Authentic Chained Data Containers

ToIP Technical Working Group Task Force

Wiki:
https://wiki.trustoverip.org/display/HOME/ACDC+%28Authentic+Chained+Data+Container%29+Task+Force
https://wiki.trustoverip.org/display/HOME/ACDC+Meeting+Page

Slack:
tswg-acdc-tf

Github:
https://github.com/trustoverip/TSS0033-technology-stack-acdc
https://github.com/WebOfTrust/vLEI
https://github.com/WebOfTrust/ietf-said

White Papers:
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/ACDC.web.pdf
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/VC_Enhancement_Strategy.md
https://hackmd.io/Ai4yhDaYRSW8_eZhuL26cw (hidden attribute ACDC)

Samuel M. Smith Ph.D.
sam@samuelsmith.org
IIW 2021 B
v1.06
2021-10-12

Deliverables

https://wiki.trustoverip.org/display/HOME/ACDC+%28Authentic+Chained+Data+Container%29+Task+Force

Deliverables

The table below lists all deliverables of the ACDC Task Force:

Acronym	Full Name of Deliverable	Deliverable Type	Link to Draft Deliverable	Lead Authors	Status/Notes
ACDC	Authentic Chained Data Container	Specification	Pre-Draft Deliverable (PDF)	@Samuel Smith	Slides from the original white paper
AID	Attributable (Autonomic) Identifiers (KERI)	Specification	IETF KERI	@Samuel Smith	
SAID	Self-Addressing Identifiers	Specification	IETF Draft	@Samuel Smith	
DID KERI	KERI DID Method	Specification	Unofficial Draft Spec	@Phil Feairheller	
SIS	Schema Immutability	Specification		@Robert Mitwicki @Kevin Griffin	
CESR	Composable Event Streaming Representation	Specification	IETF CESR Draft	@Samuel Smith	
CESR Proof	CESR Proof Format	Specification		@Phil Feairheller	
IXP	Issuance Exchange Protocol	Specification		@Phil Feairheller	
PXP	Presentation Exchange Protocol	Specification		@Phil Feairheller	
PTEL	Public Transaction Event Log	Specification		@Phil Feairheller	

Authentic

authentic: having an origin supported by unquestionable evidence; authenticated; verified.

authenticity: is *the quality of being authentic; genuineness.*

authenticate: to establish the authorship or origin of conclusively or unquestionably.

authenticatable: Capable of being authenticated.

Why SAIDs

Preferred cryptographically bound self-referential identifier with agility.

SAID (Self-Addressing IDentifier) Generation Protocol
https://github.com/WebOfTrust/ietf-said

```
{
    "said": "",
    "first": "Sue",
    "last": "Smith",
    "role": "Founder",
}
```

As before the SAID will be a 44 character CESR encoded Blake-256 digest. The serialization will be JSON. The said field value in the dict is to be populated with the resulting `SAID`. First the value of the `said` field is replaced with a 44 character dummy string as follows:

```
{
    'said': '############################################',
    'first': 'Sue',
    'last': 'Smith',
    'role': 'Founder',
}
```

The dict is then serialized into JSON with no extra whitespace. The serialization is the following string:

```
{"said":"############################################","first":"Sue","last":"Smith","role":"Founder"}
```

The Blake3-256 digest is then computed on that serialization above and encoded in CESR to provide the SAID as follows:

```
EnKa0ALimLL8eQdZGzglJG_SxvncxkmvwFDhIyLFchUk
```

The value of the said field is now replaced with the computed and encoded SAID to produce the final serialization with embedded SAID as follows:

```
{"said":"EnKa0ALimLL8eQdZGzglJG_SxvncxkmvwFDhIyLFchUk","first":"Sue","last":"Smith","role":"Founder"}
```

The final serialization may be converted to a python dict by deserializing the JSON to produce:

```
{
    'said': 'EnKa0ALimLL8eQdZGzglJG_SxvncxkmvwFDhIyLFchUk',
    'first': 'Sue',
    'last': 'Smith',
    'role': 'Founder'
}
```

Top Level Structure Compact

```
{
  "v": "ACDC10JSON00011c_", # Version String Enables Different Serializations
  "d": "EBdXt3gIXOf2BBWNHdSXCJnFJL5OuQPyM5K0neuniccM",  # SAID (digest) of ACDC
  "i": "EmkPreYpZfFk66jpf3uFv7vklXKhzBrAqjsKAn2EDIPM",  # attributable ID to controlling (issuer) key state (AID, DID etc)
  "s": "E46jrVPTzlSkUPqGGeIZ8a8FWS7a6s4reAXRZOkogZ2A",  # Schema Section SAID of Schema or Embedded Schema
  "a": "EgveY4-9XgOcLxUderzwLIr9Bf7V_NHwY1lkFrn9y2PY",  # SAID of attributes section
  "p": "EgveY4-9XgOcLxUderzwLIr9Bf7V_NHwY1lkFrn9y2PY",  # SAID of provenance section
  "r": "EwLIr9Bf7V_NHwY1lkFrn9y2PYgveY4-9XgOcLxUderz",  # SAID of rules section
}
```

Top Level Structure Simple

```
{
  "v": "ACDC10JSON00011c_", # Version String Enables Different Serializations
  "d": "EBdXt3gIXOf2BBWNHdSXCJnFJL5OuQPyM5K0neuniccM",  # SAID of ACDC
  "i": "EmkPreYpZfFk66jpf3uFv7vklXKhzBrAqjsKAn2EDIPM",  # attributable ID to controlling (issuer) key state (AID,DID etc)
  "s": "E46jrVPTzlSkUPqGGeIZ8a8FWS7a6s4reAXRZOkogZ2A",  # Schema Section SAID of Schema or Embedded Schema
  "a": {  # Data Attributes Section SAID of attributes or Embedded attributes
    "d": "EgveY4-9XgOcLxUderzwLIr9Bf7V_NHwY1lkFrn9y2PY",
    "i": ":EQzFVaMasUf4cZZBKA0pUbRc9T8yUXRFLyM1JDASYqAA",  # subject or issues identifier
    "attribute": "254900OPPU84GM83MG36",
  },
  "p": [  # provenance section
    {
      "qualifiedvLEIIssuervLEICredential": {
        "d": "EIl3MORH3dCdoFOLe71iheqcywJcnjtJtQIYPvAu6DZA",  # SAID of chained (provenanced) ACDC
        "i": "Et2DOOu4ivLsjpv89vgv6auPntSLx4CvOhGUxMhxPS24"  # attributable identifier (issuer)
      }
    }
  ],
  "r": [  # rules section
    ]
}
```

