Decentralized Identifiers
Internet-Draft
Intended status: Informational
Expires: 25 September 2026

M. Herman
Web 7.0 Foundation

24 March 2026

Decentralized Universal Resource Name (URN) DID Method (Web 7.0)
draft-herman-did-web7-urn-00

Abstract

This document specifies the did7:web7 Decentralized Identifier (DID) method, which defines a deterministic mapping from Uniform Resource Names (URNs) (RFC 8141) into a DID-compatible identifier format called a Decentralized Universal Resource Name (URN). The did7:web7 method preserves URN semantics, enables DID resolution without mandatory centralized infrastructure, and provides optional cryptographic and service-layer extensibility. The method is fully compatible with the W3C DID Core specification (W3C DID Core, 2022) and the broader DID ecosystem.

Derivation Notice

This note is to be removed before publishing as an RFC.

This Internet-Draft is derived from the Web 7.0 Foundation specification "SDO: W3C Decentralized Resource Name (URN) DID Method (Web 7.0)" authored by Michael Herman, published 24 March 2026 at https://hyperonomy.com/2026/03/24/ sdo-web-7-0-decentralized-resource-name-urn-did-method/ and licensed under the Creative Commons Attribution-ShareAlike 4.0 International Public License. Web 7.0(TM), Web 7.0 DIDLibOS(TM), TDW AgenticOS(TM), TDW(TM), Trusted Digital Web(TM), and Hyperonomy(TM) are trademarks of the Web 7.0 Foundation.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

Uniform Resource Names (URNs) [RFC8141] provide a well-established mechanism for assigning persistent, location-independent identifiers to resources. However, URNs predate the Decentralized Identifier (DID) ecosystem [W3C.DID-CORE] and lack native support for DID resolution, DID Document retrieval, cryptographic verification methods, or service endpoint declaration.

At the same time, many existing information systems such as bibliographic catalogues, digital libraries, standards registries, and supply-chain systems rely heavily on URN-based identification. Retrofitting these systems with entirely new identifier schemes is often impractical.

The did7:web7 method bridges this gap. It defines a deterministic, reversible transformation from any well-formed URN into a DID-compatible identifier called a Decentralized Universal Resource Name (URN). The resulting DID is fully resolvable, is backwards compatible with the source URN, requires no mandatory centralized registry, and is composable with other DID methods such as did:key, did:web, and did:peer.

The primary design goals of did7:web7 are:

* Preservation of URN semantics and namespace-specific comparison rules.

* Deterministic, stateless baseline resolution requiring no external infrastructure.

* Optional cryptographic extensibility through verification methods.

* Optional service-layer extensibility through service endpoints.

* Full conformance with the W3C DID Core specification [W3C.DID-CORE].

The did7:web7 method is positioned as a universal adapter between the URN and DID ecosystems, serving as a semantic identity bridge that preserves existing meaning while enabling participation in the modern decentralized identity landscape.

2. Conventions and Definitions

The key words MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, NOT RECOMMENDED, MAY, and OPTIONAL in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals as shown here.

ABNF notation used in this document follows [RFC5234].

3. Terminology

URN (Uniform Resource Name): A persistent, location-independent identifier conforming to the syntax defined in [RFC8141], of the form urn:<NID>:<NSS>.

NID (Namespace Identifier): The registered URN namespace label (e.g., isbn, uuid, ietf).

NSS (Namespace-Specific String): The portion of a URN following the NID, interpreted according to the rules of the corresponding URN namespace registration.

URN (Decentralized Universal Resource Name): A URN expressed within the did7:web7 method namespace; the method-specific identifier portion of a did7:web7 DID.

DID Document: A set of data describing the DID subject, as defined in Section 5 of [W3C.DID-CORE].

Resolver: A software component that, given a DID, returns a DID Document conforming to the requirements of [W3C.DID-RESOLUTION].

Controller: An entity, as identified by a DID, that has the capability to make changes to a DID Document, as defined in [W3C.DID-CORE].

Fingerprint: A cryptographic hash of a canonical representation of the embedded URN, used to derive a did:key-compatible equivalent identifier.

