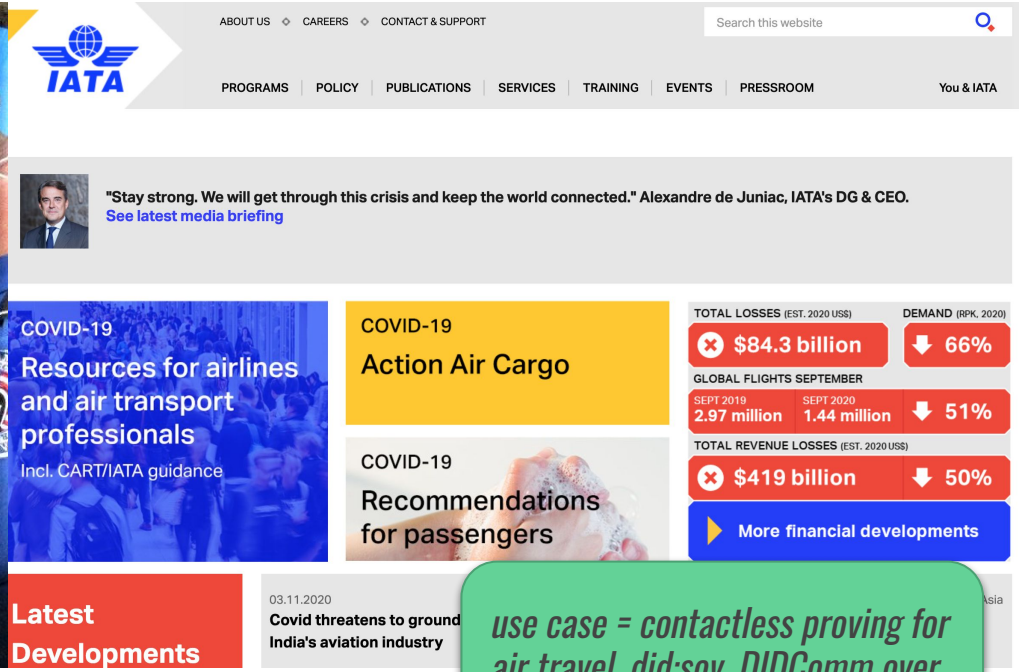
didcomm_message = {"@id": "5678876542345", "@type": "https://didcomm.org/didexchange/1.0/request", "~thread": {"pthid": 1}, "connection": {"did": "did:peer:1z6awaAJ2DaHcbaRiMz6BeEvDH99E13mFUKsBnLi4EmNScN",



Use case = secure messaging and custom transports. did:peer, custom transport, no internet, very low bandwidth and high latency.

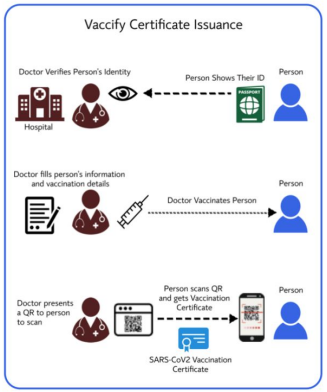
Pilot Highlight: IATA

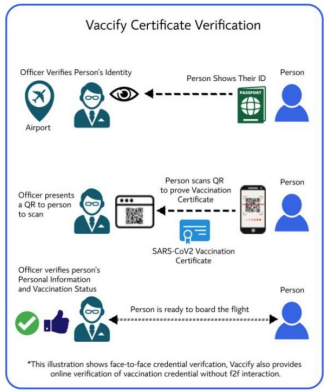
contactless proving for air travel

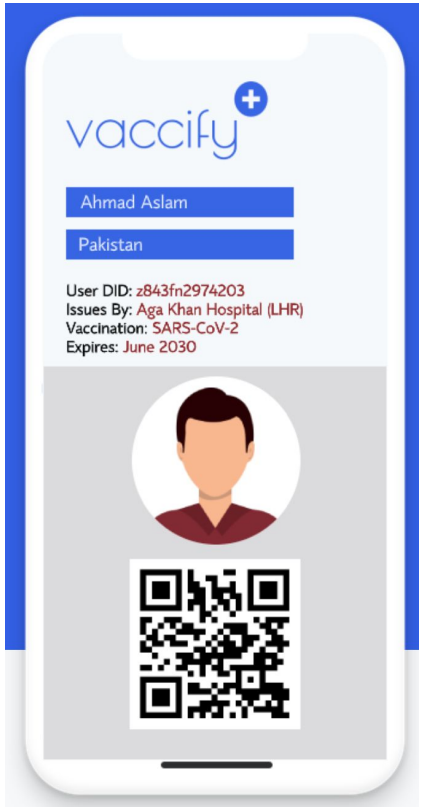


use case = contactless proving for air travel. did:sov, DIDComm over RESTful HTTP.

POC Highlight: Vaccify in Pakistan





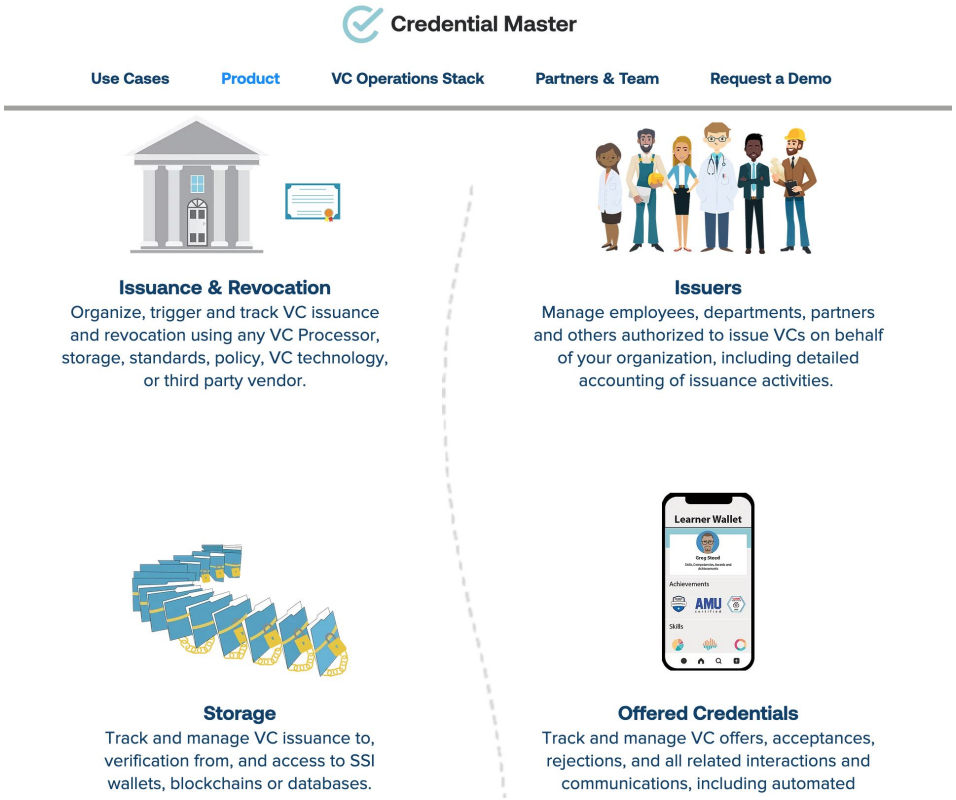


Use case = general proving for government interactions and travel around COVID-19 and other diseases. did:sov, DIDComm with library calls.