Top Level Structure More Fields

```
{
  "v": "ACDC10JSON00011c_", # Version String Enables Different Serializations
  "d": "EBdXt3gIXOf2BBWNHdSXCJnFJL5OuQPyM5K0neuniccM",  # SAID of ACDC
  "i": "EmkPreYpZfFk66jpf3uFv7vklXKhzBrAqjsKAn2EDIPM",  # attributable ID to controlling (issuer) key state (AID, DID etc)
  "s": "E46jrVPTzlSkUPqGGeIZ8a8FWS7a6s4reAXRZOkogZ2A",  # Schema Section SAID of Schema or Embedded Schema
  "a": {  # Data Attributes Section SAID of attributes or Embedded attributes
    "d": "EgveY4-9XgOcLxUderzwLIr9Bf7V_NHwY1lkFrn9y2PY",
    "i": ":EQzFVaMasUf4cZZBKA0pUbRc9T8yUXRFLyM1JDASYqAA",  # subject or issues identifier
    "dt": "2021-06-09T17:35:54.169967+00:00",  # datetime of issuance
    "ri": ":EymRy7xMwsxUelUauaXtMxTfPAMPAI6FkekwlOjkggt",  # Registry Identifier
    "LEI": "254900OPPU84GM83MG36",
    "t": [ # type section
      "VerifiableCredential",
      "LegalEntityvLEICredential"
    ]
  },
  "p": [  # provenance section
    {
      "qualifiedvLEIIssuervLEICredential": {
        "d": "EIl3MORH3dCdoFOLe71iheqcywJcnjtJtQIYPvAu6DZA",  # SAID of chained (provenanced) ACDC
        "i": "Et2DOOu4ivLsjpv89vgv6auPntSLx4CvOhGUxMhxPS24"  # attributable identifier (issuer)
      }
    }
  ],
  "r": [  # rules section
    {
      "usageDisclaimer": "Usage of a valid Legal Entity vLEI…”
    },
    {
      "issuanceDisclaimer": "Issuance of a Legal Entity..."
    }
  ]
}
```

Top Level Structure Hidden

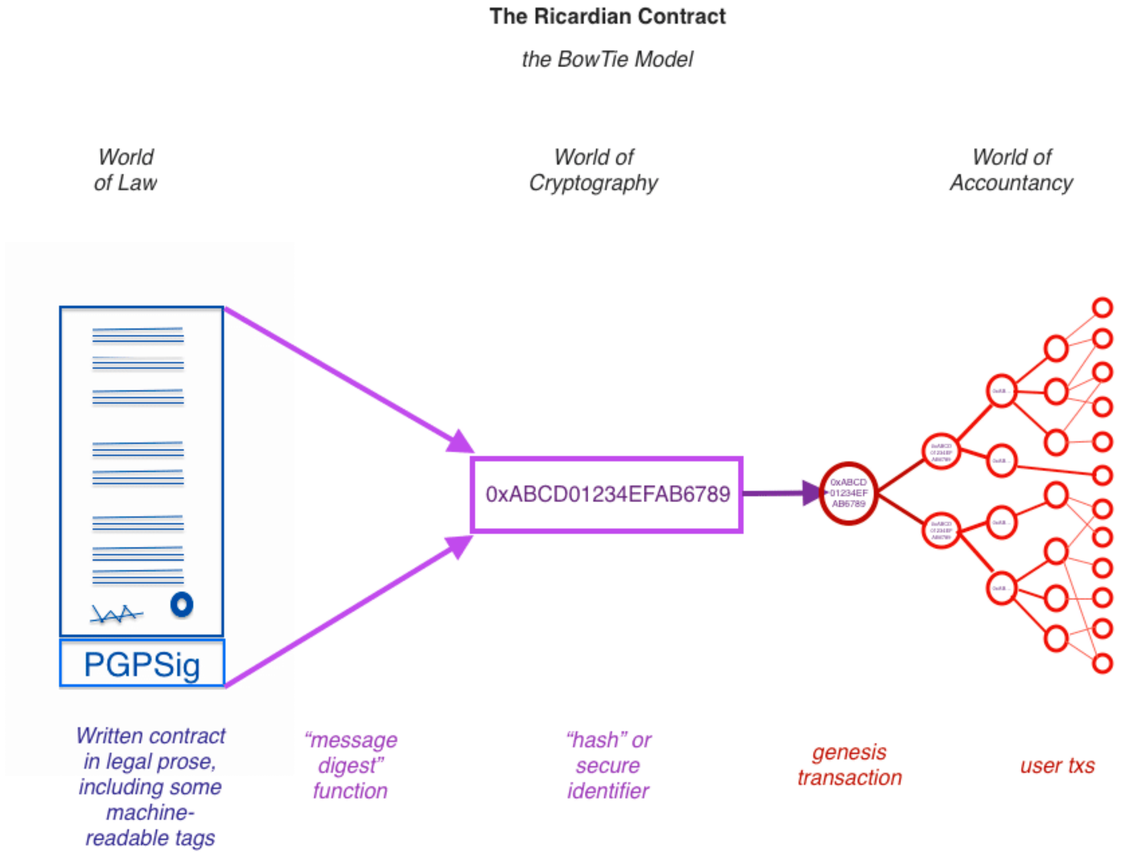
```
{
  "v": "ACDC10JSON00011c_", # Version String Enables Different Serializations
  "d": "EBdXt3gIXOf2BBWNHdSXCJnFJL5OuQPyM5K0neuniccM",  # SAID of ACDC
  "i": "EmkPreYpZfFk66jpf3uFv7vklXKhzBrAqjsKAn2EDIPM",  # attributable ID to controlling (issuer) key state (AID, DID etc)
  "s": "E46jrVPTzlSkUPqGGeIZ8a8FWS7a6s4reAXRZOkogZ2A",  # Schema Section SAID of Schema or Embedded Schema
  "a":"EgveY4-9XgOcLxUderzwLIr9Bf7V_NHwY1lkFrn9y2PY",  # non disclosed attributes
  "p": [  # provenance section
    {
      "qualifiedvLEIIssuervLEICredential": {
        "d": "EIl3MORH3dCdoFOLe71iheqcywJcnjtJtQIYPvAu6DZA",  # SAID of chained (provenanced) ACDC
        "i": "Et2DOOu4ivLsjpv89vgv6auPntSLx4CvOhGUxMhxPS24"  # attributable identifier (issuer)
      }
    }
  ],
  "r": [  # rules section
    {
      "usageDisclaimer": "Usage of a valid Legal Entity vLEI…"
    },
    {
      "issuanceDisclaimer": "Issuance of a Legal Entity..."
    }
  ]
}
```