4. Method Name

The method name that identifies this DID method is: urn.

A DID conforming to this specification begins with the prefix did7://web7/. This prefix is case-insensitive for resolution purposes, but implementations SHOULD produce lowercase prefixes in all output.

5. Method-Specific Identifier

5.1. Syntax

The ABNF grammar for a did7:web7 DID is as follows:

```
did-web7-urn = "did7://web7/" urn
urn     = "urn:" NID ":" NSS
NID     = <URN Namespace Identifier per RFC 8141>
NSS     = <Namespace-Specific String per RFC 8141>
```

The following are conformant examples of did7:web7 identifiers:

```
did7://web7/urn:isbn:9780141036144
did7://web7/urn:uuid:6ba7b810-9dad-11d1-80b4-00c04fd430c8
did7://web7/urn:ietf:rfc:8141
did7://web7/urn:epc:id:sgtin:0614141.107346.2017
```

5.2. Normalization

Implementations MUST normalize the embedded URN according to the lexical equivalence and case-folding rules specified in Section 3.1 of [RFC8141] before constructing or comparing a did7:web7 identifier. Namespace-specific comparison rules (q-component handling, etc.) as registered with IANA for each NID MUST also be preserved.

Percent-encoding normalization (Section 2.1 of [RFC3986]) applies to the NSS component where permitted by the applicable namespace registration.

6. Core Properties

6.1. Determinism

A given URN MUST map deterministically to exactly one did7:web7 identifier. The transformation is purely syntactic; no randomness or external state is introduced. Two URNs that are lexically equivalent per [RFC8141] MUST produce the same did7:web7.

6.2. Reversibility

The original URN MUST be exactly recoverable from the did7:web7 identifier without loss of information. No encoding, hashing, or irreversible transformation is applied to the URN content.

6.3. Infrastructure Independence

Baseline resolution of a did7:web7 identifier MUST NOT require access to any centralized registry, distributed ledger, or network service. A conformant resolver MUST be capable of constructing a minimal conformant DID Document entirely from the information contained within the DID string itself (see Mode 1, Section 7.3).

7. DID Resolution

7.1. Resolution Input

The resolution input is a did7:web7 string conforming to the syntax defined in Section 5.1, optionally accompanied by resolution options as defined in [W3C.DID-RESOLUTION].

Input: did7://web7/<urn>

7.2. Resolution Output

A conforming resolver MUST return a DID Document. The minimum conformant DID Document for any did7:web7 identifier is:

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did7://web7/urn:isbn:9780141036144",
  "alsoKnownAs": [
    "urn:isbn:9780141036144"
  ]
}
```

The alsoKnownAs property MUST contain the embedded URN in its normalized form (per Section 5.2).

7.3. Resolution Modes

7.3.1. Mode 1 - Stateless Resolution (REQUIRED)

A conformant resolver MUST support stateless resolution. In this mode the resolver constructs the DID Document locally from the DID string alone, without any external network lookup.

Properties of this mode:

* Fully deterministic.

* Zero infrastructure dependency.

* Always available regardless of network connectivity.

7.3.2. Mode 2 - Deterministic Fingerprint (RECOMMENDED)

Resolvers SHOULD support derivation of a cryptographic fingerprint from the canonical URN. The fingerprint is derived as:

fingerprint = hash(canonical-urn)

where canonical-urn is the normalized URN string (UTF-8 encoded) and hash is a cryptographic hash function registered for use with did:key (e.g., SHA-256 with multibase encoding [I-D.multiformats-multibase]). The derived fingerprint SHOULD be expressed as a did:key identifier and added to the DID Document as follows:

```
"equivalentId": [
  "did:key:<multibase-encoded-fingerprint>"
]
```

7.3.3. Mode 3 - Discovery-Enhanced Resolution (OPTIONAL)

Resolvers MAY perform external discovery to supplement the locally constructed DID Document. Permitted discovery mechanisms include:

* DNS-based lookup (e.g., using the DNS-SD mechanism).

* HTTPS well-known endpoints (e.g., /.well-known/did.json).

* Content-addressed storage systems (e.g., IPFS).

Discovery rules SHOULD be namespace-aware, such that a resolver for urn:isbn: DIDs may apply different discovery heuristics than one for urn:uuid: DIDs.

When external discovery yields a DID Document, that document MUST be validated for consistency with the locally constructed baseline document before being returned to the caller. Specifically, the id and alsoKnownAs values MUST match the baseline.

8. DID Document Structure

8.1. Base Document

Every DID Document produced by a did7:web7 resolver MUST conform to the following template:

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did7://web7/<urn>",
  "alsoKnownAs": ["<urn>"]
}
```

Where <urn> is the normalized URN as defined in Section 5.2.

8.2. Optional Properties

8.2.1. Verification Methods

A DID Document MAY include one or more verification method entries to support cryptographic operations associated with the identified resource. The following is an example using the Ed25519VerificationKey2020 type:

```
"verificationMethod": [
  {
    "id": "did7://web7/<urn>#key-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did7://web7/<urn>",
    "publicKeyMultibase": "z6Mk..."
  }
]
```

Verification methods MUST conform to Section 5.2 of [W3C.DID-CORE].

8.2.2. Service Endpoints

A DID Document MAY include service endpoint entries to enable discovery of resources or services associated with the URN. The following is an illustrative example:

```
"service": [
  {
    "id": "did7://web7/<urn>#resource",
    "type": "URNResourceService",
    "serviceEndpoint":
      "https://example.com/urn/<encoded-urn>"
  }
]
```

Service endpoints MUST conform to Section 5.4 of [W3C.DID-CORE]. The type value SHOULD be registered in a publicly accessible DID Specification Registries entry [W3C.DID-SPEC-REGISTRIES].

8.2.3. Equivalent Identifier

Where Mode 2 resolution (Section 7.3.2) is supported, the DID Document MAY include an equivalentId property expressing the deterministic fingerprint-derived did:key as described in Section 7.3.2.

9. Controller Model

9.1. Default Behaviour

A did7:web7 identifier does not inherently assert or imply a controller. In the baseline stateless resolution mode (Mode 1), the DID Document contains no controller property. The absence of a controller property indicates that control has not been established through this mechanism.

9.2. Establishing Control

Control over a did7:web7 DID Document MAY be asserted through any of the following mechanisms:

* Verifiable Credentials [W3C.VC-DATA-MODEL] binding a controller identity to the URN.

* Signed DID Documents, where the document is signed by a verification method under the controller’s authority.

* Namespace authority attestations, where the registrant or maintainer of the relevant URN namespace asserts controller status.

When a controller is established, the controller property MUST be included in the DID Document and MUST reference a resolvable DID.

10. Verification and Trust

The did7:web7 method does not inherently provide authenticity guarantees. A DID Document produced by a stateless resolver (Mode 1) is constructed locally and carries no cryptographic proof of its origin or integrity.

Implementations that require trust assurances SHOULD layer one or more of the following mechanisms on top of the baseline:

* *Cryptographic proofs:* Attach verification methods and associated proofs (e.g., JSON-LD Proofs, JOSE signatures) to the DID Document as described in Section 8.2.1.

* *Third-party attestations:* Bind Verifiable Credentials from trusted issuers to the URN to assert provenance, authenticity, or ownership.

* *Namespace authority validation:* Dereference the URN through its canonical namespace registry to verify that the identified resource exists and that any asserted attributes are consistent.

Consumers of did7:web7 DID Documents SHOULD NOT infer trustworthiness solely from the presence of the DID; trust evaluation MUST take into account the verification mechanisms present in the DID Document and the verifier’s trust policy.

11. CRUD Operations

The did7:web7 method supports the following subset of CRUD operations as defined in [W3C.DID-CORE]:

Operation	Status	Notes
Create	Implicit	A URN is created implicitly by forming the syntactic transformation of a well-formed URN per Section 5.1. No registration step is required.
Read	REQUIRED	Resolution MUST be supported in at least Mode 1 (stateless), per Section 7.3.1.
Update	NOT SUPPORTED	The baseline stateless method does not support document updates. Updates are only possible in Mode 3 via an external discovery service that supports document management.
Deactivate	NOT SUPPORTED	Deactivation is not supported in the baseline method. External service layers may implement deactivation semantics independently.