Production Solution Highlight: VON

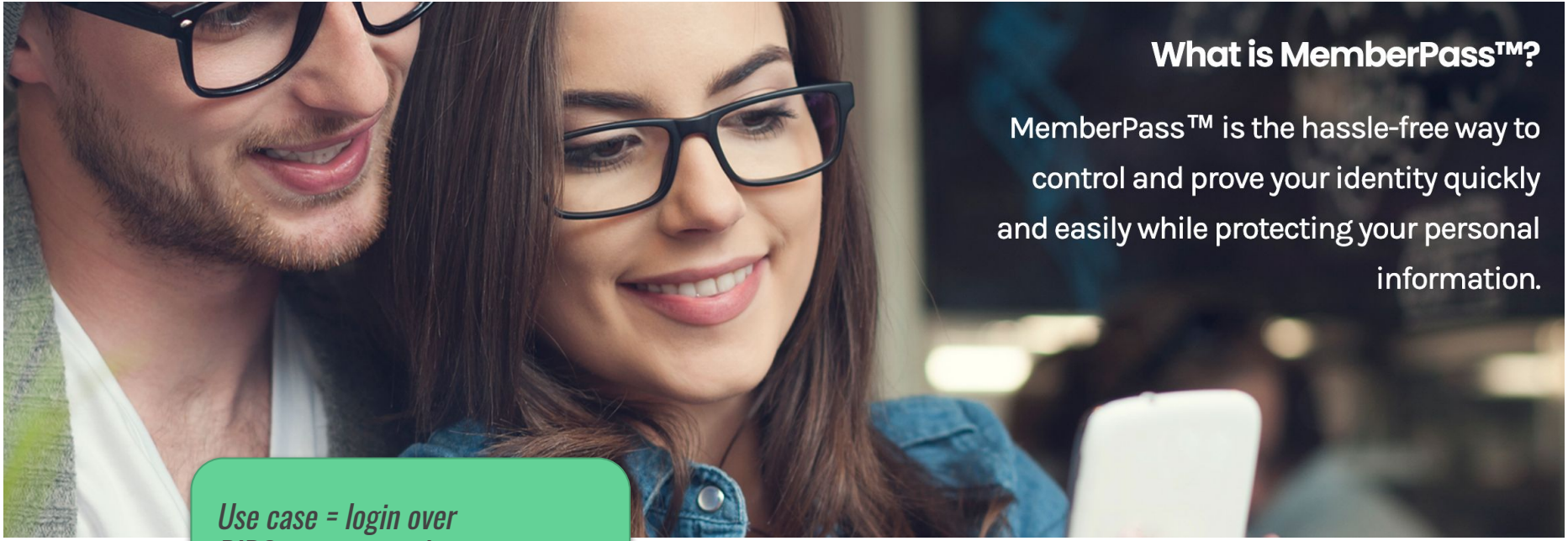
Use case = millions of business licenses as VCs; public registry for discovery and querying (no privacy concerns). DIDComm implemented in python.

Product Highlight: CredentialMaster



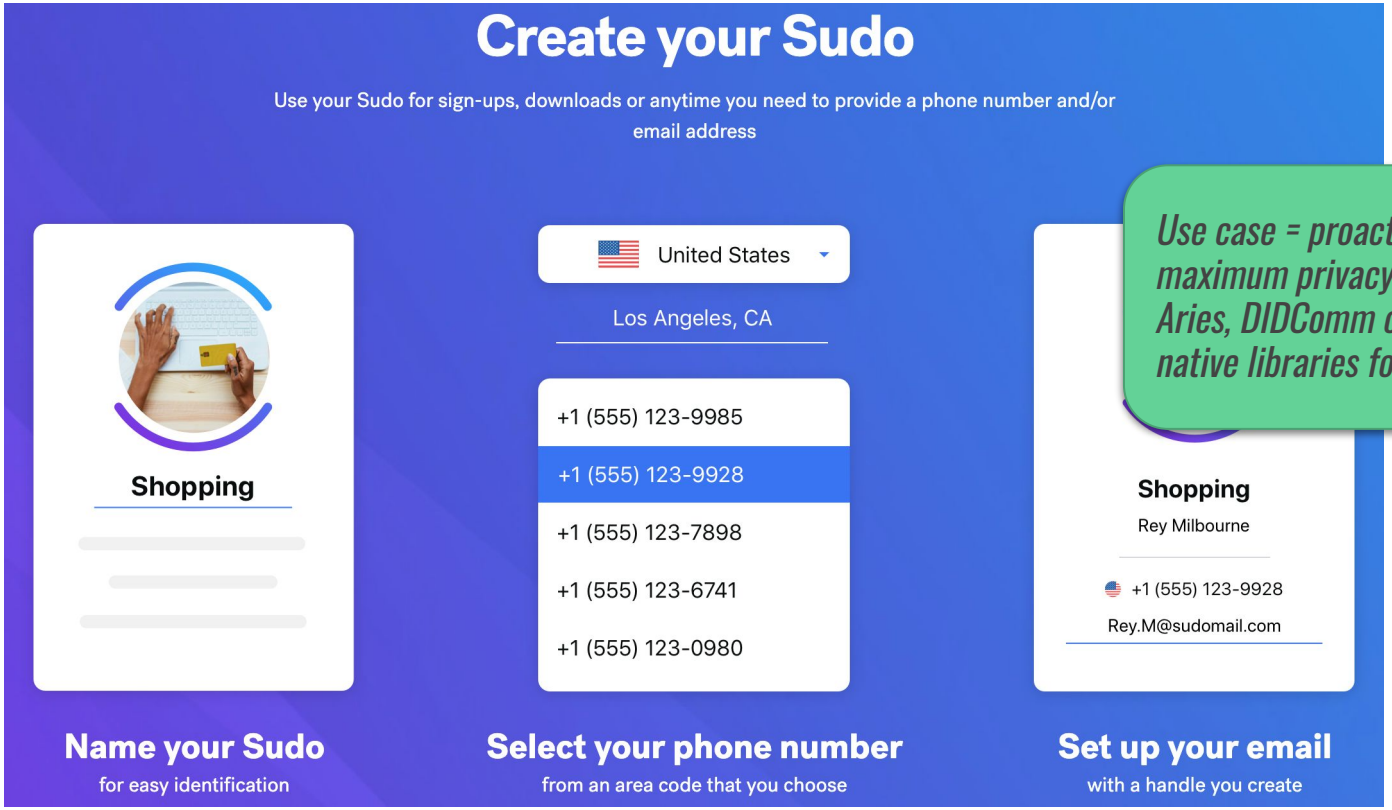
Use case = bulk issuance and management of VCs from multiple ecosystems at massive scale. Salesforce integration. Multiple DID methods, DIDComm with library calls.

Production Solution Highlight: CULedger MemberPass



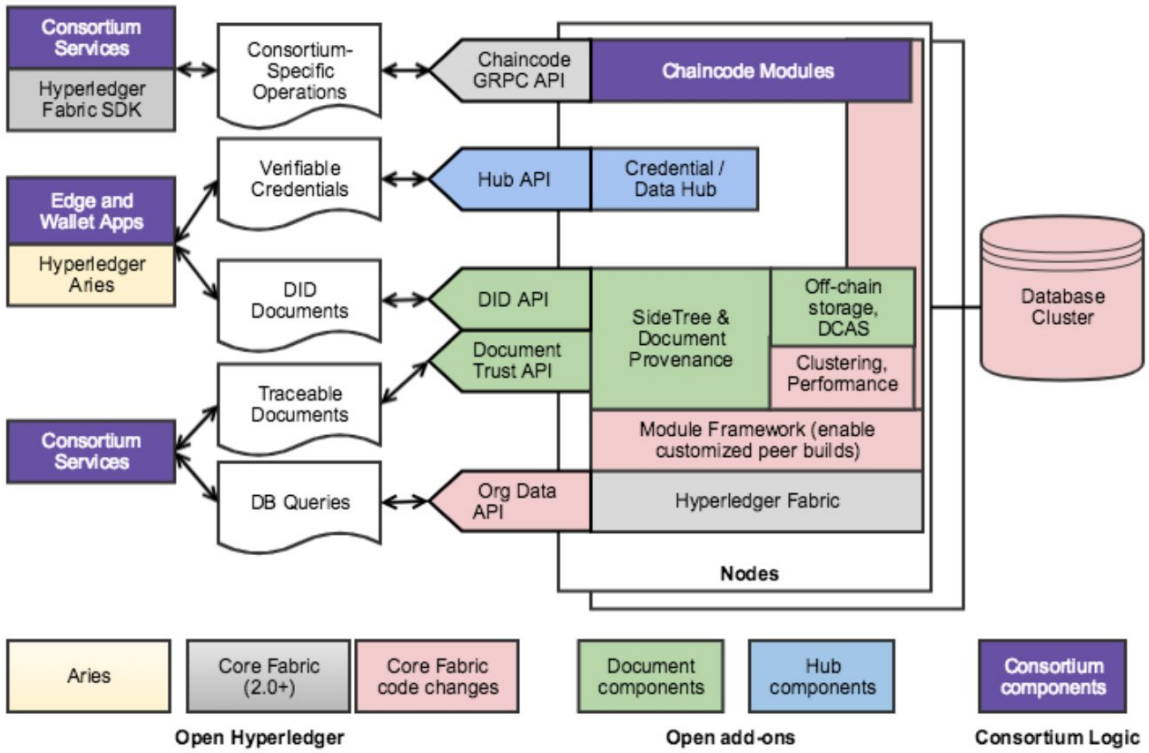
Use case = login over DIDComm-secured messaging; consent, structured interviews.