Top Level Structure Un-Hidden

```
{
  "v": "ACDC10JSON00011c_", # Version String Enables Different Serializations
  "d": "EBdXt3gIXOf2BBWNHdSXCJnFJL5OuQPyM5K0neuniccM",  # SAID of ACDC
  "i": "EmkPreYpZfFk66jpf3uFv7vklXKhzBrAqjsKAn2EDIPM",  # attributable ID to controlling (issuer) key state (AID, DID etc)
  "s": "E46jrVPTzlSkUPqGGeIZ8a8FWS7a6s4reAXRZOkogZ2A",  # Schema Section SAID of Schema or Embedded Schema
  "a": {  # Data Attributes Section SAID of attributes or Embedded attributes
    "d": "EgveY4-9XgOcLxUderzwLIr9Bf7V_NHwY1lkFrn9y2PY",
    "i": "EQzFVaMasUf4cZZBKA0pUbRc9T8yUXRFLyM1JDASYqAA",  # subject or issues identifier
    "n": "0ANghkDaG7OY1wjaDAE0qHcg",  # Nonce field
    "dt": "2021-06-09T17:35:54.169967+00:00",  # datetime of issuance
    "ri": ":EymRy7xMwsxUelUauaXtMxTfPAMPAI6FkekwlOjkggt",  # Registry Identifier
    "LEI": "254900OPPU84GM83MG36",
    "t": [ # type section
      "VerifiableCredential",
      "LegalEntityvLEICredential"
    ]
  },
  "p": [  # provenance section
    {
      "qualifiedvLEIIssuervLEICredential": {
        "d": "EIl3MORH3dCdoFOLe71iheqcywJcnjtJtQIYPvAu6DZA",  # SAID of chained (provenanced) ACDC
        "i": "Et2DOOu4ivLsjpv89vgv6auPntSLx4CvOhGUxMhxPS24"  # attributable identifier (issuer)
      }
    }
  ],
  "r": [  # rules section
    {
      "usageDisclaimer": "Usage of a valid Legal Entity vLEI…"
    },
    {
      "issuanceDisclaimer": "Issuance of a Legal Entity..."
    }
  ]
}
```

Hidden NDA

Presentation Exchange receipts the NDA in the rules section before disclosing the attributes section.



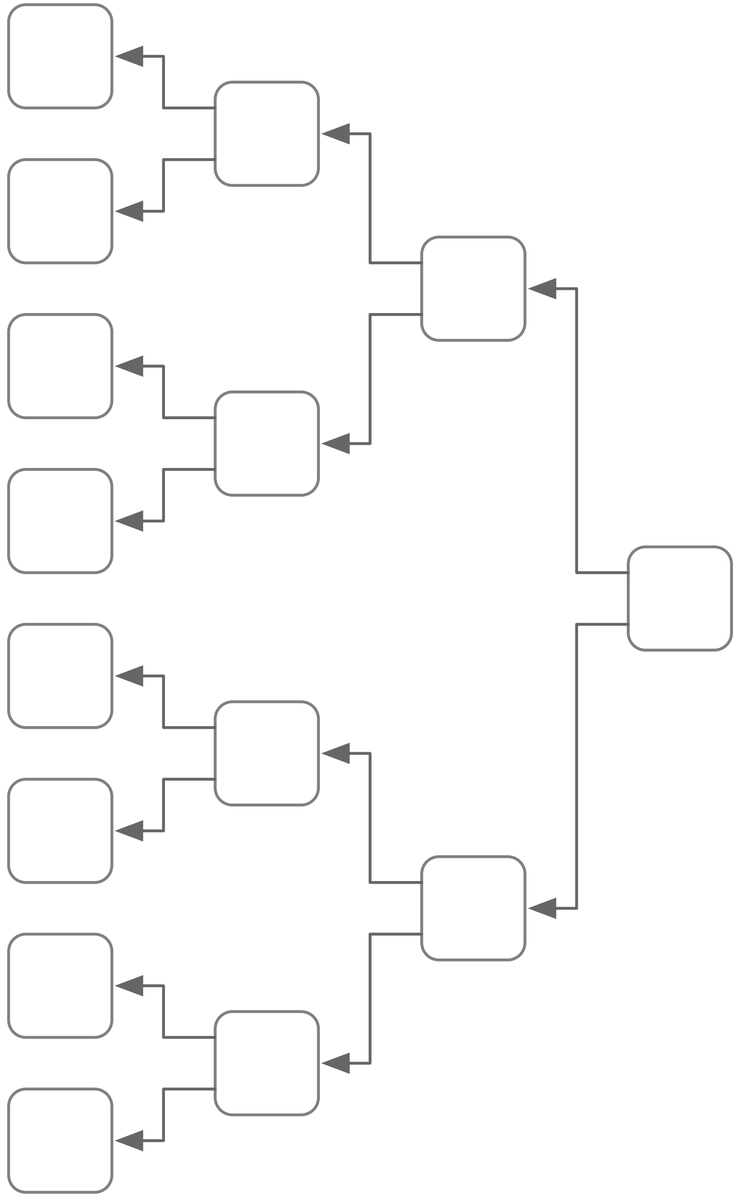
Authentic = Provenanced = Securely Attributed

Securely Attributed:

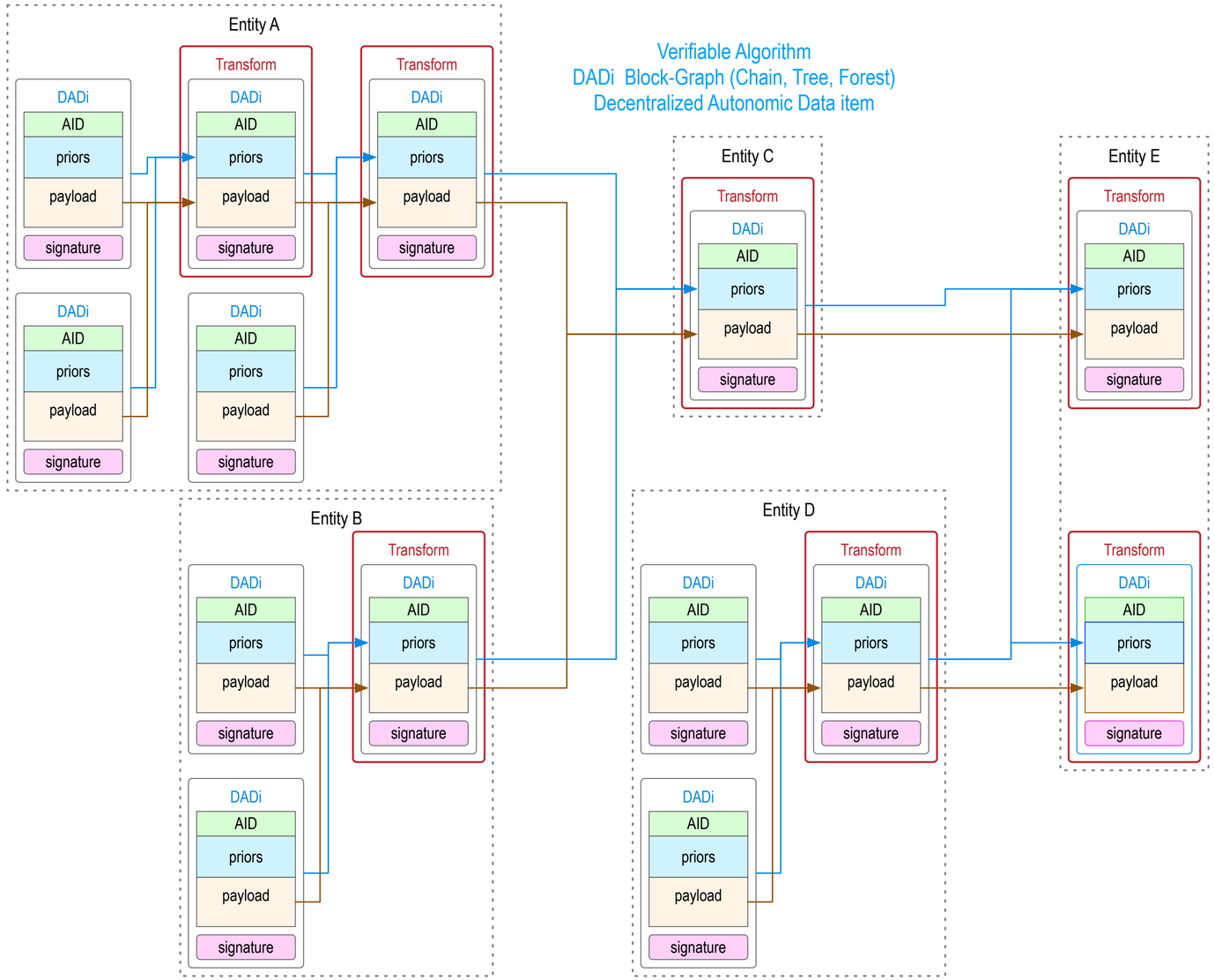
Nonrepudiably Authenticated via Digital Signatures