Table 1

12. Interoperability

12.1. With URN Systems

The did7:web7 method is fully backward compatible with existing URN infrastructure. The embedded URN is preserved verbatim (after normalization) within the DID string, and no changes to existing URN registries, resolvers, or applications are required.

The alsoKnownAs property in the DID Document ensures that a did7:web7 DID can always be mapped back to its source URN, enabling interoperability with legacy systems that do not support DID resolution.

12.2. With the DID Ecosystem

The did7:web7 method is compatible with the W3C DID Core specification [W3C.DID-CORE] and the DID Resolution specification [W3C.DID-RESOLUTION]. It is composable with the following DID methods:

* did:key - via the deterministic fingerprint mechanism (Section 7.3.2).

* did:web - a did7:web7 DID Document MAY reference a did:web service endpoint for resource discovery.

* did:peer - pairwise did:peer identifiers MAY be used in conjunction with did7:web7 to reduce correlation in privacy-sensitive contexts (see Section 14.2).

Implementations MAY register additional DID method compositions in a publicly accessible DID Method Registry.

13. Design Rationale

The following design decisions underpin the did7:web7 specification.

Deterministic mapping: Aligning with the broader principle that DID methods SHOULD be deterministic where possible, the syntactic transformation from URN to URN requires no external state and produces stable, reproducible identifiers.

Use of alsoKnownAs: The alsoKnownAs property from [W3C.DID-CORE] is used rather than a custom extension to ensure semantic preservation while remaining fully conformant with the core specification.

Stateless baseline: Requiring only syntactic processing for baseline resolution maximises portability and eliminates single points of failure that would arise from mandatory registry dependencies.

Acknowledged trade-offs: The method does not include a built-in trust layer or lifecycle operations (Update/Deactivate) at the baseline level. These capabilities are intentionally delegated to optional layers (Modes 2 and 3, and the controller model of Section 9) so that implementations may adopt only the complexity they require.

14. Privacy Considerations

14.1. Correlation Risks

The deterministic mapping from URN to URN means that any party who observes a did7:web7 identifier can immediately recover the underlying URN. Where the URN encodes personally identifiable information (e.g., a personal UUID or a registry identifier linked to an individual), this creates a direct correlation vector.

Additionally, because the transformation is deterministic and publicly known, two parties who independently resolve the same URN will arrive at the same URN, enabling linkage across otherwise unrelated contexts.

14.2. Mitigations

Implementers handling sensitive or personal identifiers SHOULD consider the following mitigations:

* *Pairwise DIDs:* Use pairwise did:peer identifiers in contexts where individual interaction tracking is a concern, rather than exposing the did7:web7 identifier directly.

* *Avoid sensitive URNs:* Refrain from forming did7:web7 identifiers from URNs that encode sensitive personal data in public or semi-public contexts.

* *Selective disclosure:* Where verification is required, use Verifiable Presentations with selective disclosure rather than directly sharing the did7:web7 identifier.

This document does not address the privacy properties of the underlying URN namespaces; implementers MUST consult the privacy considerations of the applicable namespace registration before using that namespace in a did7:web7 context.

15. Security Considerations

15.1. Limitations

The baseline did7:web7 method (Mode 1) provides no inherent proof-of-control. Any party can construct a syntactically valid did7:web7 DID from any well-formed URN without demonstrating authority over the named resource. This is an intentional consequence of the zero-infrastructure design; however, it means that a did7:web7 DID alone cannot be used to assert ownership or authority.

In Mode 3 (Discovery-Enhanced), resolvers that accept DID Documents from external services are susceptible to spoofed or tampered service endpoints. A malicious service could return a crafted DID Document containing false verification methods or service endpoints.