Product Highlight: Anonyme and MySudo



Use case = proactive personas for maximum privacy. Hyperledger Aries, DIDComm over HTTP with native libraries for iOS.

Architecture Highlight: Trustbloc



Use case = KYC and similar VC/proving interactions. did:ion (SideTree), Hyperledger Fabric, Hyperledger Aries. DIDComm over HTTP with libraries in Go. Universal Resolver and Go-library equivs.

Production Solution Highlight: Kiva

Use case = 3.5 million government-issued national IDs in Sierra Leone; economic empowerment. Hyperledger Indy/Aries. Moving to did:indy. DIDComm for issuance and proving.

Kiva Protocol

Digital infrastructure for **inclusive financial systems**

ID2020

Solution Highlight: NHS

NHS staff to be given 'Covid-19 passports' so they can be redeployed quickly in any second wave

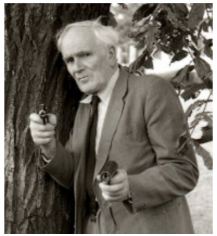
Move will help nurses, doctors and other staff transfer quickly between NHS trusts

Shaun Lintern Health Correspondent | @ShaunLintern | Wednesday 12 August 2020 16:03

Private beta project involving over 20 UK hospitals issuing and verifying digital staff passports, and further use cases such as sign-on/authentication and messaging being investigated.

Research Highlight: Q

Q supplied James Bond and other secret agents with cool gadgets:



dcs

A command-line tool ("DIDComm send") that lets you send an arbitrary A2A message to s
Scriptable.

fileagent

An agent that interacts by reading and writing files in a folder in the filesystem is a useful w
behavior of other agents. Observe what your agent is sending by watching a folder. Take a
any message you want, drop it in that folder as a response, and see how your agent reacts
playback agent behaviors by doing simple file I/O.

polyrelay

A pluggable relay that lets you translate any agent transport into different transports (either 1-to-1, o
many), for arbitrary testing scenarios.

mailmediator

An agent that uses SMTP and IMAP as its transports is a useful way to experiment with something ot
It makes the asynchronous nature of DID Communication very obvious. And the best part is, you don
run one to use one--there's an instance of this agent running at indyagent1@gmail.com. Send it an e

DIDComm where transport = file system or email. Complex DIDComm routing.

Greetings from the TAG (TAG, 30 min)

Horizontal Review (Editors, 30 min)

End of Day 2

Decentralized Identifier WG Virtual Face-to-Face meeting

Day 3: November 4, 2020
Chairs: Brent Zundel, Dan Burnett
Location: The Metaverse

Today’s agenda

10:00		
10:00	Review and Agenda	Dan Burnett
10:15	W3C Process and Patent Policy	Brent
10:45	Test suite - working session	Orie
11:30	Break	
12:00	Presentation - content identifier	ISCC
12:30	Deterministic Equivalent Id	Daniel Buchner
13:00	Deterministic Equivalent Id	Daniel Buchner

W3C Process and Patent Policy 2020 (Chairs, 30 min)

Process 2020

We are now operating under Process 2020

- Explainer Wiki for Process 2020

Process 2020 introduces:

- enhancements to the REC track to allow easier updating of RECs and CRs
- strengthens the patent policy
- provides a Living Standards capability as a native capability of the W3C Recommendation Track

Process 2020

Substantive Changes to Recommendations

- Substantive changes to Recommendations, e.g. in response to errata, can be annotated inline as Candidate Changes. Republication with these informative annotations is as simple as a WD update.
- Candidate Changes which have received wide review and implementation experience can be folded inline by
  - issuing a Last Call for Review of Proposed Changes, which bundles patent review and AC review together
  - issuing an update request (similar to a PR transition request) to republish the Recommendation.

Feature Additions to Recommendations

- Recommendations which are identified as expandable can accept feature additions, using the same process as substantive changes, above.

Streamlined Director's Approval

- In the most straightforward and uncontroversial cases, the Director's Approval for issuing an updated CR Snapshot or updated Recommendation is automatic.

Process 2020

CR Drafts vs. Snapshots

- The current process for “Candidate Recommendation” publications, which involves a transition or update request for Director's Approval and triggers a patent review, is now called a “Candidate Recommendation Snapshot”. CR snapshots should be published every 6-24 months if there have been changes.
- Additionally, between CR Snapshots, WGs are now allowed to publish “Candidate Recommendation Drafts”, which are supposed to be at the same level of quality as a CR, but can be published as easily as a WD (without Director's Approval). This allows the WG to continuously keep its official specification up to date with the latest WG thinking between CR snapshots. CR Drafts have the same Patent Policy implications as a Working Draft.
- CRs (both kinds) can also be annotated as non-normative Candidate Changes or Candidate Additions, to facilitate wide review of proposals. The process for incorporating these changes into the normative text is just republication of the CR.

Process 2020

Improved Patent Policy

- Patent licenses now take effect at CR, instead of at REC, protecting the implementations that are required to exist to get to REC.

Process 2020

- CR is now a CR Snapshot and is the legal basis for patent licenses
  - this allows implementers to have patent protection for their implementations
- Rather than using a working draft to track changes between CR snapshots, we can use CR Drafts.
- Makes our process flow more automated, allows us to use echidna to publish CR Drafts
- If changes made to CR Drafts are not substantive, we can go directly from there to PR

Patent Policy 2020

We are not currently operating under Patent Policy 2020,
we are under Patent Policy 2017

It is not clear precisely how to operate under Process 2020 and Patent Policy 2017, because the updated process and patent policies are designed to work together.

Things will be much smoother if we’re able to operate under Patent Policy 2020

Patent 2020 Diff

Most of the text changes are just like the following:

```
77 licensing goals for W3C Recommendations
78 licensing obligations that Working Group p
```

```
82 licensing goals for W3C Specifications
83 licensing obligations that Working Group
```

```
162 10. If the
    Recommendation is rescinded [PROCES
    s granted before the
```

```
191 10. If the Patent Review Draft or
    Recommendation is rescinded [PROCESS,
    s granted before the
```

Patent Policy 2020 Diff

Other changes are only slightly more extensive:

```
93 3.1. W3C RF Licensing Requirements for All Working Group Participants
   As a condition of participating in a Working Group, each participant (W3C Members, W3C Team members, invited ex
94 perts, and members of the public) shall agree to make
   available under W3C RF licensing requirements
   any Essential Claims related to the work of that particular Working Group.
    This requirement includes Essential Claims that the participant owns and any that the participant has the righ
   t to license without obligation of payment or other consideration to an unrelated third party. With the excepti
```

```
100 3.1. W3C RF Licensing Requirements for All Working Group Participants
    As a condition of participating in a Working Group, each participant (W3C Members, W3C Team members, invited ex
101 perts, and members of the public) shall agree to make
    Specification Licensing Commitments under W3C RF licensing requirements for
    any Essential Claims related to the work of that particular Working
    Group that are not excluded pursuant to section 4.
     This requirement includes Essential Claims that the participant owns and any that the participant has the righ
```

Patent Policy 2020 Additions

They added this explanation of what “specification” means, and add the concept of a “patent review draft”:

```
94
For the purpose of this policy, “Specification” refers to a W3C technical report published on the Recommendatio
n Track, see [PROCESS]. “Patent Review Draft refers to a version of a W3C Specification defined as such by the
95 W3C Process [PROCESS], that is published for patent review and exclusion.
96
```

Patent Policy 2020 Additions

They added this section about licensing commitments:

```
3.5. Specification Licensing Commitments
Working Group participants who forego the right to exclude Essential Claims against a Specification when provided the opportunity to do so see section 4, commit to license those Essential Claims under the W3C Royalty-Free Licensing Requirements. This Specification Licensing Commitment is effective at the later of:

The first publication of the Specification (after participant joins the Working Group) as either a Patent Review Draft or Recommendation in which the claim is essential;
The end of the participant's first Exclusion Opportunity pertaining to that claim.
```

Patent Policy 2020 Additions

They added this section about the persistence of those licensing commitments:

3.6. Licensing Commitment Persistence

If a Working Group participant makes Licensing Commitments on a Specification for an Essential Claim, the Licensing Commitment carries forward to a subsequent Patent Review Draft or Recommendation of the Specification if:

the subsequent Patent Review Draft or Recommendation uses the Essential Claim in a substantially similar manner and to a substantially similar extent with a substantially similar result as the Essential Claim was used in the Specification on which the Working Group participant made the Licensing Commitment; and

the subsequent Patent Review Draft or Recommendation is within, or only a minor expansion of, the scope of the Working Group's charter as it existed at the time of the participant's Licensing Commitment to the Specification.