Secure Attribution Provenance:

Chain, Tree, or Graph



Provenance Semantics: Chaining and Rules



Authenticity Verification (Attribution/Provenance) Model Properties

Bipartite vs. Tripartite vs. Multipartite

Open Loop vs. Closed Loop

Chained vs. Unchained

Aggregative vs. Unaggregative

Weighted vs. Unweighted (Qualified vs Unqualified)

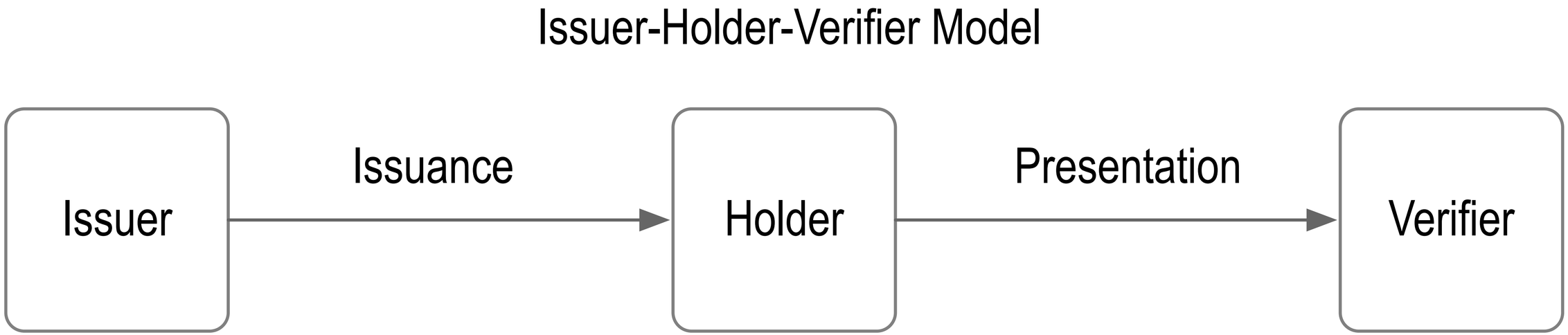
Attenuable vs. Unattenuable

Persistent vs. Ephemeral

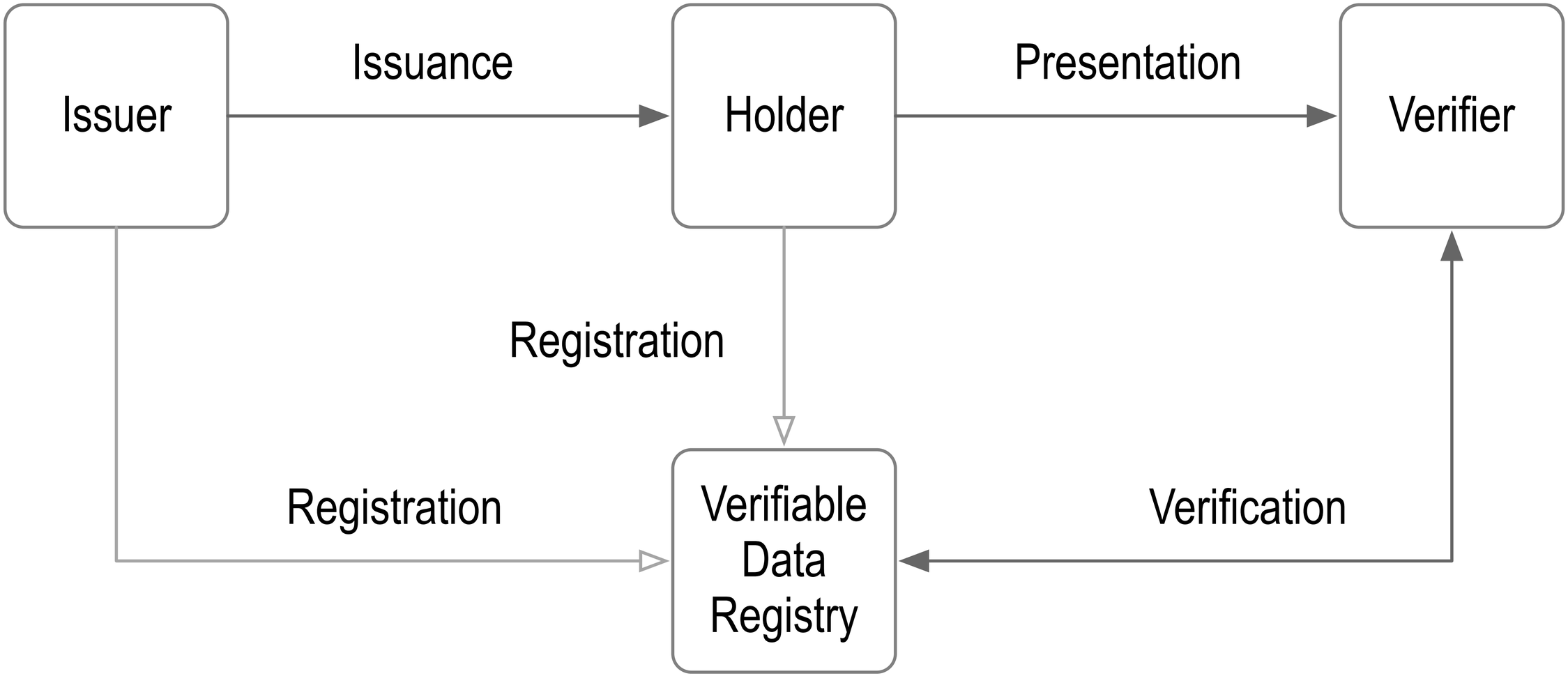
Implicit vs. Explicit

Cooperative vs. Uncooperative (Unilateral vs. Bilateral vs. Multilateral)

