

Secure Asset Transfer Protocol
Internet-Draft
Intended status: Standards Track
Expires: 20 April 2026

N. Smith
Independent
17 October 2025

A SATP Core Binding for vLEI Identities
draft-smith-satp-vlei-binding-01

Abstract

The verifiable Legal Entity Identifier (vLEI) is a cryptographically verifiable extension of the LEI standard, designed to automate trust in organizational identity. Governed by the Global Legal Entity Identifier Foundation (GLEIF), the vLEI system uses Authentic Chained Data Containers (ACDCs), Self-Addressing Identifiers (SAIDs), and Key Event Receipt Infrastructure (KERI) to issue and verify credentials for legal entities and their authorized representatives. It enables secure, machine-readable identity assertions across financial, regulatory, and supply chain ecosystems, supporting role-based delegation and interoperability with decentralized trust frameworks.

This specification defines vLEI for verifiable gateway operator identities and cryptographically links the gateway operator identity to the gateway identity. Thus SATP core lock assertions are cryptographically linked to gateway operator identities.

About This Document

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

The latest revision of this draft can be found at <https://nedmsmith.github.io/draft-smith-satp-vlei-binding/draft-smith-satp-vlei-binding.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-smith-satp-vlei-binding/>.

Discussion of this document takes place on the Secure Asset Transfer Protocol Working Group mailing list (<mailto:sat@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/sat/>. Subscribe at <https://www.ietf.org/mailman/listinfo/sat/>.

Source for this draft and an issue tracker can be found at <https://github.com/nedmsmith/draft-smith-satp-vlei-binding>.

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."

This Internet-Draft will expire on 20 April 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Conventions and Definitions	4
2.1. Terminology	4
3. vLEI Identities and Credentials	4
3.1. vLEI Credential Attributes	4
3.2. KERI Key Management	5
3.3. SATP Credentialing Assumptions	6
3.4. SATP Identity Binding	6
3.5. vLEI Roles	8
3.5.1. vLEI Schemas	9
3.5.2. LegalEntityEngagementContextRolevLEICredential Credentials	9
4. vLEI Binding Architecture	9
4.1. SATP vLEI Mapping	10
4.1.1. vLEI Deployment Considerations	12

4.2.	Key Structures	13
4.3.	SATP Message Wrapper Schema	13
4.3.1.	SATP Transfer Initiation (Stage 1) Message Binding	13
4.3.2.	vLEI Wrapper	13
4.3.3.	Content References	14
4.3.4.	Key Wrappers	14
4.4.	vLEI Media Types	15
4.4.1.	Profile Optional Parameter	15
4.4.2.	Encoding Optional Parameter	16
4.4.3.	Charset Optional Parameter	16
5.	Verification of vLEI Payloads	17
6.	Implementation Status	17
7.	Security Considerations	17
8.	IANA Considerations	17
8.1.	Media Type Assignment	17
8.1.1.	application/cesr+json	17
8.1.2.	application/cesr+cbor	19
8.1.3.	application/cesr+msgpk	21
8.1.4.	application/cesr	23
8.2.	CoAP Content-Format ID Assignments	25
9.	References	27
9.1.	Normative References	27
9.2.	Informative References	30
Appendix A.	Full CDDL	31
Appendix B.	Examples in JSON	32
Acknowledgments	34
Author's Address	35

1. Introduction

The SATP architecture [I-D.ietf-satp-architecture] defines an interoperability architecture for interconnection between networks or systems that anticipates a secure asset transfer protocol that satisfies security, privacy, atomicity and liveness requirements in the transfer of assets. The SATP core protocol [I-D.ietf-satp-core] is a protocol for exchanging digital assets that ensures the state of the asset is preserved across inter-domain transfers. It is an extensible protocol where fields containing identity and payload values that are not defined by SATP core may be defined by companion specifications. This specification defines a SATP core protocol binding for Verifiable Legal Entity Identifiers (vLEI) [ISO17442-3] used to identify SATP gateways and the organizations that operate them. In some use cases, the assets being transferred have legal considerations such that officers of the organization are expected to authorize digital asset transfers. This specification details the various vLEI credentials needed and how to integrate them with SATP core messages. SATP core message binding anticipates use of a message wrapper that uses media type [STD91] and content format

[RFC7252] identifiers to facilitate interoperability with vLEI and other credential types.

