Addressability is The Missing Link (in the Web of Trust)

LinkedClaims: An Open Standard for Addressable Claims

Golda Velez[1], ...[2], and Agnes Koinange[1]

[1]LinkedTrust, [2]...

January 20, 2025

Abstract

Trust and credibility of information is critical to a functioning society. While cryptographic signing and blockchain validation provide technical verification, they are insufficient to predict the truth of an assertion. This paper introduces LinkedClaims, an open standard for addressable claims that enables cross-domain credibility assessment. We present the technical specification, analyze existing implementations across diverse domains, and outline the ecosystem development pathway.

1 Executive Summary

"**Resistance to lies** continues to be the first step in the pursuit of freedom from fear and coercion" [1] - nobel prize winner Liu Xiaobo centers the ability to resist lies as the core effort that anyone can make towards a free society. Clearly sharing information online by itself, can accelerate the dissemination of truth OR lies - or various shades of misinformation. The question, then, is what type of technical specification can enable resistance to lies - what enables each viewer to assess for themselves the credibility of what they see, and if desired to add their assessment in a meaningful way?

How do people decide what to believe? The tendency to believe statements that align with our existing beliefs, without the ability to check evidence, has pernicious consequences. Making it easy to **examine** the chain of trust and the evidence with some confidence, as well as to **add** into that chain in a way that others can inspect, are two key elements we want to recognize and enable. Therefore we start with three MUST requirements:

- A LinkedClaim MUST be cryptographically signed, such as with a DID. This allows a viewer to inspect at least who has signed the claim and thus staked some of their credibility.
- A LinkedClaim MUST **itself have an identifier** that is a well-formed URI. This allows anyone to make at attestation ABOUT the claim itself, whether to support, reject or qualify it.
- A LinkedClaim MUST have a subject that can be any valid URI. This allows two claims to be clearly made about the same subject, and for subjects to be clearly connected to each other.

In many cases, the user of the technology will not be the one who has first hand knowledge about the claim. Thus it is important also to provide a source or evidence, and it is desireable for that evidence to be tamper proof, leading to the first SHOULD

- SHOULD contain evidence such as links to a source or attachments, optionally hashlinked

In this paper, we will examine current, compelling real world use cases for LinkedClaims, as well as existing technical implementations that ALREADY qualify under the proposed standard. We will expand on these first requirements to the full specification of LinkedClaims Conformance Requirements published at the Decentralized Identify Foundation Lab.

Finally, we will demonstrate that conformance to the LinkedClaims requirements allows the connection of claims created with different technical implementations and in different domains to be combined in a credibility assessment that can result in greater confidence than examining one focus domain alone.

2 Introduction: Case Studies Across Domains

Independent verification of claims is needed in many disparate domains.

2.1 Philanthropy: Candid.org

At Candid, a simple and frequent issue is to identify whether the claimant to administer a profile is genuinely a representative of the nonprofit.

2.2 Skill and Experience Credentials: T3 Innovation Network

Individuals outside of traditional academia often lack a way to validate the skills they have attained in a reliable digital manner. The T3 Innovation Network, in cooperation with LinkedTrust and the US Chambers of Commerce Foundation, has developed a system of self-attested credentials that can be self-signed and linked to recommender validations that are separately signed and linked to the original claim.

2.3 Climate Action: Open Forest Protocol

Carbon credits are notoriously subject to false claims, as well as excessive bureaucracy for real forestry projects. Open Forest Protocol has developed a simple app for gathering the required data for tree growth in a reliable way, and enables independent validators to attest to the quality of the data.

2.4 Supply Chain

2.5 Digital Identity

2.6 Proof of Personhood Credentials (PHC)

2.7 Universal Media Identifiers (UMiD)

3 Sources of Trust and Risk Assessments

3.1 Issuer Registries and Progressive Trust

Progressive Trust is a key concept.

3.2 Risk Assets as a Concept

.. in the Risk profession, there is the concept of the 'assets' of an attacker, being any long-lived entity where trust may be assigned: an IP address, device address, card fingerprint, login, email, and similar ..

3.3 Reliance on DNS

3.4 Blockchain and Incentive Mechanisms

4 Technical Specification

4.1 URI-addressability Requirements

4.2 Hashability and Content Integrity

4.3 Concept of Inbox

4.4 Desired Fields

4.5 Privacy Preservation and Access Control

5 Implementation Analysis

5.1 Reference Implementation

The minimal semantic vocabulary defined at http://cooperation.org/credentials/v1/ may be used for new implementations or as a 'glue' to connect existing addressable claims.

5.2 Recognition of Existing Compliant Systems

5.2.1 Philanthropy: Candid.org

..vocab used, json example..

5.3 Skill and Experience Credentials: T3 Innovation Network

..OBV3, json example, links..

5.4 Climate Action: Open Forest Protocol

..address to atlas, address to NEAR Protocol signed data..

5.5 Supply Chain

..the id standard..

5.6 Digital Identity

..

5.7 Proof of Personhood Credentials (PHC)

..

5.8 Universal Media Identifiers (UMiD)

..

5.9 Profile and Mappings

5.10 Compliance Testing Framework

5.11 Open Source Libraries

5.12 Private Data Handling Patterns

6 Technical Aspects

6.1 Issuer Registries

6.2 Blockchain vs Verifiable Credentials

6.3 Publishing and Discoverability

6.3.1 Ceramic Network

6.3.2 ATProto

7 Community Applications & Use Cases

7.1 Current Implementations

7.2 Network Effects

7.3 Cross-domain Benefits

A widely used, heterogeneous trust network will be more robust against attack, and will enable important but rare applications.

7.4 Public/Private Data Models

8 Ecosystem Development

8.1 Integration Pathways

8.2 Partnership Examples

8.3 Network Growth Patterns

8.4 Commercial Implementation Opportunities

8.5 Value Capture Models

8.6 Marketplace Dynamics

9 Technical Roadmap

9.1 Standards Development

9.2 Research Directions

9.3 Open Challenges

9.4 Community Contribution Framework

9.5 Commercial Extension Patterns

References

[1] Liu Xiaobo. Using truth to undermine a system of lies. In *No Enemies, No Hatred: Selected Essays and Poems*. Belknap Press, 2013.

A Technical Implementation Details

B Integration Examples

C Security Considerations