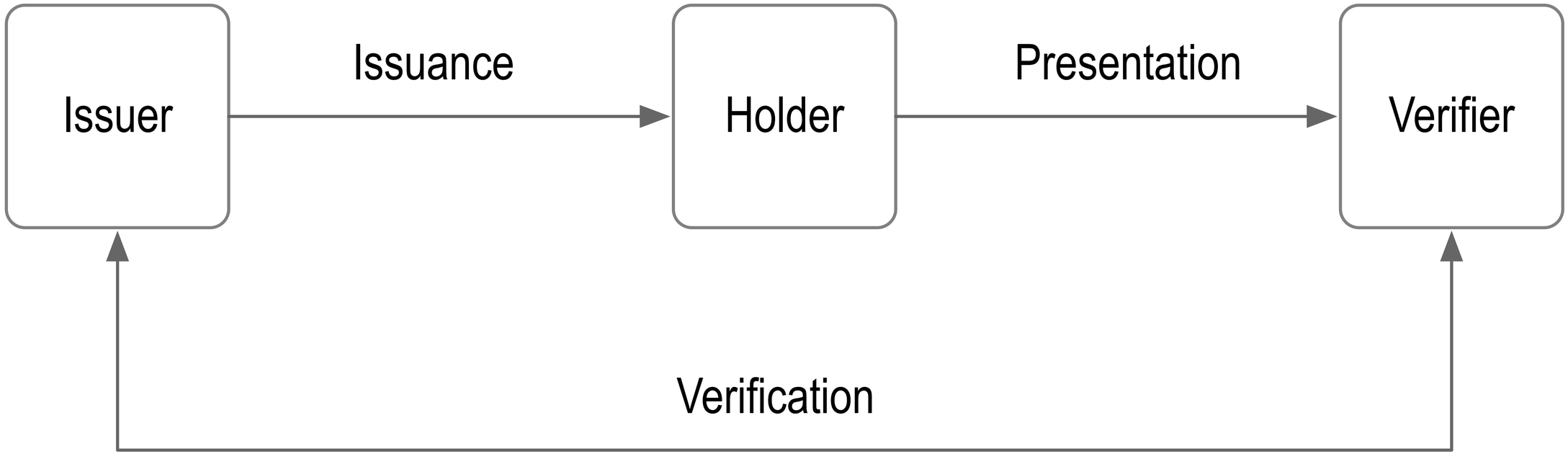
Entrained vs. Unentrained


Issuer-Holder-Verifier Model
Issuer
Issuance
Holder
Presentation
Verifier

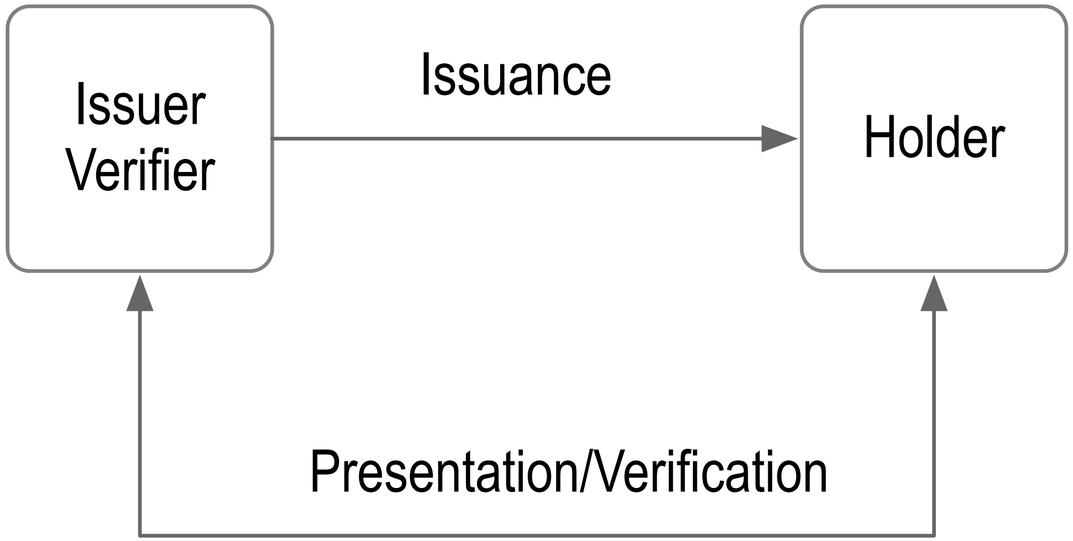
Issuer-Holder-Verifier Model with Verification at Verifiable Data Registry

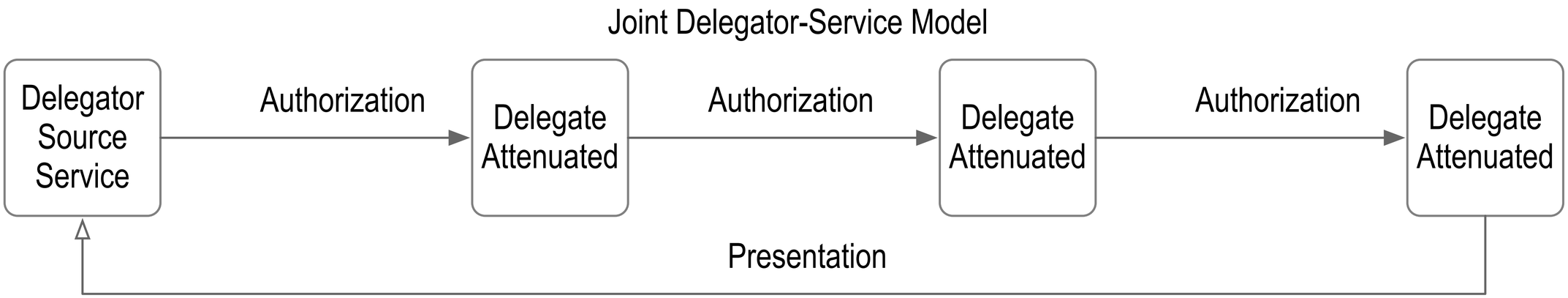


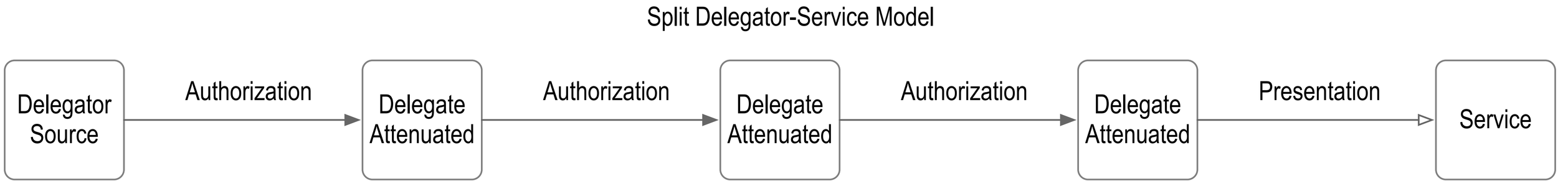
Issuer-Holder-Verifier Model with Verification at Issuer