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.

2.1. Terminology

- * Legal Entity : any organization or structure that is legally or financially responsible for its actions and can enter into financial transactions, explicitly excluding natural persons except where they act as sole proprietors recognized as legal entities [ISO17442-1_2020].
- * Natural person : a living human being (LLI (https://www.law.cornell.edu/wex/natural_person)).

3. vLEI Identities and Credentials

The SATP core protocol [I-D.ietf-satp-core] defines a set of entities that participate in an asset transfer. These entities are represented in different ways including identifiers, credentials and public keys. SATP entities are presumed to have been issued cryptographically relevant identities prior to the SATP Transfer Initiation Stage (Stage 1) and subsequent exchanges. An entity (see Section 3 [RFC4949] that weilds a cryptographic key pair can be described as a principal [ACM-Calculus]. SATP Gateways and Networks as well as the key management infrastructure that authorizes these keys are all principals.

3.1. vLEI Credential Attributes

A legal entity identifier (LEI) is essentially a globally unique value issued by a well-known entity trusted to manage the LEI namespace correctly. A verifiable LEI (vLEI) [ISO17442-3] is an Authentic Chained Data Container (ACDC) [ACDC-Spec] credential that contains three attributes:

- * Legal Entity Identifier (LEI)
- * Person Identifier - human friendly name

- * Organizational Role Identifier - defined by a namespace controller such as GLEIF [GLEIF-vLEI-EGF].

A vLEI ACDC attributes also contain an Autonomic Identifier (AID (<https://trustoverip.github.io/kerisuite-glossary#term:autonomic-identifier>)) that identifies the principal to which the other vLEI attributes are bound. In PKIX terminology, this AID identifies the `_subject_`. A vLEI ACDC also contains an issuer AID that identifies the issuing principal. vLEI credentials are issued to non-natural person legal entities (see [GLEIF-vLEI-Part2] and [ISO17442-3]). Nevertheless, these credentials contain `personLegalName` and `engagementContextRole` attributes that are typically associated with natural persons.

3.2. KERI Key Management

AIDs reference Key Event Log (KEL) events that can be verified by outside entities; as such is a form of key attestation. An ACDC issuer is anchored to a key inception event which is a digest of the current and pre-rotated keys and other key management context. The digest becomes the issuer's autonomic identifier (AID). An ACDC credential can be identified by hashing its contents. The resulting digest is called a Self-Addressing Identifier (SAID) [KERI-Spec].

Periodically, key events are appended to the KEL resulting in a different key state. However, the key inception event (the first event) remains unchanged. Anchoring AIDs to inception events means the identifier is relatively long lived as even key rotation events are anticipated at inception. Key rotation events that exceed the number of pre-rotated keys results in a new key inception event that consequently invalidates its previous AID.

When applying vLEI to SATP, ACID properties suggest that the state of the exchanged asset, the protocol state, and the key state play a role in determining the overall state of the asset exchange. Ideally, SATP principals (including key state) is locked down as part of reliable asset exchange where the complete state can be rolled back to a known-good state. However, if key state can't be locked as part of a SATP asset exchange, key state verification at each SATP stage may be needed to verify the subsequent key state changes occurring during SATP stages does not present a security relevant condition.

3.3. SATP Credentialing Assumptions

SATP signing keys (e.g., `senderGatewaySignaturePublicKey`) that are based on ACDC credentials implicitly support key attestation as part of key verification. SATP device keys (e.g., `senderGatewayDeviceIdentityPubKey`) used for device authentication or device attestation can further strengthen trustworthiness claims of SATP endpoints. Some SATP keys do not use vLEI credentials, but could still be based on ACDC credentials. Still other credential types (e.g., PKIX [RFC5280]) could be leveraged, but complicates key and trust management.