In addition, even if the above requirements are not met, if an implementation of a subsequent Patent Review Draft is also an implementation of a prior Patent Review Draft, then implementation of the subsequent Patent Review Draft or Recommendation will also benefit from the license commitments made by participants in the Working Group that developed the prior Patent Review Draft or Recommendation.

Patent Policy 2020 Additions

Section 4 has the most changes, we’re not going to go into them in detail here.

These are the changes that are most important for member companies to review.

These changes are all related to the ability of a working group to now produce several, subsequent patent review drafts.

Patent Policy 2020 Summary

1. IANAL
2. Mostly minor changes from previous version, almost all of them exclusively to address the need for multiple patent exclusions and disclosures during CR and thereafter.
3. Should we accept it? I think so. What will be the impact for your organization?
4. Accepting this means:
    a. We revise the charter to use Patent Policy 2020
    b. The director approves the revised charter on December 1
    c. Participants will have 45 days to rejoin the group

Test Suite - Working Session (Orie, 45 min)

Testing 101

1. Create tests that are deterministic (avoid randomness).
2. Compare expected values to static fixtures / test vectors
3. Break up your tests into scenarios
4. Make sure to cover positive and negative test cases
5. Don’t make your test cases too long
6. Document what your scenarios are covering in plain english
7. Use links to issues / spec text
8. Use realistic looking data (avoid obviously broken / unhelpful examples if possible)
9. Know your test coverage percentage
10. DRY, KISS

Write tests that **prove** that behavior exists, don’t “**trust**”.

Architecture Approach

- Inspired by Jest, we've built a dockerized test server, capable of generating a test report.

- A scenario is a collection of tests, in Jest scenarios are called describe blocks.
  - Scenarios are composed of structured input, expected output and Javascript programs that process the input and output and determine conformance.
  - For example, "DID Syntax" describes a series of tests about the DID, and the DID Document "id" property.

- An assertion is a statement about an input that is true or false.
  - For example, "**did:Example**" **contains no upper case letters** is **false**.
    - **did:Example** is structured input
    - **contains no upper case letters** is an assertion
    - **False** is the value of the assertion
    - This is an example of a negative test case, because the assertion is false.

- Even if you don't know Javascript, you can probably think of examples and assertions for positive and negative test cases for a given scenario. Writing these down in plain English is the first step to testing with confidence.

What are we doing?

We need to convert sections of normative statements to issues, and then close them when tests for them exist.

Q: Do I create a scenario for a single statement, or should a scenario cover multiple statements?
A: It depends, but when in doubt create a scenario per statement.

Q: What if I can’t test a statement?
A: Still open an issue for it, nobody will be able to close it, and eventually it will either get removed or exempted.

Q: What if I don’t know how to program?
A: you can still ensure the issues opened have a good “test plan” on them. A test plan describes possible structured inputs, possible assertions… You can provide examples of data you would want to see tested.

Getting Started

See getting started instructions here: https://github.com/w3c/did-test-suite

Review https://github.com/w3c/did-core/issues/384 for a list of normative statements.

Find a normative statement you think you can test, or help describe... search for it on https://github.com/w3c/did-test-suite/issues.

If its not open yet, open an issue with the normative statement as the issue title.
If you find a duplicate, mark it as a duplicate.
Write out the test plan on the issue in plain English.

Only assign yourself the issue if you plan to submit a PR that addresses the normative statement.

DO NOT start working on tests for normative statements without checking to see if someone else has been assigned the associated issues.

When you open a PR to implement the tests associated with the issue, make sure to reference the issue in the PR description.

Break (30 min)

ISCC Presentation (Titusz Pan, 30 min)

ISCC

Identifiers for Digital Content

DIDWG Virtual TPAC 2020

2020-11-04, *Titusz Pan*

A **Proposal** for a Modern and Open Content-Based Identifier

- A universal identifier for digital text, image, audio, video ...
- Lightweight, multi-faceted fingerprint designed for **digital content**
- Cross-sector applicability (journalism, book & academic publishing, music, film etc.)
- Cross-ledger registry for global discoverability
- Goal: establish **content** as the **subject** of **transactions** in decentralized and networked environments

Digital-Content-Based Identifier
Market Need

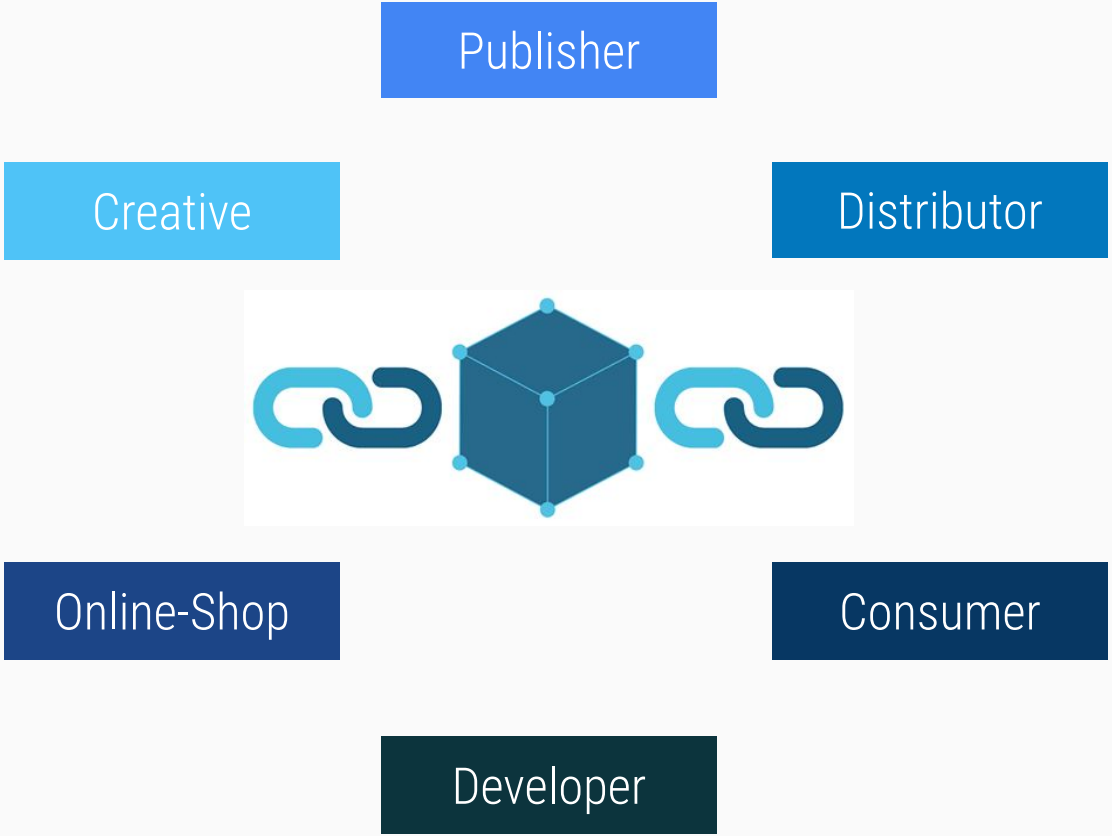
- Most of the existing digital content does not enjoy the benefits of a standard identifier
- Classic registry-based standard identifers involve considerable administrative overhead
- Find agreement about an identifier for a given digital asset without a third party
- Proprietary content-based identification systems create a competitive imbalance
- DLT is commodotizing secure machine-to-machine interactions and transactions
- Need for data integrity - secure immutable binding of identifier / referent (bitstream)
- Need for interoperability across different sectors and content-formats

ISCC - Decentralized Content Identifier

In a multi-sided ecosystem **anybody** may have legitimate interest to create, lookup or register an **identifier** for some content.

Authorship or copyright is **not** a requirement. But **an identifier is a requirement** to communicate and agree on authorship, copyright ...

Intelligent linking of **Identifier <-> Content** can be done by standardizing fingerprinting algorithms.



Layers of “Content” Identification

Content identification is a complex topic and there is often confusion about what exactly is being identified.

In our model for digital content identification we distinguish 6 layers that exist naturally on a scale from abstract to concrete.