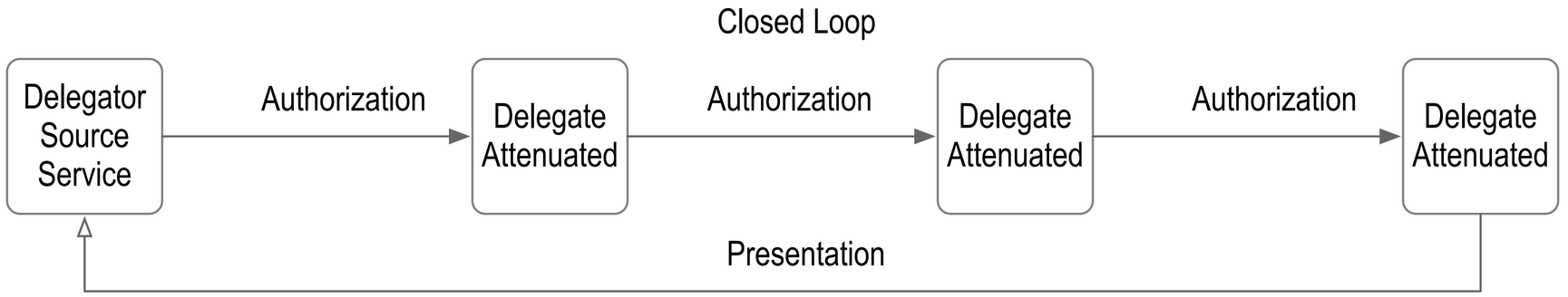
Issuer-Holder Model with Verification at Issuer

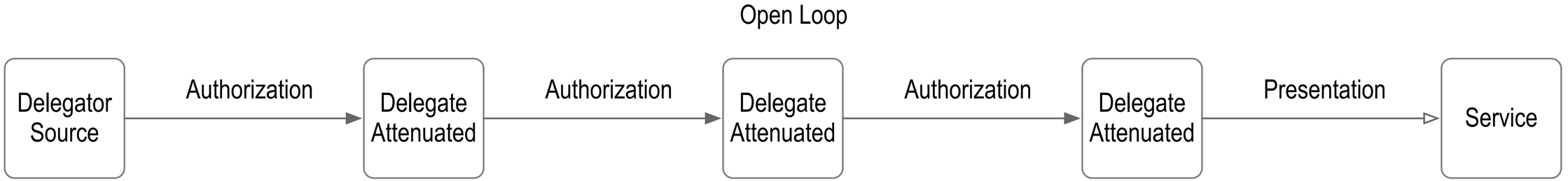


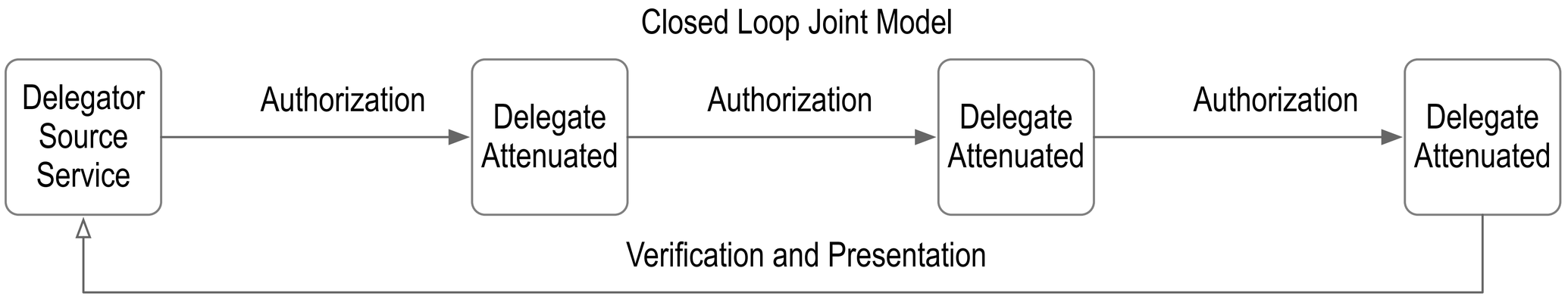

Joint Delegator-Service Model
Delegator Source Service
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Presentation

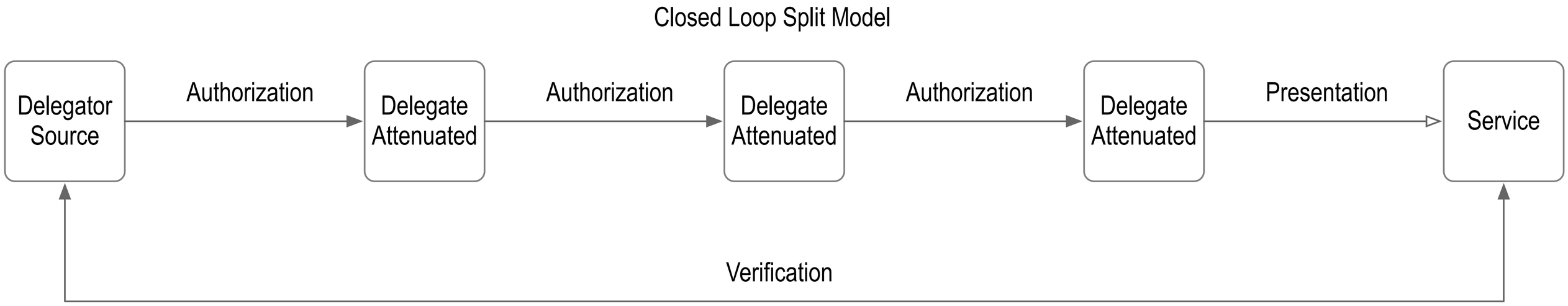

Split Delegator-Service Model
Delegator Source
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Presentation
Service

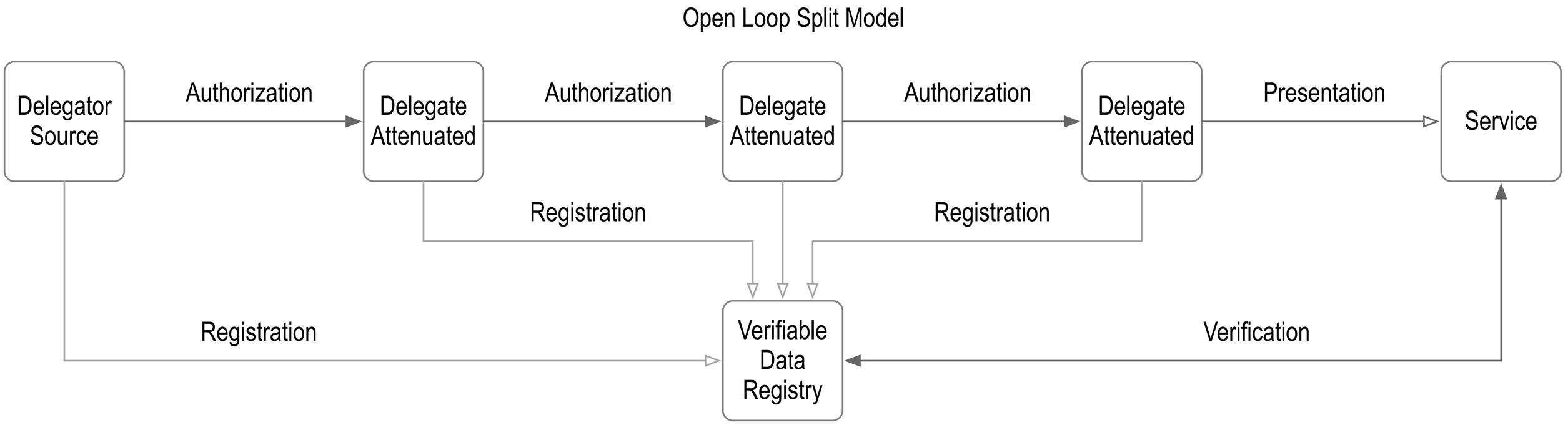
Closed vs Open Loop






Closed Loop Joint Model
Delegator Source Service
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Verification and Presentation