RFCThis assumes SATP stage 1 messages that contain identifiers and public keys are artifacts of credentials that have been issued to SATP defined entities. In addition, SATP entities are authorized by vLEI hierarchy that supplies a legal context for asset exchange. Nevertheless, the `GatewayDeviceIdentityPublicKey` could be associated with a different credential from that belonging to the `GatewaySignaturePublicKey`. Consequently, there MAY be additional credentials issued to SATP principals that require additional verifier processing that ensures the asset transfer legal context is in force despite bifurcated credential formats and infrastructure.

3.4. SATP Identity Binding

Table 3 shows SATP entities with corresponding SATP message types mapped to a suitable credential structure. Stage 1 defines uses credential artifacts (i.e., identifiers and public keys) implying credential issuance occurred earlier, possibly during Stage 0. RFCThis assumes all credentials issued are (or can be) ACDCs. The entity identifier within an ACDD is an autonomic identifier (AID), which is semantically aligned with SATP IDs.

SATP Entity	SATP Message	Structure
Originator	OriginatorCredential _-implied-_	vLEI
	verifiedOriginatorEntityID	AID
	originatorPubkey	KEL or other
Sender Gateway Owner	senderGatewayOwnerCredential _-implied-_	vLEI
	senderGatewayOwnerID	AID

Sender Gateway (G1)	senderGatewayCredential __-implied-__	ACDC
	senderGatewayId	AID
	senderGatewaySignaturePublicKey	KEL or other
Sender Gateway (G1)	senderGatewayDeviceIdentityCredential __-implied-__	ACDC
	senderGatewayDeviceIdentityId __-implied-__	AID
	senderGatewayDeviceIdentityPubkey	KEL or other
Sender Network	senderNetworkCredential __-implied-__	ACDC
	senderGatewayNetworkId	AID
.....
Beneficiary	BeneficiaryCredential __-implied-__	vLEI
	beneficiaryPubkey	KEL or other
	verifiedBeneficiaryEntityID	AID
Receiver Gateway Owner	receiverGatewayOwnerCredential __-implied-__	vLEI
	senderGatewayOwnerID	AID
Receiver Gateway (G2)	receiverGatewayCredential __-implied-__	ACDC
	receiverGatewayId	AID
	receiverGatewaySignaturePublicKey	KEL or other
Receiver Gateway (G2)	receiverGatewayDeviceIdentityCredential __-implied-__	ACDC
	receiverGatewayDeviceIdentityId __-implied-__	AID

	receiverGatewayDeviceIdentityPubkey	KEL or other
Recipient Network	recipientNetworkCredential _-implied-_	ACDC
	recipientGatewayNetworkId	AID

Table 1: Mapping of SATP Entities and Messages to Credential Type

3.5. vLEI Roles

The vLEI ecosystem defines roles-specific credentials. Version 1.0 of vLEI defines six ecosystem roles.

vLEI Role	Abbreviation
QualifiedvLEIIssuervLEICredential	QVI
LegalEntityvLEICredential	LEID
OORAuthorizationvLEICredential	OOA
LegalEntityOfficialOrganizationalRolevLEICredential	OO
ECRAuthorizationvLEICredential	EC
LegalEntityEngagementContextRolevLEICredential	EC

Table 2: vLEI Ecosystem Roles

The vLEI role architecture is a hierarchical namespace. The QVI role manages the top-level namespace. It oversees the lifecycle of subordinate namespaces (e.g., LEID, OOA, and EC) which are also characterized as roles. The LEID role manages the LEID namespace. The OOA role manages the OOA namespace and lifecycle of its subordinate OO role. The EC role manages the EC namespace and lifecycle of its subordinate EC role. The LEID, OO, and EC are non-natural person roles (see [ISO17442-1_2020]). Non-vLEI credentials are used to identify and authenticate such entities.