1. **Abstract**
2. Semantic Field (vector embeddings)
3. **Generic Manifestation (Perceptual)**
4. **Format Specific Manifestation**
5. **Exact Digital Manifestation (bitstream)**
6. Individual Copy

ISCC

The **DNA** of your digital content

Estimate similarity of content by comparing their ISCC codes

ISCC :	Meta-Code	Content-Code	Data-Code	Instance-Code
	CCDFPFc87MhdT	CTWAGYJ9HZGj1	CDhydSjQXDXVk	CRd5bk4SrBpzt

Abstract & Persistent — Concrete & Volatile

Metadata Similarity	Content Similarity	Data Similarity	Data Checksum

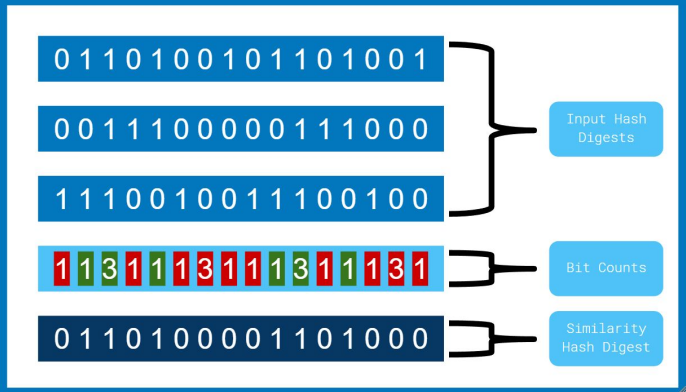
Components are self-describing and can be extended and used standalone or in combination

CCDFPFc87MhdT | CTWAGYJ9HZGj1 | CDhydSjQXDXVk | CRd5bk4SrBpzt

Meta-ID

A similarity preserving hash over metadata.

ISCC - Similarity Hash Diagram



Layer 1 - Abstract Creation

The Meta-ID is seeded from Metadata!

Title for content or work or series (max 128 bytes)

Optional extra metadata or text for disambiguation (max ~400 bytes). Eventually with sector specific schema based kernel metadata.

- Identifies at any desired level of abstraction (series, work ...)
- Top level of grouping a content collection or hierarchy
- Independent of digital manifestations
- Supports *progressive disambiguation*
- Requires minimal (optionally no metadata)

Seed Metadata is metadata that is used to establish a **Meta-ID** and stays frozen (immutable) throughout its existence. **Floating Metadata** is any mutable metadata that is managed in context with an **ISCC**.

CCDFPFc87MhdT CTWAGYJ9HZGj1 CDhydSjQXDXVk CRd5bk4SrBpzt

Semantic-ID

Identification of Meaning :).

Layer 2 - Semantic Field

king − man + woman ~= queen

CCDFPFc87MhdT | CTWAGYJ9HZGj1 | CDhydSjQXDXVk | CRd5bk4SrBpzt

Content-ID (Image)

Similarity hash over normalized generic data. Self-Describing and media-type specific.

If we want to identify "Content" we cannot compare on encoded "Data":

- Two "identical" images
- Yet the data is completely different
- Due to different file formats
- Content-ID encodes information structure - not raw data

Layer 3 - Generic Manifestation

Data ≠ Content

JPG Image	JPG Data	JPG SHA1	JPG Content-ID
	49 74 27 73 20 6e 6f 74 20 61 62 6f 75 74 20 62 61 6e 6b 69 6e 67 20 74 68 65 20 75 6e 62 61 6e 6b 65 64 2e	7b 24 1f 77 f0 f2 96 df 73 b5 e0 38 97 6a 5e 3b d0 12 bd 23	CYHa5UMqq1iQS
=	≠	≠	=
PNG Image	PNG Data	PNG SHA1	PNG Content-ID
	54 68 65 20 43 75 72 72 65 6e 63 79 20 75 73 65 64 20 6f 6e 20 43 6f 62 6c 6f 20 69 73 20 43 68 61 72 6d 2e	7e bd c5 c5 c0 30 d5 4c 30 c0 31 df 4c 9e ff d5 b2 ad e8 2d	CYHa5UMqq1iQS

Layer 4 - Format Specific Manifestation

Data-ID

Similarity over raw encoded data.

- Identifies encoded content
- Clusters file versions
- Spectrum of tolerance
- Shift resistant chunking (CDC)
- **Similarity hash over variable sized chunk hashes**

Fixed Size Data Chunking

AAAA | BBBB | CCCC | DDDD |

EAAA | ABBB | BCCC | CDDD | D

Content Defined Chunking - Shift Resistant - Variable Size Chunks

AAAA | BBBB | CCCC | DDDD |

EAAAA | BBBB | CCCC | DDDD |

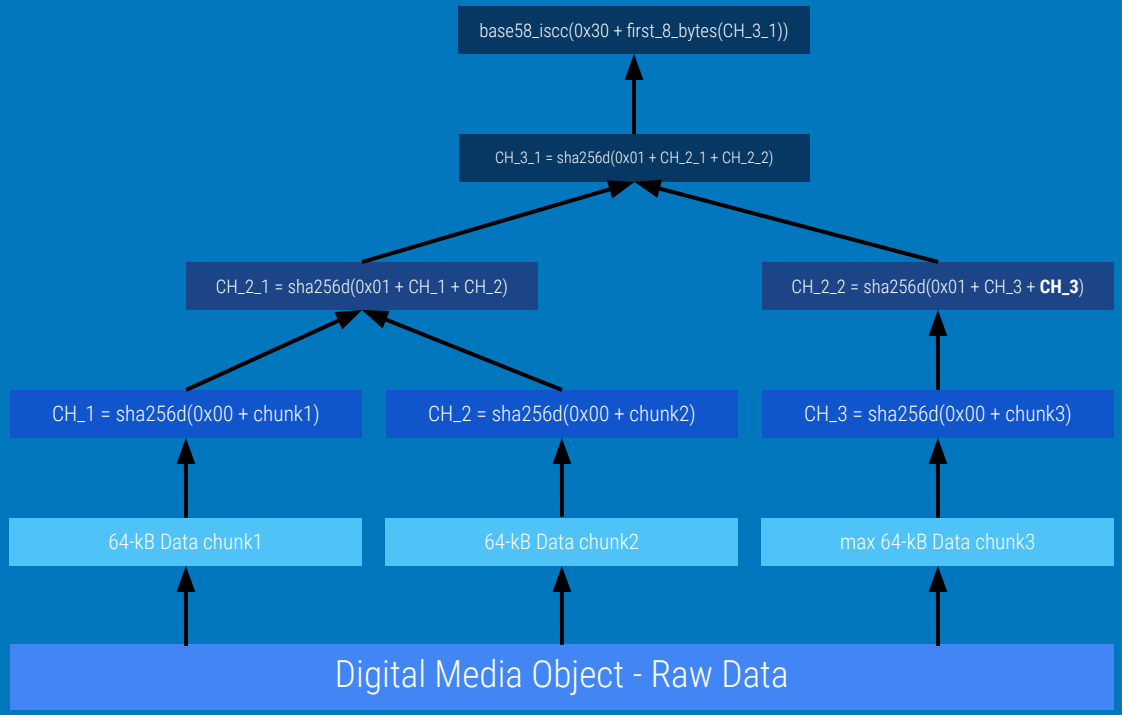
CCDFPFc87MhdT | CTWAGYJ9HZGj1 | CDhydSjQXDXVk | CRd5bk4SrBpzt