Closed Loop Split Model
Delegator Source
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Presentation
Service
Verification


Open Loop Split Model
Delegator Source
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Authorization
Delegate Attenuated
Presentation
Service
Registration
Registration
Registration
Verifiable Data Registry
Verification

Its all about Automated Reasoning

Automated Business Process Workflows as Automated Decision Processes

Secure Attribution is essential to cross entity decision processes and cross entity data supporting those decision processes.

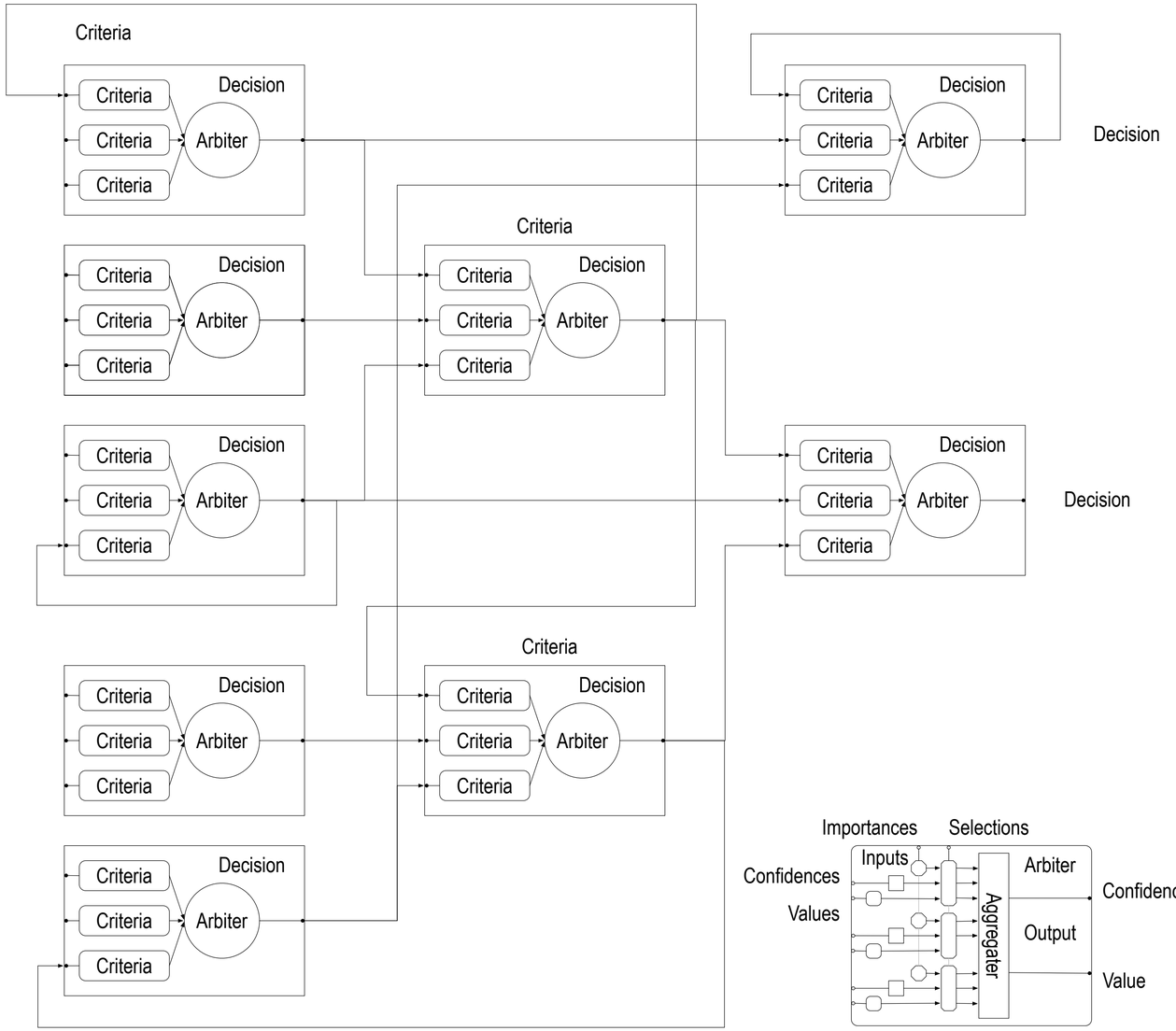
Decentralized Automated Decision Making depends on securely attributable decision process data flows.

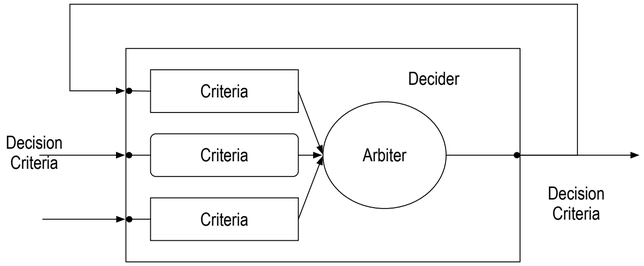
Secure Attribution provided by a portable decentralized identity system security overlay for data in motion and at rest.

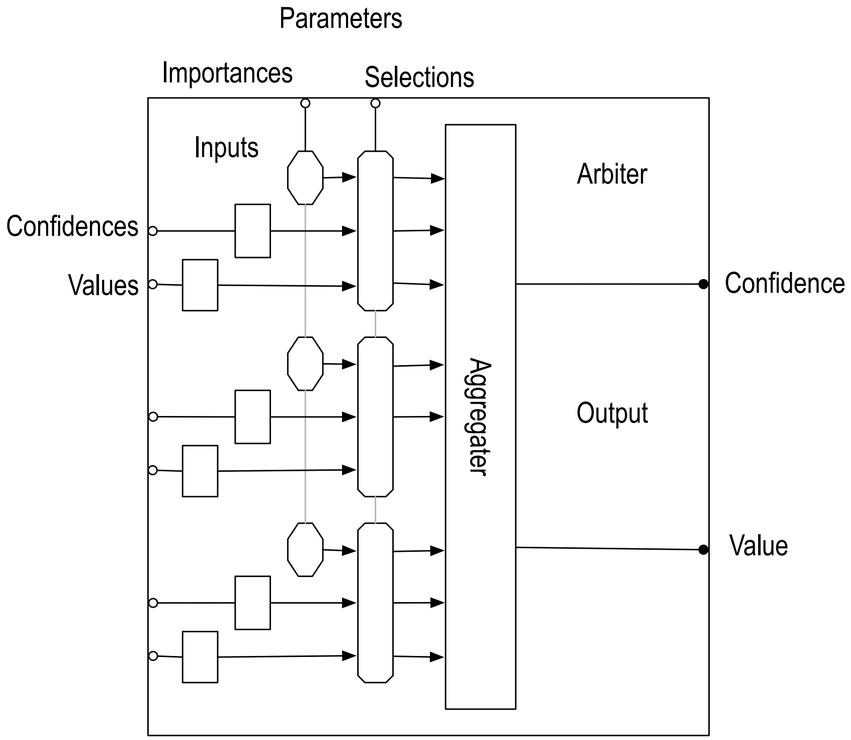
Automated Reasoning *with* *Authentic Data*