3.5.1. vLEI Schemas

The various vLEI ACDC objects conform to JSON Schemas:

- * LEID (<https://github.com/GLEIF-IT/vLEI-schema/blob/main/legal-entity-vLEI-credential.json>).
- * QVI (<https://github.com/GLEIF-IT/vLEI-schema/blob/main/qualified-vLEI-issuer-vLEI-credential.json>).
- * OORA (<https://github.com/GLEIF-IT/vLEI-schema/blob/main/oor-authorization-vlei-credential.json>).
- * ECRA (<https://github.com/GLEIF-IT/vLEI-schema/blob/main/ecr-authorization-vlei-credential.json>).
- * OOR (<https://github.com/GLEIF-IT/vLEI-schema/blob/main/legal-entity-official-organizational-role-vLEI-credential.json>).
- * ECR (<https://github.com/GLEIF-IT/vLEI-schema/blob/main/legal-entity-engagement-context-role-vLEI-credential.json>).

These schemas are used to validate JSON realizations of vLEI credentials. Other representations such as CBOR [STD94] and message pack [MSGPCK] can be realized, but the schemas used to validate them are not available at the time of this writing.

3.5.2. LegalEntityEngagementContextRolevLEICredential Credentials

The SATP Messages in row 3 of Table 3 is a LegalEntityEngagementContextRolevLEICredential as defined by the LEECRvLEIC (<https://github.com/GLEIF-IT/vLEI-schema/blob/main/legal-entity-engagement-context-role-vLEI-credential.json>) schema.

These messages are realized using a LEECRvLEIC because they identify the gateways and hosts within the respective networks involved in transferring digital assets.

4. vLEI Binding Architecture

The SATP core protocol [I-D.ietf-satp-core] defines several extensible protocol fields that contain identity and other values not defined by SATP core. To facilitate interoperability these fields SHOULD contain a media type [STD91] or content format [RFC7252] wrapper. This specation requests IANA assignment of media type and content format identifiers for vLEIs which are serialized as Composable Event Streaming Representation (CESR) [CESR-Spec] objects in JSON and other formats. See Section 4.4.

```
// Note: SATP describes Gateway secure channel establishment public
// key-pair but this isn't represented in the list of message
// publickey message types. Gateway Credential type isn't used in
// any of the stages afaik. There should be an IANA registry for the
// allowed credential types (vLEI, SAML, OAuth, PKIX).
//
// -- Ned Smith
```

4.1. SATP vLEI Mapping

The SATP protocol [I-D.ietf-satp-core] defines a set of SATP flows that are divided into protocol message exchange blocks called stages. The stage-1 messages are illustrated in Table 1. The SATP entity that authors the various stage-1 messages is also depicted in Table 1. The authority used to assert SATP messages is based on a cryptographic credential that is used to authenticate the message. SATP asset transfers depend on properly established organizational authority contexts. Table 3 illustrates the relationships between the various SATP entities, some of which are implied, and the source of authority. The table is ordered according to an authority hierarchy with the root authority in the first row and leaf entities on the 6th row. Authority is therefore cumulative from row to row. The type of credential used to represent authority is in column 3.

#	SATP Entity	vLEI Type & Authority Chain	Credential Type	Notes
1	Root vLEI Issuer _ -implied- _	GLEIF	vLEI	Root namespace authority (e.g., GLEIF)
2	Qualified vLEI Issuer _ -implied- _	GLEIF>>QVI	vLEI	Inter organizational namespace authority
3	Organizational vLEI Issuer _ -implied- _	QVI>>LEID	vLEI	Organizational level namespace authority
4	Originator, Beneficiary, Gateway Owner	LEID>>OORA, LEID>>ECRA, LEID>>OORA>>OOR, LEID>>ECRA>>ECR	vLEI	Person-in-role credential
5	Gateway / Network Operations Manager / Admin _ -implied- _	ECR>>ACDC>>KEL, ECR>>KEL, ECR(as other issuer)>>other	ACDC, KEL, other	Operational credentials (not defined by vLEI)
6	Sender/Receiver Gateway, Sender/ Recipient Network	n/a	KEL, other	Device or system identity

Table 3: Mapping SATP Entity to vLEI Role

- Row 1. GLEIF is a well-known root authority in the vLEI ecosystem. The GLEIF AID is public knowledge.
- Row 2. Second tier QVI authorities are credentialed by a root authority. Typically, second tier authorities are inter-organizational issuing credentials to multiple organizational entities.
- Row 3. Orgainzational entities use an LEID credential to manage intra-organizational namespaces.