15.2. Recommendations

To mitigate the limitations identified above, implementations SHOULD apply the following measures:

* *Signed metadata:* Require that DID Documents obtained via Mode 3 discovery carry a valid cryptographic proof (e.g., a JSON-LD Data Integrity Proof) before accepting them as authoritative.

* *Verifiable Credentials for binding:* Use Verifiable Credentials [W3C.VC-DATA-MODEL] issued by a trusted authority to bind the URN to a controller identity, rather than relying solely on the DID Document structure.

* *TLS for discovery endpoints:* All HTTPS endpoints used in Mode 3 discovery MUST be protected with TLS 1.2 or higher [RFC8446] and SHOULD use certificate transparency.

* *Input validation:* Resolvers MUST validate the embedded URN against the ABNF grammar of [RFC8141] before performing any resolution activity.

16. IANA Considerations

This document requests registration of the following DID method name in the W3C DID Specification Registries [W3C.DID-SPEC-REGISTRIES]:

Field	Value
Method Name	urn
Status	provisional
Specification	This document
Contact	See Author’s Address

Table 2

This document has no other IANA actions.

17. References

17.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/rfc/rfc5234>.

[RFC8141] Saint-Andre, P. and J. Klensin, "Uniform Resource Names (URNs)", RFC 8141, DOI 10.17487/RFC8141, April 2017, <https://www.rfc-editor.org/rfc/rfc8141>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[W3C.DID-CORE] Sporny, M., Guy, A., Sabadello, M., and D. Reed, "Decentralized Identifiers (DIDs) v1.0", W3C Recommendation, July 2022, <https://www.w3.org/TR/did-core/>.

[W3C.DID-RESOLUTION] Sabadello, M., "Decentralized Identifier Resolution (DID Resolution) v0.3", W3C Working Group Note, 2023, <https://w3c-ccg.github.io/did-resolution/>.

17.2. Informative References

[I-D.multiformats-multibase] Sporny, M., "The Multibase Data Format", Work in Progress, Internet-Draft, draft-multiformats-multibase, 2023, <https://datatracker.ietf.org/doc/ draft-multiformats-multibase/>.

[W3C.DID-SPEC-REGISTRIES] Sporny, M. and O. Steele, "DID Specification Registries", W3C Working Group Note, 2023, <https://www.w3.org/TR/did-spec-registries/>.

[W3C.VC-DATA-MODEL]
Sporny, M., Longley, D., and D. Chadwick, "Verifiable Credentials Data Model v2.0", W3C Candidate Recommendation, 2024, <https://www.w3.org/TR/vc-data-model-2.0/>.

[WEB70-URN]
Herman, M., "SDO: W3C Decentralized Universal Resource Name (URN) DID Method (Web 7.0)", Licensed under Creative Commons Attribution-ShareAlike 4.0 International Public License, March 2026, <https://hyperonomy.com/2026/03/24/sdo-web-7-0-decentralized-resource-name-urn-did-method/>.

Appendix A. Complete Example

This appendix illustrates a complete did7:web7 resolution using an ISBN URN as input, with Mode 2 (fingerprint) and a service endpoint included.

Source URN:

urn:isbn:9780141036144

Derived URN DID:

did7://web7/urn:isbn:9780141036144

Resolved DID Document (Modes 1 + 2 + service endpoint):

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did7://web7/urn:isbn:9780141036144",
  "alsoKnownAs": [
    "urn:isbn:9780141036144"
  ],
  "equivalentId": [
    "did:key:zQm..."
  ],
  "service": [
    {
      "id": "did7://web7/urn:isbn:9780141036144#info",
      "type": "BookMetadata",
      "serviceEndpoint":
        "https://example.org/isbn/9780141036144"
    }
  ]
}
```

Acknowledgements

The author thanks the members of the W3C Decentralized Identifier Working Group and the broader DID community for their foundational work on the DID Core specification, and the IETF URN community for their long-standing stewardship of URN namespaces.

Author’s Address

Michael Herman
Web 7.0 Foundation
Bindloss Alberta
Canada
Email: mwherman@gmail.com
URI: https://hyperonomy.com/about/