Decision Making: finding actions that best satisfy goals and constraints

Provenance Semantics: Chaining and Rules







Attribution Chain

Super semantic is an attribution chaining semantic.

Need first make secure attribution of source of information = issuers of ADC

Attribution tree (aggregation)

Then once we have made secure attribution to issuers (AID KERI etc)

Then we can color the edges of the attribution tree with layered semantic

Provenance Tree/Chain

Delegation Tree/Chain

Attestation Tree/Chain

Etc.

Cooperative Delegation Relationship

Authority flows source to sink (down or left to right)

Credence (trust) flows sink to source (up or right to left)

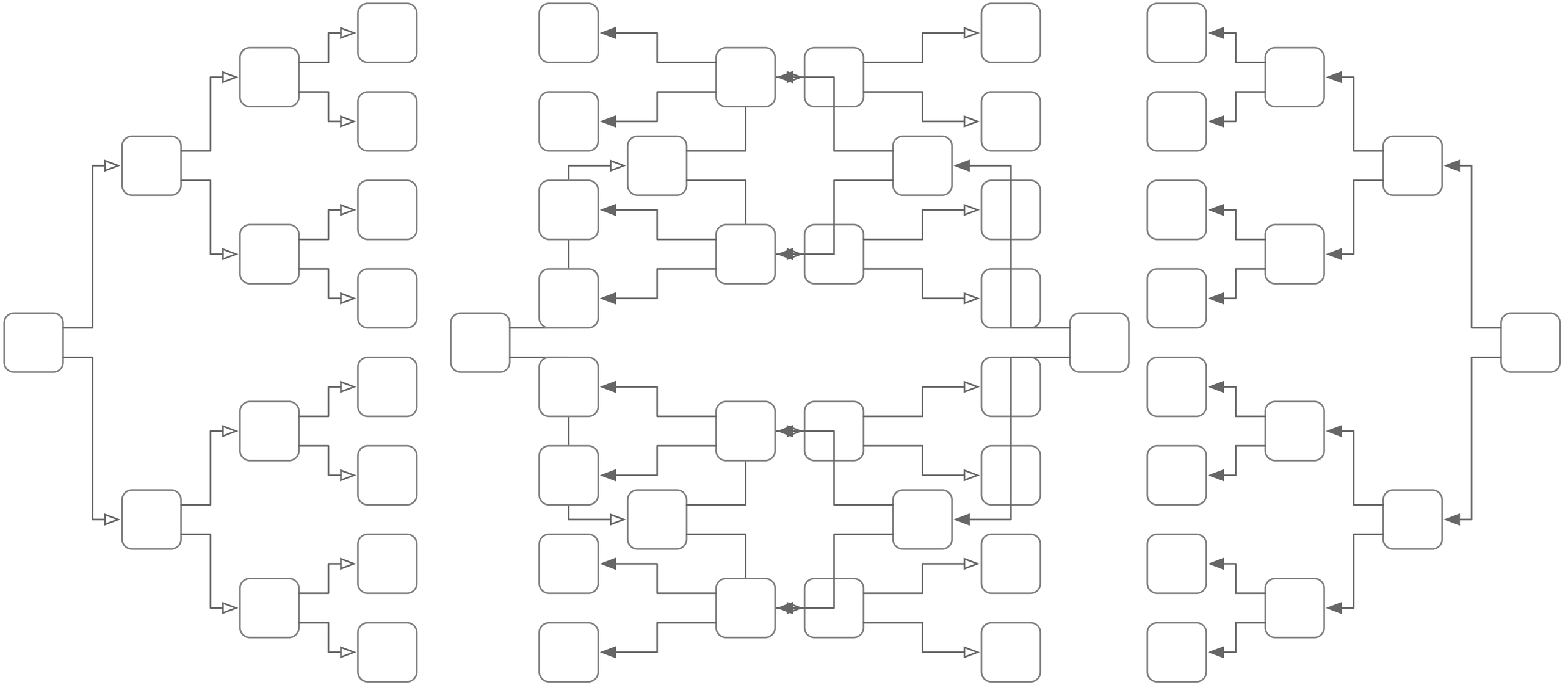
Provenance requires tracing relationships both ways

Cooperative delegation flows both ways.

Delegator sends authority to Delegate.

Delegate sends credence to Delegator.

Cooperative Delegation



Cooperative Verification Relationship

Delegator has rules (constraints)

Delegate has rules (objectives)

Verifier has rules (constraints and objectives)

Authorization success upon the conjoint satisfaction of the three sets of rules

Authorization success upon the satisfaction of rule chain

Background

Weighted Aggregation of Authorizations

Analogous to thresholded multi-signature

$$\widehat{C}_l = \left[C_l^1, \ldots, C_l^{L_l} \right]_l \quad \widehat{K}_l = \left[U_l^1, \ldots, U_l^{L_1} \right]_l \quad 0 < U_l^j \leq 1 \quad \bar{U}_l = \sum_{i=s_0}^{s_{S_k-1}} U_l^i \geq 1 \quad \widehat{s}_k^l = \left[s_0, \ldots, s_{S_k^l-1} \right]_k^l$$

$$\widehat{C} = \left[C^1, C^2, C^3 \right] \qquad U_l^j = 1/K_l \qquad \widehat{K} = \left[1/2, 1/2, 1/2 \right]$$

$$\widehat{K}_l = \left[1/2, 1/2, 1/4, 1/4, 1/4, 1/4 \right]_l$$

$$\widehat{K}_l = \left[\left[1/2, 1/2, 1/4, 1/4, 1/4, 1/4 \right], \left[1/2, 1/2, 1/2, 1/2 \right], \left[1, 1, 1, 1 \right] \right]$$

Terminology

credential: *evidence of authority, status, rights, entitlement to privileges, or the like.*

license: *formal permission from a constituted authority to do something, as to carry on some business or profession.*

a certificate, tag, plate, etc., giving proof of such permission; official permit: a driver's license.

authorization: *permission or power granted by an authority; sanction.*

In decision making context, *authentic credential* = *proof of satisfaction of authority constraint*