- Row 4. SATP stage-1 messages imply the existence of organization level entities such as Originator, Beneficiary, and Gateway Owners. vLEI defines two forms of person-in-role credentials that map to these SATP entities. OOR for organizational officers and ECR for organizational departments or functions. SATP use cases likely depend on ECR credentials. A legal entity may delegate credential issuance by naming an alternate legal entity using OOR Authority (OORA) or ECR Authority (ECRA) delegation credentials.
- Row 5. SATP architecture assumes the existence of intra-organizational entities that manage and administer networks and servers. vLEI doesn't define such roles and SATP stage-1 messages don't explicitly mention the existence of such entities. However, the people responsible for administering and managing the systems that implement SATP message exchange have credentials that tie into the organizational accountability framework envisaged by vLEI. These credentials can be KERI based (e.g., KEL, ACDC) or other (e.g., PKIX).
- Row 6. SATP stage-1 messages describe various services and networks that have been credentialed with device or system identities. These credentials can be KERI based or other. KERI based credentials reference the key holders AID that is the identity of the gateway or network principal that weilds the corresponding private key. An PKIX device certificate associates a _subject name_ to the public key of the gateway or network principal that weilds the corresponding private key. A SATP gateway or network can be a principal that has multiple key management subsystems (e.g., KERI and PKIX).

4.1.1. vLEI Deployment Considerations

SATP deployments could utilize other vLEI roles. For example, an ECR role might be defined for a SATP Gateway Operations Manager or Network Administrator. See row 4 Table 3. Although SATP Stage 1 messages don't directly refer to ECR credentials, the credentials referenced could link to ECR credentials which in turn link to ECRA credentials etc...

```
// Note: Need to describe how this draft approaches both top-down and
// bottom-up protocol binding e.g., http and tls.
//
// -- Ned Smith
```

4.2. Key Structures

Keys embedded in hardware or firmware may not easily be converted to an interoperable format, hence support for multiple key formats ensures the SATP protocols can be implemented by a wide variety of systems.

The SATP PublicKey messages SHALL be encoded using JSON Web Key (JWK) [RFC7517], COSE key [STD96], PKIX key in PEM or DER, or as key events [KERI-Spec].

Other key formats SHOULD be allowed but are out of scope for RFCthis.

4.3. SATP Message Wrapper Schema

The following CDDL [RFC8610] defines the wrapper and application to SATP fields.

4.3.1. SATP Transfer Initiation (Stage 1) Message Binding

The SATP stage 1 messages containing identifiers use a vLEI wrapper that contains a payload and payload content identifier. Other stage 1 messages are public key values that use a key wrapper that disambiguates the key type and format or can be expressed as a wrapped vLEI.

```
satp-message = {  
  ? verifiedOriginatorEntityId: wrapped-vlei  
  ? verifiedBeneficiaryEntityId: wrapped-vlei  
  ? senderGatewayOwnerId: wrapped-vlei  
  ? receiverGatewayOwnerId: wrapped-vlei  
  
  ? senderGatewayId: wrapped-vlei  
  ? recipientGatewayId: wrapped-vlei  
  ? senderGatewayNetworkId: wrapped-vlei  
  ? recipientGatewayNetworkId: wrapped-vlei  
  
  ? originatorPubkey: wrapped-vlei / wrapped-key  
  ? beneficiaryPubkey: wrapped-vlei / wrapped-key  
  ? senderGatewaySignaturePublicKey: wrapped-vlei / wrapped-key  
  ? receiverGatewaySignaturePublicKey: wrapped-vlei / wrapped-key  
  ? senderGatewayDeviceIdentityPubkey: wrapped-vlei / wrapped-key  
  ? receiverGatewayDeviceIdentityPubkey: wrapped-vlei / wrapped-key  
}
```

4.3.2. vLEI Wrapper

```

; =====
; --- Wrapped vLEI Payloads ---
; =====

wrapped-vlei = {
  content: content-ref
  payload: bstr / tstr
}