Layer 5 - Exact Digital Manifestation

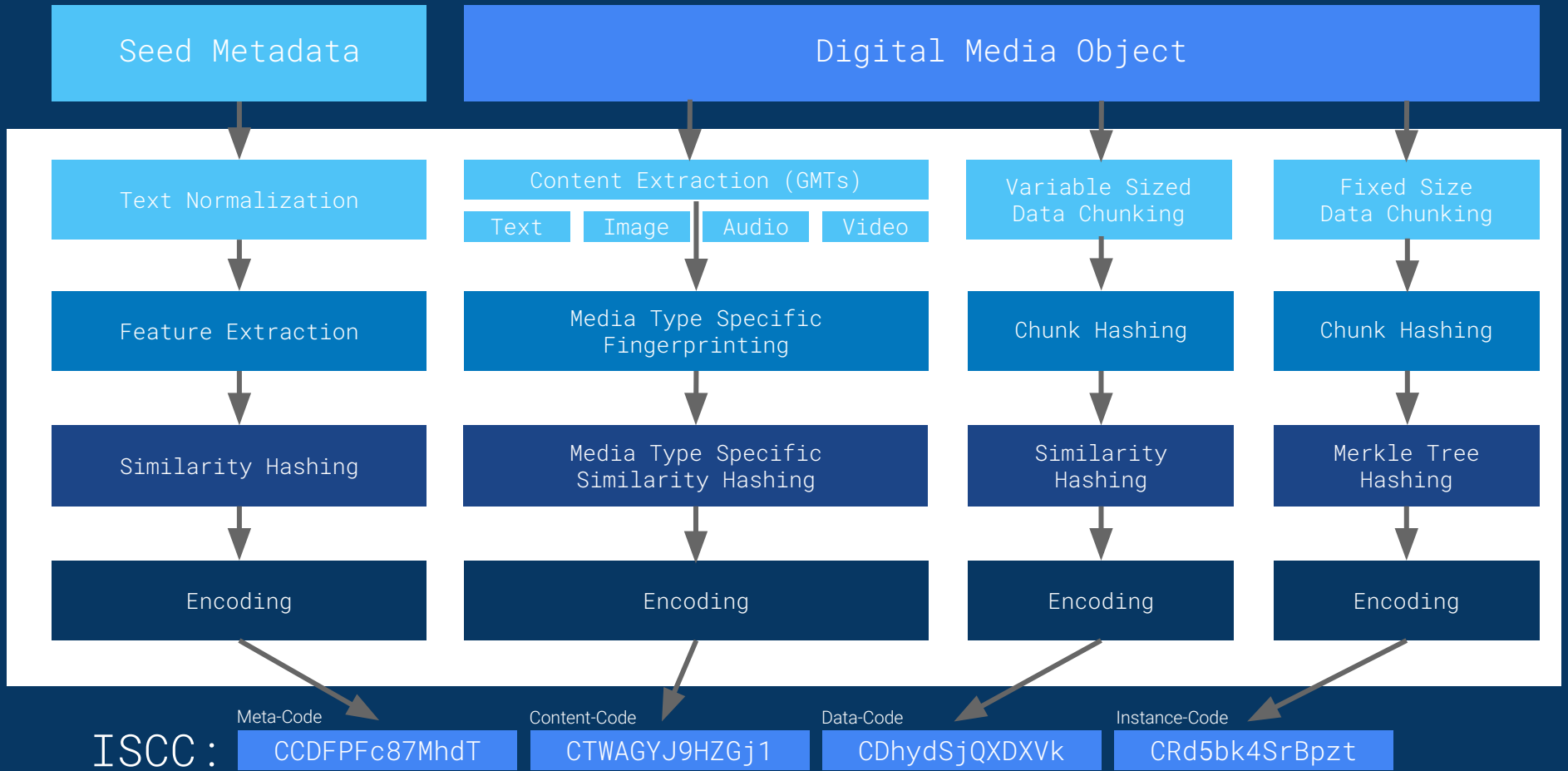
Instance-ID

Cryptographic hash. The root of a hash tree over raw data.

- Precise data identification
- Proof of data containment
- Separate Tophash (256 bit)
- Data integrity (via tophash)



Overview of **ISCC** Creation Process



Example one **DOI** multiple matching **ISCC**




Paper: Neural Computation of Surface Border Ownership and Relative Surface Depth from Ambiguous Contrast Inputs

Host	DOI	ISCC
hal.archives-ouvertes.fr	10.3389/fpsyg.2016.01102	CCDyud5ZWAkDR-CTTq25WFQTWaU-CDbUZg6v3qzzM-CRrxfuPk2nP3Q
arxiv.org	10.3389/fpsyg.2016.01102	CCDyud5ZWAkDR-CTTRs5cQY1D11-CDPqUxrqN7YRx-CRcUmq2SmgN18
hal.archives-ouvertes.fr	10.3389/fpsyg.2016.01102	CCDyud5ZWAkDR-CTfNotD3KMMd1-CD481J7LDBQPH-CR8rZ9QzTzJRL
frontiersin.org	10.3389/fpsyg.2016.01102	CCDyud5ZWAkDR-CTfNotD3KMMd1-CDMXxzVp63Mpt-CRZ5iRuFkENb7

See on chain: https://explorer.coblo.net/stream/iscc?keys=CCDyud5ZWAkDR

Estimated Similarity of Meta-ID: 100.00 %
Estimated Similarity of Content-ID Text: 84.38 %
Estimated Similarity of Data-ID: 53.12 %

Comparing two **ISCC** Codes yields various insights (draft)

	Meta-ID	Content-ID	Data-ID	Instance-ID	Explanation
1	=	=	=	=*	**Totally identical file** (same metadata, content structure, file encoding and file)
2	=|=	=	=	=*	Different metadata, same content, file encoding and identical file > e.g. a special edition or inconsistent metadata
3	=|=	=|=	=|=	=|=	Totally different file (different metadata, content structure, file encoding and file)
4	= or ~	=|=	=|=	=|=	Same/similar* metadata, but different content and file encoding and file, e.g. manual clustering
5	= or ~	= or ~	=|=	=|=	Same/similar metadata, same/similar content but in a different file encoding, e.g. related product
6	= or ~	= or ~	= or ~	=|=	Same/similar metadata, same/similar content in same/similar file encoding
7	=|=	= or ~	=|=	=|=	Different metadata, same/similar content but in a different file encoding
8	=|=	= or ~	= or ~	=|=	Different metadata, but same/similar content and file encoding, e.g. a special edition

=* compare top-hash of both files to be sure there is no accidental Instance-ID collision.

first 3 components are compact binary codes (bit vectors) that can be compared to measure estimated similarity by haming dinstance

Decentralized Content Identifiers
comparison of approaches

Identifier	Example	Bits	Method
UUID	`550e8400-e29b-11d4-a716-446655440000`	128	Random / Hash / Time
SHA256	`a1bdd0de0d1f27b227cbf43ac110bb09827a40d734ea0c29585c98a34b80413d`	256	Cryptographic Hash
ISCC-CODE	`CCDFPFc87MhdTCTWAGYJ9HZGj1CDhydSjutScgECR4GZ8SW5a7uc`	288	Multifaceted Fingerprint
ISCC-ID	`SiCTWhy4GZhdT`	72+	DLT / Short FP / Counter

ISCC combines cryptographic hashes, similarity preserving compact binary codes, standardized fingerprints and DLT.
We have POC for registration of ISCC-CODES via Ethereum/IPFS to generate short, unique, owned and resolvable ISCC-IDs

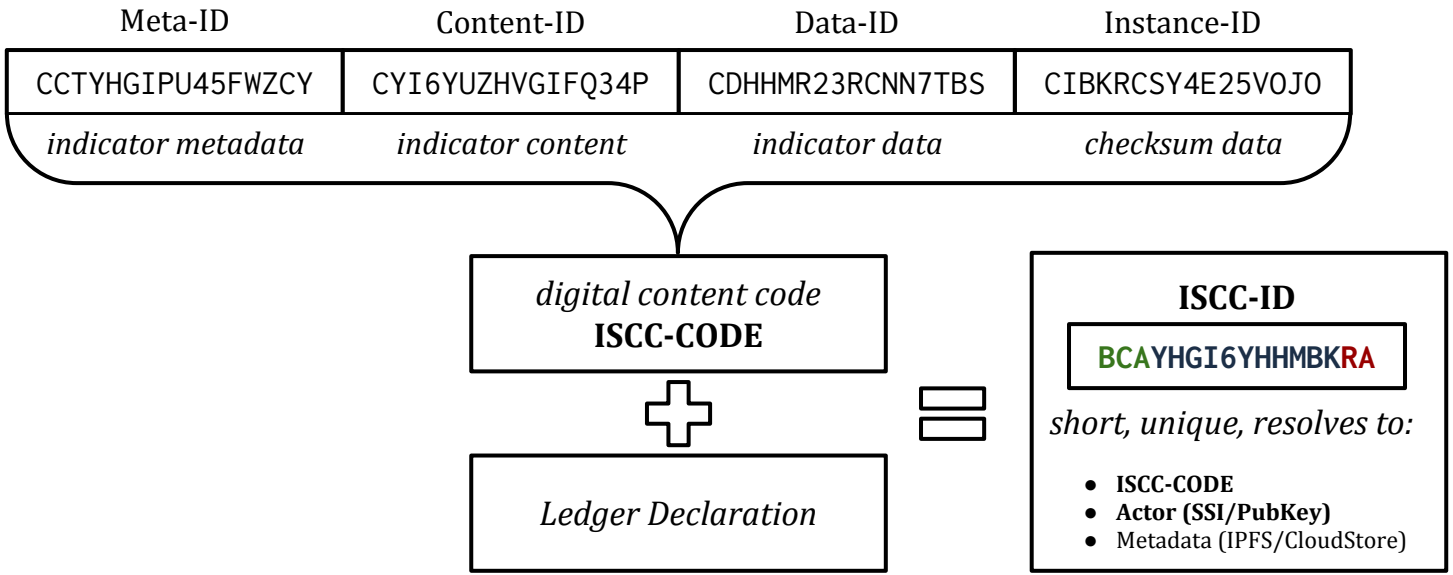
ISCC - Decentralized Registration Protocol

