SCITT
Internet-Draft
Intended status: Standards Track
Expires: November 7 2026

D. Brooks
Business Cyber Guardian

May 6 2026

The 'ztdnaid' URI Scheme for Zero-Trust Digital DNA Identifiers (ZTDNAID)

draft-brooks-ztdnaid-new-01

Abstract

This document defines the 'ztdnaid' Uniform Resource Identifier(URI) scheme, used to represent globally unique, cryptographically verifiable Digital DNA Identifiers (ZTDNAIDs) within Zero Trust architecture implementations. A ZTDNAID binds an entitys immutable, unique Digital DNA Record "DDR" to a resolvable identifier suitable for authentication, authorization, attestation, and trust-registry lookup. The scheme is designed for use with trust registries, such as SAG-CTR and supports deterministic resolution, offline verification, and secure dereferencing.

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/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

Copyright Notice

Table of Contents

1. Introduction

Zero Trust architectures increasingly rely on cryptographically strong, non-repudiable identifiers that bind an entity to a verifiable digital record. Digital DNA Identifiers (ZTDNAIDs) provide a compact, canonical identifier for entities whose trust posture is continuously evaluated.

The ’ztdnaid’ URI scheme enables interoperable representation, transport, and dereferencing of these identifiers across protocols, trust registries, and attestation systems. The scheme is designed to be:

* Opaque (no hierarchical semantics)
* Deterministic (canonical encoding)
* Cryptographically bound (hash-based)
* Resolvable (via trust registries such as SAG-CTR)
* Suitable for Zero Trust enforcement

This document registers the ’ztdnaid’ URI scheme with IANA under the procedures of RFC 7595.

1.1. Requirements Notation

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. described in [RFC2119].

3. Scheme Definition

3.1. Overview

A ZTDNAID is a cryptographic identifier derived from a globally unique Digital DNA Record "DDR". The identifier is encoded using URL-safe UTF-8 characters. The scheme is opaque and does not define hierarchical components.

Example:
A DDR example unique identifier string using "/" delimiter:
Microsoft Corporation/Bill Gates/EmployeeID: 002
Equivalent ztdnaid UTF-8 result:
62588568DE0D42ABF9BBFF9B0FD8D2FEB9A24C950AC66AFCD8679FA4C831392A

3.2. Syntax

The syntax of the ’ztdnaid’ URI scheme is defined using ABNF (RFC 5234):

```
ztdnaid-uri   = "ztdnaid:" ztdnaid-value
ztdnaid-value = 1*utf8url-char
utf8url-char = ALPHA / DIGIT
```

The value MUST be a URL-safe, UPPERCASE UTF-8 encoding of a cryptographic digest (e.g., SHA-256, SHA-384, or SHA-512)[RFC6234].

3.3. Semantics

A ’ztdnaid’ identifies a Digital DNA Record (DDR) that describes an entitys unique immutable attributes, provenance, and other identifying characteristics.

The DDR may be stored in:

* A Zero Trust trust registry (e.g., SAG-CTR)
* A verifiable credential
* A distributed ledger
* A local cache

Dereferencing a ZTDNAID yields metadata, attestations, and trust-policy-relevant information.

4. Resolution

Resolution of a ZTDNAID is performed by querying a trust registry that supports the ZTDNAID resolution API. The resolution process:

1. Accepts a ZTDNAID
2. Locates the corresponding DDR
3. Returns metadata, endorsements, and attestation material
4. Verifies the cryptographic binding between the DDR and the ZTDNAID value

This document does not mandate a specific resolution protocol; however, implementations SHOULD support the SCITT-aligned trust registry API defined by the Software Assurance Guardian - Community Trust Registry (SAG-CTR).

5. Security Considerations

* Cryptographic Binding: ZTDNAIDs MUST be represent a cryptographic UTF-8 UPPERCASE SHA-256 hash of the DDR data to prevent substitution attacks.
* Privacy: ZTDNAIDs are opaque and SHOULD NOT embed personally identifiable information.
* Replay Protection: Resolvers SHOULD verify freshness of attestation material.
* Transport Security: Resolution MAY occur over authenticated, encrypted channels (e.g., TLS 1.3).
* Trust Registry Integrity: Implementations MUST validate registry signatures and trust anchors.

6. Internationalization Considerations

The ZTDNAID value is restricted to UPPERCASE UTF-8 URL-safe characters. No internationalization issues are anticipated.

7. IANA Considerations

This document registers the ’ztdnaid’ URI scheme under the procedures of RFC 7595.

URI Scheme Registration

* Scheme name: ztdnaid
* Status: Provisional (to be updated to Permanent upon RFC publication)
* Applications/protocols that use this scheme name: Zero Trust architectures, trust registries, attestation systems, SCITT Trust Registry Transparency Services
* Contact: Richard Brooks <dick@businesscyberguardian>
* Change controller: Business Cyber Guardian
* References: This document

Scheme Syntax: Section 3.2
Scheme Semantics: Section 3.3
Security Considerations: Section 5

8. Examples

62588568DE0D42ABF9BBFF9B0FD8D2FEB9A24C950AC66AFCD8679FA4C831392A

10. References

10.1. 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://doi.org/10.17487/RFC2119>.

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

[RFC6234] Eastlake, D. 3rd, "US Secure Hash Algorithms", May 2011, https://datatracker.ietf.org/doc/html/rfc6234

Author’s Address

Dick Brooks
Business Cyber Guardian
23 Linda Dr.
Westfield, Massachusetts 01085
United States of America
Email: dick@businesscyberguardian.com