```

4.3.3. Content References

```

content-ref = non-empty<{
  ? mt: vlei-media-type ; TBA
  ? cf: uint ; TBA content format id
  ? cbt: bool ; payload contains CBOR tagged content in the TN() range if true, if fals
e not cbor tagged and "mt" is required
  ? oid: tstr ; generated from content-format-id e.g., "1.3.6.1.4.1.37476.2.1.5"
}>

```

4.3.4. Key Wrappers

```

; =====
; --- Wrapped Key Definitions ---
; =====

wrapped-key = $key-type
$key-type /= cose-key
$key-type /= jwk-key
$key-type /= pkix-key

cose-key = {
  content: "application/cose;cose-type=cose-key" / uint,
  encoding: "cbor" / "base64uri" / "text",
  payload: bstr / tstr
}

jwk-key = {
  content: "application/jwk+json" / uint,
  payload: tstr
}

pkix-key = {
  content: "application/pkix-cert" / uint,
  encoding: "PEM" / "DER",
  payload: tstr / bstr
}

```

4.4. vLEI Media Types

vLEI credentials are expressed as Authentic Chained Data Containers (ACDC) [ACDC-Spec]. Section 8 request IANA assignment of media types [STD91] and content format identifiers [RFC7252].

SATP core [I-D.ietf-satp-core] anticipates JSON encoded message. vLEI credentials can subsequently be JSON encoded while also being CESR [CESR-Spec] compliant. CESR defines JSON, CBOR, MSGPK and native CESR variants. The following media types MAY be used when building credential payloads for SATP:

Media Types
application/cesr+json
application/cesr+cbor
application/cesr+msgpk
application/cesr

Table 4: vLEI media types

The media types in Table 4 have start codes that comply with the media type's structured syntax suffix, but require CESR-aware parsers that can detect them. The "cesr" subtype informs parsers that they have to do start code look-ahead processing.

The "cesr" subtype also informs parsers that the CESR stream may contain a variety of objects including ACDCs, AIDs, and SAIDs (as mentioned in previous sections of RFCthis).

4.4.1. Profile Optional Parameter

The media type assignments have an optional parameter named "profile=" that MAY be any value. It can be used to identify a vLEI profile such as vLEI credential type. It SHOULD be expressed in URI format as illustrated in Table 5.

Profile name	Profile ID
QualifiedvLEIIssuervLEICredential (QVI)	profile=urn:vlei:qvi
LegalEntityvLEICredential (LEID)	profile=urn:vlei:leid
ECRAuthorizationvLEICredential (ECRA)	profile=urn:vlei:ecra
LegalEntityEngagementContextRolevLEICredential (ECR)	profile=urn:vlei:ecr
OORAuthorizationvLEICredential (OORA)	profile=urn:vlei:oor
LegalEntityOfficialOrganizationalRolevLEICredential (OOR)	

Table 5: vLEI profiles

The various vLEI credential types can be specified in a media type using the profile option. Table 5 summarizes the profile identifiers for the various vLEI credential types. A comprehensive listing of vLEI profiles is provided even though some of the vLEI credential types are not anticipated by the vLEI binding to SATP at this time.

4.4.2. Encoding Optional Parameter

The media type assignments have an optional encoding ("encoding=") parameter that can be used to tunnel an alternative encoding. Typically, encodings fall into two broad categories; text or binary. An encoding MAY be any value, but RFCthis anticipates the following:

- * "base64uri" -- the payload is binary, as indicated by the media-type, but base64 encoded when the bounding protocol is a text stream. See Section 5, [RFC4648].

4.4.3. Charset Optional Parameter

The media type assignments have an optional character set ("charset=") parameter that can be used to identify the character encoding scheme when the payload is a text encoding. By default "utf-8" is assumed. Alternative character set encodings MUST populate "charset=".