ISCC-CODE = Decentralized, Content-Based, Similarity-Preserving Code

`ISCC:CCTYHGIPU45FWZCY-CYI6YUZHVGIFQ34P-CDHHMR23RCNN7TBS-CIBKRCSY4E25VOJO`

ISCC-ID = Short, Unique, Owned, Persistent, Resolvable Identifier (via public declaration)

`ISCC:BCAYHGI6YHHMBKRA` (Structure: **chain-id** - **simhash** - **counter**)



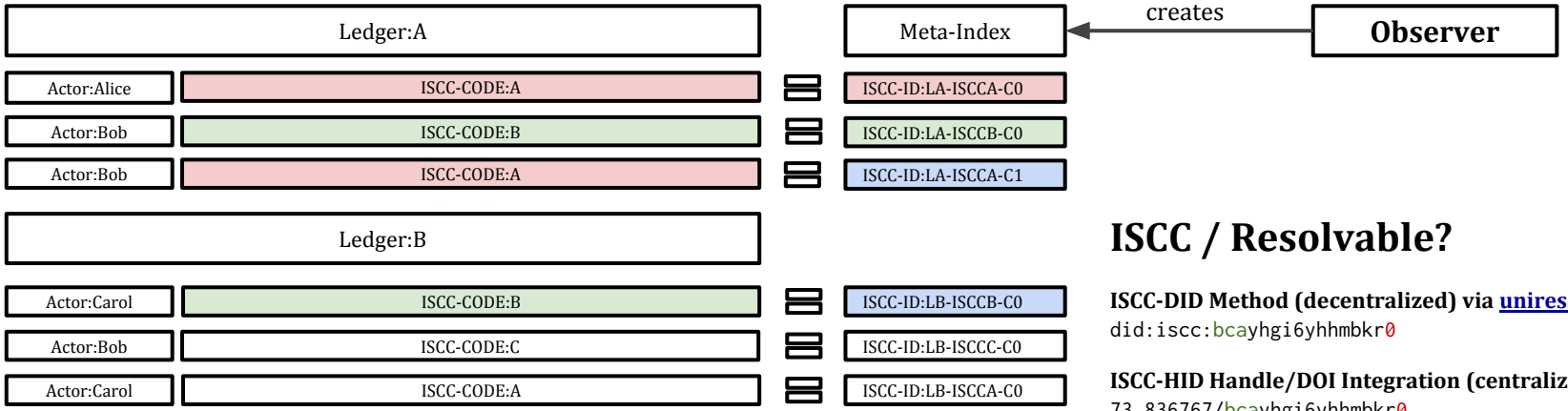
ISCC - Decentralized Registration Protocol

ISCC-CODE = Decentralized, Content-Based, Similarity-Preserving Code

`ISCC:CCTYHGIPU45FWZCY-CYI6YUZHVGIFQ34P-CDHHMR23RCNN7TBS-CIBKRCSY4E25VOJO`

ISCC-ID = Short, Unique, Owned, Verifiable, Persistent, Resolvable Identifier

`ISCC:BCAYHGI6YHHMBKRA` (Structure: **chain-id** - **simhash** - **counter**)



The **blue** colored **ISCC-IDs** in the Meta-Index illustrate how duplicate **ISCC-CODE** registrations on a single or accross multiple ledgers result in **unique** but **matchable** **ISCC-IDs**

ISCC / Resolvable?

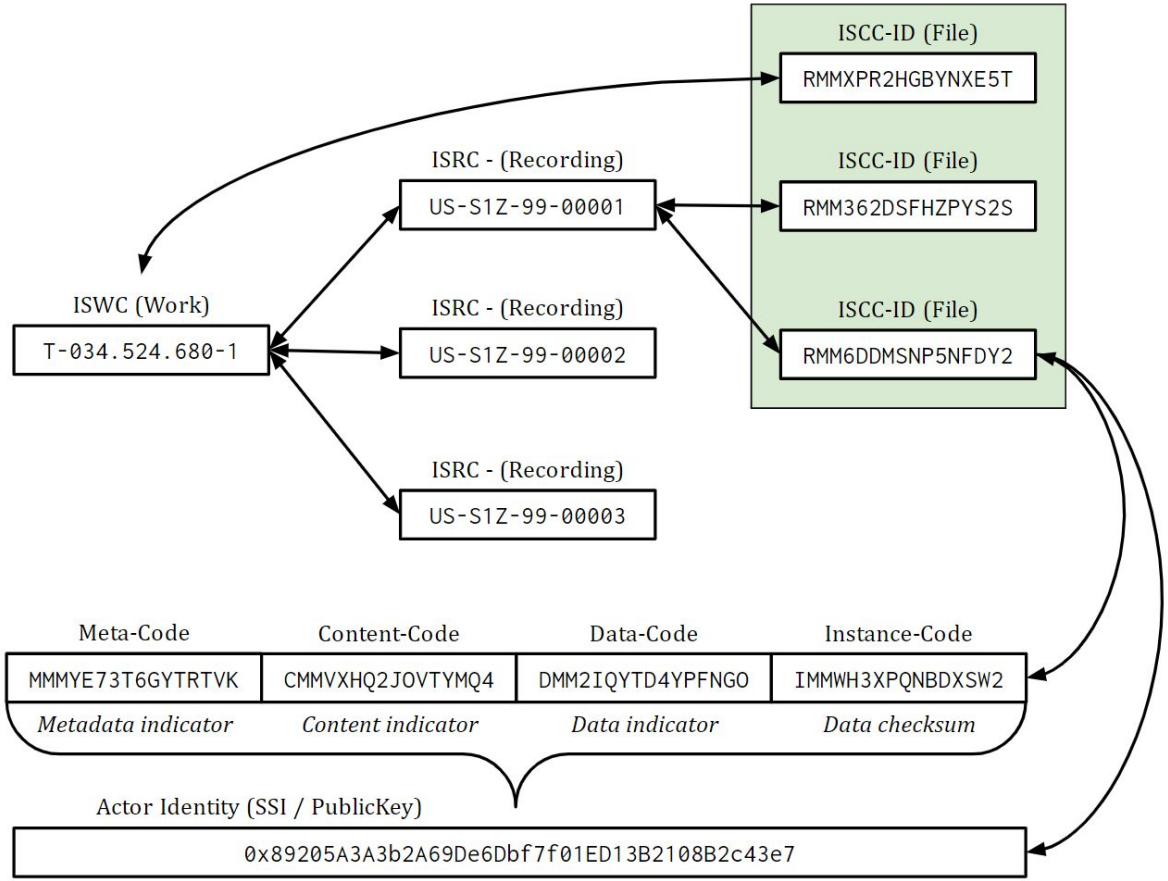
ISCC-DID Method (decentralized) via uniresolver.io

`did:iscc:bcayhgi6yhhmbkr0`

ISCC-HID Handle/DOI Integration (centralized)

`73.836767/bcayhgi6yhhmbkr0`

ISCC - In Context with ISWC and ISRC



V0.3, 2020-10-04, *Titusz Pan*

ISCC - Status

ISO/TC 46/SC 9/WG 18

We are here :)

STAGE	SUBSTAGE						
				90 DECISION			
	00 REGISTRATION	20 START OF MAIN ACTION	60 COMPLETION OF MAIN ACTION	92 REPEAT AN EARLIER PHASE	93 REPEAT CURRENT PHASE	98 ABANDON	99 PROCEED
00 PRELIMINARY	00.00 Proposal for new project received	00.20 Proposal for new project under review	00.60 Close of review			00.98 Proposal for new project abandoned	00.99 Approval to ballot proposal for new project
10 PROPOSAL	10.00 Proposal for new project registered	10.20 New project ballot initiated	10.60 Close of voting	10.92 Proposal returned to submitter for further definition		10.98 New project rejected	10.99 New project approved
20 PREPARATORY	20.00 New project registered in TC/SC work programme	20.20 Working draft (WD) study initiated	20.60 Close of comment period			20.98 Project deleted	20.99 WD approved for registration as CD
30 COMMITTEE	30.00 Committee draft (CD) registered	30.20 CD study/ballot initiated	30.60 Close of voting/ comment period	30.92 CD referred back to Working Group		30.98 Project deleted	30.99 CD approved for registration as DIS
40 ENQUIRY	40.00 DIS registered	40.20 DIS ballot initiated: 12 weeks	40.60 Close of voting	40.92 Full report circulated: DIS referred back to TC or SC	40.93 Full report circulated: decision for new DIS ballot	40.98 Project deleted	40.99 Full report circulated: DIS approved for registration as FDIS
50 APPROVAL	50.00 Final text received or FDIS registered for formal approval	50.20 Proof sent to secretariat or FDIS ballot initiated: 8 weeks	50.60 Close of voting. Proof returned by secretariat	50.92 FDIS or proof referred back to TC or SC		50.98 Project deleted	50.99 FDIS or proof approved for publication
60 PUBLICATION	60.00 International Standard under publication		60.60 International Standard published				
90 REVIEW		90.20 International Standard under periodical review	90.60 Close of review	90.92 International Standard to be revised	90.93 International Standard confirmed		90.99 Withdrawal of International Standard proposed by TC or SC
95 WITHDRAWAL		95.20 Withdrawal ballot initiated	95.60 Close of voting	95.92 Decision not to withdraw international Standard			95.99 Withdrawal of International Standard

