URL-Based Credential Chaining for Transitive Trust Graphs

Ramprasad Anandam Gaddam
Vouch Protocol Project
https://vouch-protocol.com
ram@vouch-protocol.com

January 2026

Abstract

This paper presents a method for constructing verifiable trust graphs using URL-based credential references. Credentials embed URLs pointing to issuer credentials, parent attestations, and supporting evidence. Verifiers traverse these URL chains to construct a complete trust graph, evaluating aggregate trustworthiness based on all participants' credentials. We formalize the trust graph model, define the credential schema with URL references, specify the graph traversal algorithm, and analyze security properties including cycle detection and depth limiting.

This paper is part of the Vouch Protocol Defensive Disclosure Series. Full index: https://vouch-protocol.com/docs/disclosures/

Keywords: trust graphs, credential chaining, transitive trust, web of trust, URL dereferencing

1 Introduction

Trust is inherently transitive: if Alice trusts Bob, and Bob vouches for Carol, Alice may extend partial trust to Carol. Traditional credential systems are flat—a single issuer vouches for a subject. Real-world trust involves chains of endorsements, evidence, and cross-references.

We present a credential chaining system where each credential contains URL references to supporting credentials. By following these URLs, a verifier can construct a complete trust graph and compute aggregate trust scores.

1.1 Contributions

- Formal model for URL-linked trust graphs
- Credential schema with embedded URL references
- Graph traversal algorithm with cycle detection
- Trust score aggregation framework

2 Background

2.1 Trust Models

Definition 1 (Direct Trust). *Direct trust is a binary or weighted relation* $T(A, B) \in [0, 1]$ *indicating A's trust in B.*

Definition 2 (Transitive Trust). *Transitive trust propagates through intermediaries:*

$$T(A, C) = f(T(A, B), T(B, C)) \tag{1}$$

where f is a trust propagation function (e.g., multiplication, minimum).

2.2 Web of Trust

The PGP Web of Trust [Zimmermann, 1995] established transitive trust through key signatures. Our work extends this concept to action attestations with richer credential semantics.

3 Trust Graph Model

3.1 Graph Structure

Definition 3 (Trust Graph). *A trust graph $G = (V, E)$ where:*

- *V: Set of credentials (nodes)*
- *E: Set of URL references (directed edges)*

3.2 Credential Schema

```
{
  "type": "attestation",
  "claim": "completed_task_xyz",
  "subject": "did:web:bob.example.com",
  "issuer": "did:web:taskmanager.example.com",
  "supporting_urls": {
    "issuer_credential":
      "https://company.com/creds/tm-auth.json",
    "parent_attestation":
      "https://chain.com/attest/parent.json",
    "evidence": [
      "https://logs.com/exec/task.json"
    ]
  },
  "signature": "eyJhbGciOiJFZERTQSJ9..."
}
```

3.3 URL Reference Types

- **issuer_credential**: Credential authorizing the issuer to make this claim
- **parent_attestation**: Credential from which this one derives
- **evidence**: Supporting documents or logs

4 Graph Traversal Algorithm

4.1 Recursive Fetch and Verify

1. Start with target credential C_0
2. Verify $\mathsf{signature}(C_0)$
3. For each URL u in $C_0.\mathsf{supporting\_urls}$:

(a) If $u \in \mathsf{visited}$: Skip (cycle detection)

(b) Fetch credential C_u from u

(c) Add u to $\mathsf{visited}$

(d) Recursively traverse C_u

4. If depth exceeds $\mathsf{max\_depth}$: Stop

5. Construct graph G from traversed credentials

4.2 Depth Limiting

Property 1 (Bounded Traversal)**.** *Traversal terminates within $O(d \cdot b)$ fetches where d is max depth and b is max branching factor.*

Recommended limits: $d = 5$, $b = 10$.

5 Trust Score Computation

5.1 Score Aggregation

Given graph G, compute trust score:

$$\mathsf{score}(C_0) = \sum_{p \in \mathsf{paths}(C_0, \mathsf{root})} \prod_{e \in p} w(e) \tag{2}$$

where $w(e)$ is edge weight based on:

- Issuer reputation
- Credential freshness
- Evidence quality

6 Security Analysis

Property 2 (Signature Verification)**.** *Every fetched credential is cryptographically verified before inclusion in the trust graph.*

Property 3 (Cycle Rejection)**.** *Circular references are detected and do not increase trust scores.*

Threat: Compromised URLs. Mitigation: Signatures are verified independently of URL source.

Threat: URL availability. Mitigation: Cache fetched credentials with TTL.

7 Related Work

Verifiable Credentials [Sporny et al., 2022] provide the credential format; our work adds URL-based chaining.

Linked Data Signatures enable credential linking via JSON-LD; our approach is simpler and REST-native.

DNSSEC Chain of Trust provides hierarchical trust for DNS; our model supports arbitrary graph topologies.

8 Implementation

Reference implementation available at https://github.com/vouch-protocol/vouch.

Features:

- Recursive credential fetcher with caching
- Cycle detection and depth limiting
- Trust score visualization

9 Conclusion

This paper presented URL-based credential chaining for constructing transitive trust graphs. By embedding URL references in credentials, verifiers can discover and traverse complete trust networks. The approach enables richer trust models than single-issuer credentials while maintaining cryptographic verifiability.

Prior Art Declaration

This document is published as a defensive prior art disclosure under the Creative Commons CC0 1.0 Universal Public Domain Dedication. The methods and systems described herein are hereby released into the public domain to prevent patent monopolization. Any party implementing similar functionality after the publication date of this document cannot claim novelty for patent purposes.
Reference Implementation: https://github.com/vouch-protocol/vouch

Cryptographically Signed Document

Signed by: Ramprasad Anandam Gaddam (`github:rampyg`)
Verify: https://v.vouch-protocol.com/p/pad006

This document's authenticity can be verified by computing its SHA-256 hash and checking against the signature registered at the verification URL above.

References

Manu Sporny, Grant Noble, Dave Longley, Daniel Burnett, Brent Zundel, and Kyle Den Hartog. Verifiable Credentials Data Model v1.1. Recommendation, W3C, March 2022. URL https://www.w3.org/TR/vc-data-model/.

Philip Zimmermann. The Official PGP User's Guide. 1995.