Roadmap:

- ISCC-ID (on top of ISCC-Code)
- Content-Code Audio (wip)
- Content-Code Video (wip)
- Semantic-ID (cross language)
- Granular fingerprints
- Desktop Application
- Indexing Server

Digital Reality

There is too much/granular content to manually assign and track content identifiers.

The Good News

All your

already have an **ISCC**.

It “just” needs to be generated.

ISCC Foundation

Contact

Titusz Pan
tp@iscc.foundation

The ISCC Project is exclusively funded by our passion.
Contributions and donations are welcome ;).

Websites

https://iscc.codes/
https://github.com/iscc/iscc-specs
https://iscc.foundation
https://iscc.coblo.net/
https://github.com/titusz/iscc-registry

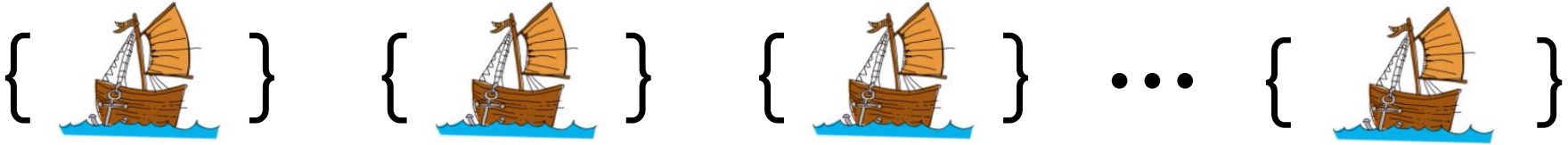
DPUB Summit Conference,
Paris, 25-26 May 2019
by Sebastian Posth

Blockchain for Science Con,
Berlin, 4th-5th Nov. 2019
by Titusz Pan

Equivalent Identifiers (Daniel Buchner, 60 min)

DIDs can change entirely over their lifetime

`did:example:theseus`



T0: Creates DID

T1: Rolls a key

T2: Changes service endpoint

T3: Total change in form from **T0**

Is the DID at **T3** the DID of Theseus?

DIDs are ‘Logical Entries’ tracked within DID Methods

```
did:example:01110100
 01101000 01100101
 01110011 01100101
 01110101 01110011
```

T0: Creates DID

```
did:example:theseus
```

T1: Rolls a key

```
did:example:Base64(theseus)
```

T2: Changes service endpoint

• • •

```
did:example:Base58(theseus)
```

T3: Total change in form from **T0**

1. Is one URI string *representation* Theseus’ DID, or is Theseus’ DID a deterministic process of identifying and outputting state associated with a logical entity maintained within a Method?

2. Can many forms of a DID string still identify Theseus’ DID?

Types of equivalence under discussion

`alsoKnownAs`

{  } ?= {  }

```
{
  id: did:example:theseus
  alsoKnownAs: [did:example:pirithous]
}
```

Claim: The resolved ID string may be somehow related to these other ID strings.

Features: Acts as an investigatory hint

Assurances: None

`sameAs / formOf`

{  } == {  }

```
{
  id: did:example:theseus
  formOf: [did:example:Hash(theseus)]
}
```

Claim: The resolved ID string is an exact logical equivalent of these other forms.

Features: Awareness of variants, upgrade path for form changes.

Assurances: Method ensures only exact logical equivalents are populated.

`canonical / preferred`

{  } ==> {  }

```
{
  id: did:example:theseus
  canonical: did:example:Hash(theseus)
}
```

Claim: The resolved ID string is an exact logical equivalent of this other form, and you should modify held references and awareness going forward.

Features: Support for Method evolution, signal for migration processes.

Assurances: Method ensures only an exact logical equivalent is populated.

End of Day 3

Decentralized Identifier WG Virtual TPAC meeting

Day 4: November 5, 2020
Chairs: Brent Zundel, Dan Burnett
Location: The Net

Today’s agenda

12:00		
12:00	Review and Agenda	Dan Burnett
12:15	ADM Working Session	Brent
13:30	Break	
14:00	F2F Goals Review	Brent
15:00	Status updates on all work items (Impl. Guide, Rubric)	Note Editors

ADM Working Session (Brent, 75 min)

Abstract Data Model Working Session

Please raise your hand in zoom if you would like to answer the following questions, as they relate to the Abstract Data Model conversation:

1. What critical use case of yours does the current spec text prohibit that you assumed would be possible?
2. What concrete change should be made to the current spec text in order enable the use case?

Group participants are invited to add themselves to the queue in IRC to answer the following questions, as they relate to the previous answers:

1. Which of your critical use cases will break if the spec text is changed as recommended?
2. What alternative spec text change should be made that would enable both use cases?

Break (30 min)

F2F Goals Review (Chairs, 60 min)

Goals for this meeting

- Make clear what work remains before we can go to CR
- Resolve all major outstanding issues (ADM and privacy concerns)
- Resolve 25% of remaining issues

Work Items Status Update (Editors, 30 min)

Use Cases (5 min)

Implementation Guide (5 min)

Rubric (20 min)

Recent Progress

- First draft populated, editors meeting regularly
- Batch of editorial changes merged
- Broadened scope: interesting characteristics, not just decentralization
- New approach to examples (contributors requested)
- Draft of new sections on Security and Privacy (feedback requested)

Approach to Examples

Old

- 6 reference methods chosen for contrast
- Evaluator must be expert in all
- Each Q evaluated for every method

Method	Spec.	Net.	Reg.	Notes
did:peer	C	n/a	B	Rules for accepting changes ...
did:git	C	n/a	D	The controllers of a git repo ...
did:btcr	C	C	A	The **spec** is maintained by ...
did:sov	B	B	B	The Sovrin Gov FW actual...
did:ethr	A	C	D	The **spec** is controlled by...
did:jolo	A	C	D	Jolocom does not expose...

New

- Let's reference dozens of DID methods throughout
- Only eval methods (max 3) that show variety on a given Q
- Seeking eval statements from contributors expert in their own method
- For given method, please include a few examples where the method is "high" in a dimension, and a few where it is "low" (for balance)

New section on security

6.1 **Robust Crypto** *(min "bits of security" the method requires impls to support)*

6.2 **Expert Review** *(crypto/security vetted by experts and battle hardened)*

6.3 **Future Proofing** *(friendly to post-quantum, larger hashes, or other security upgrades)*

6.4 **Self Certification** *(is entropy on identifier provably connected to inception key)*

6.5 **Availability** *(protections against DDoS, hacking, legal challenge)*

6.6 **Evolution** *(exposes provable DID doc history)*

6.7 **Many Eyes** *(code published, has many contributors, has vuln disclosure mechanism)*

6.8 **Diffuse Control** *(DID can be controlled by m-of-n, threshold sigs, etc)*

6.9 **Regulatory Compliance** *(satisfies FIPS, legal back door regulations, etc)*

Are these good questions? What's missing? Are possible responses appropriate?
Which DID methods exhibit interesting variety?

New section on privacy

7.1 **Per-DID constraints on visibility** *(allows some DID to be less than public?)*

7.2 **Cross-DID Leakage** *(hard to connect DIDs that have a common controller?)*

7.3 **Incentives for Multicontext DIDs** *(does cost/hassle encourage overuse of a DID?)*

7.4 **Deletion** *(can mistakes be corrected? right to be forgotten?)*

7.5 **Help with best practice** *(gives tech, policy, or explanatory safeguards for endpoints and other DID doc data)*

Are these good questions? What's missing? Are possible responses appropriate?
Which DID methods exhibit interesting variety?

End of Day 4