5. Verification of vLEI Payloads

TODO

6. Implementation Status

TODO

7. Security Considerations

The following security properties are assumed for all payloads identified by media types defined in RFCthis:

- * ACDC payloads are cryptographically signed.
- * CESR payloads are cryptographically signed and self-framing.
- * Signature verification is required to ensure authenticity and integrity.
- * Credential provenance must be anchored to a trusted root. For example, the GLEIF Root AID via ACDC edges (see [GLEIF-vLEI-EGF]).
- * vLEIs must be validated against the vLEI schema. See [GLEIF-vLEI-Part3].

8. IANA Considerations

8.1. Media Type Assignment

IANA is requested to add the following media types to the "Media Types" registry [IANA.media-types].

8.1.1. application/cesr+json

This media type indicates the payload is a JSON formatted vLEI.

Type name:

- * application

Subtype name:

- * cesr+json

Required parameters:

- * None

Optional parameters:

- * profile — Indicates the payload conforms to a specific vLEI credential type.
- * encoding — Indicates the ACDC stream is text or binary. If binary, encoding MUST make the payload text-safe (e.g., encoding=base64uri). Defaults to text.
- * charset — Indicates character set for text encodings. Defaults to UTF-8.

Encoding considerations:

- * 8-bit; JSON text encoding defaults to UTF-8.
- * Binary payloads are text-safe encoded for use in JSON streams.

Security considerations:

- * See Section 7.

Interoperability considerations:

- * Binary payloads must be base64 encoded to make payloads compatible with text streams.
- * Section 9.4 and 9.5 in the CESR specification (cold start) in CESR
- * Section 11.5 Version String Field in CESR

Published specification:

- * RFCthis
- * Key Event Receipt Infrastructure (KERI) — [KERI-Spec]
- * Authentictic Chained Data Containers (ACDC) — [ACDC-Spec]
- * Composable Event Streaming Representation (CESR) — [CESR-Spec]
- * GLEIF vLEI Credential Schema Registry — [GLEIF-vLEI-Part3]

Applications that use this media type:

- * GLEIF vLEI issuance and verification systems.
- * SATP-compliant credential exchange platforms.

- * Forensic credential chaining and audit systems.

Fragment identifier considerations:

- * None

Additional information:

- * _Magic number(s):_ None

- * _File extension(s):_ .acdcjson

- * _Macintosh file type code(s):_ None

Person & email address to contact for further information:

- * N. Smith ned.smith.ietf@outlook.com
(mailto:ned.smith.ietf@outlook.com)
- * GLEIF IT Team vlel-support@gleif.org (mailto:vlei-support@gleif.org)

Intended usage:

- * COMMON

Author:

- * N. Smith ned.smith.ietf@outlook.com
(mailto:ned.smith.ietf@outlook.com)
- * GLEIF IT Team vlel-support@gleif.org (mailto:vlei-support@gleif.org)

Change controller:

- * IETF / GLEIF

8.1.2. application/cesr+cbor

Type name:

- * application

Subtype name:

- * cesr+cbor

Required parameters:

- * None

Optional parameters:

- * profile — Indicates the payload conforms to a specific vLEI credential type.
- * encoding — Indicates the ACDC stream is text or binary. Defaults to cbor.
- * charset — Indicates character set for text encodings. Defaults to UTF-8.

Encoding considerations:

- * ACDC streams are CBOR encoded for use with binary transports. If the transport is a text stream the encoding option should be specified.

Security considerations:

- * See Section 7.

Interoperability considerations:

None.

Published specification:

- * RFCthis
- * Key Event Receipt Infrastructure (KERI) — [KERI-Spec]
- * Authentictic Chained Data Containers (ACDC) — [ACDC-Spec]
- * Composable Event Streaming Representation (CESR) — [CESR-Spec]
- * GLEIF vLEI Credential Schema Registry — [GLEIF-vLEI-Part3]

Applications that use this media type:

- * GLEIF vLEI issuance and verification systems
- * SATP-compliant credential exchange platforms
- * Forensic credential chaining and audit systems

Fragment identifier considerations:

- * None

Additional information:

- * Magic number(s): None
- * File extension(s): .acdcbor
- * Macintosh file type code(s): None

Person & email address to contact for further information:

- * N. Smith ned.smith.ietf@outlook.com
(mailto:ned.smith.ietf@outlook.com)
- * GLEIF IT Team vlel-support@gleif.org (mailto:vlei-support@gleif.org)

Intended usage:

- * COMMON

Author:

- * N. Smith ned.smith.ietf@outlook.com
(mailto:ned.smith.ietf@outlook.com)
- * GLEIF IT Team vlel-support@gleif.org (mailto:vlei-support@gleif.org)

Change controller:

- * IETF / GLEIF

8.1.3. application/cesr+msgpk

Type name:

- * application

Subtype name:

- * cesr+msgpk

Required parameters:

- * None

Optional parameters:

- * profile — Indicates the payload conforms to a specific vLEI credential type.
- * encoding — Indicates the ACDC stream is text or binary. Defaults to msgpk.
- * charset — Indicates character set for text encodings. Defaults to UTF-8.

Encoding considerations:

- * ACDC streams are MSGPK encoded for use with binary transports. If the transport is a text stream the encoding option should be specified.

Security considerations:

- * See Section 7.

Interoperability considerations:

None.

Published specification:

- * RFCthis
- * Key Event Receipt Infrastructure (KERI) — [KERI-Spec]
- * Authentictic Chained Data Containers (ACDC) — [ACDC-Spec]
- * Composable Event Streaming Representation (CESR) — [CESR-Spec]
- * GLEIF vLEI Credential Schema Registry — [GLEIF-vLEI-Part3]

Applications that use this media type:

- * GLEIF vLEI issuance and verification systems
- * SATP-compliant credential exchange platforms
- * Forensic credential chaining and audit systems

Fragment identifier considerations:

* None

Additional information:

* Magic number(s): None

* File extension(s): .acdcmsgpk

* Macintosh file type code(s): None

Person & email address to contact for further information:

* N. Smith ned.smith.ietf@outlook.com
(mailto:ned.smith.ietf@outlook.com)

* GLEIF IT Team vlel-support@gleif.org (mailto:vlei-
support@gleif.org)

Intended usage:

* COMMON

Author:

* N. Smith ned.smith.ietf@outlook.com
(mailto:ned.smith.ietf@outlook.com)

* GLEIF IT Team vlel-support@gleif.org (mailto:vlei-
support@gleif.org)

Change controller:

* IETF / GLEIF

8.1.4. application/cesr

Type name:

* application

Subtype name:

* cesr

Required parameters:

* None

Optional parameters:

- * profile — Indicates the payload conforms to a specific vLEI credential type.
- * encoding — Indicates the CESR stream is text or binary. Defaults to text. encoding=binary indicates the CESR stream is binary encoded.
- * charset — Indicates character set for text encodings. Defaults to UTF-8.

Encoding considerations:

- * CESR defaults to UTF-8 text encoding and is self-framing.
- * CESR can also be a binary stream. When used in binary mode the encoding option MUST be specified (e.g., encoding=binary).

Security considerations:

- * See Section 8.

Interoperability considerations:

None.

Published specification:

- * RFCthis
- * Key Event Receipt Infrastructure (KERI) — [KERI-Spec]
- * Authentictic Chained Data Containers (ACDC) — [ACDC-Spec]
- * Composable Event Streaming Representation (CESR) — [CESR-Spec]
- * GLEIF vLEI Credential Schema Registry — [GLEIF-vLEI-Part3]

Applications that use this media type:

- * GLEIF vLEI issuance and verification systems
- * SATP-compliant credential exchange platforms
- * Forensic credential chaining and audit systems

Fragment identifier considerations:

* None

Additional information:

* Magic number(s): None

* File extension(s): .acdccesr

* Macintosh file type code(s): None

Person & email address to contact for further information:

* N. Smith ned.smith.ietf@outlook.com
(mailto:ned.smith.ietf@outlook.com)

* GLEIF IT Team vlel-support@gleif.org (mailto:vlei-support@gleif.org)

Intended usage:

* COMMON

Author:

* N. Smith ned.smith.ietf@outlook.com
(mailto:ned.smith.ietf@outlook.com)

* GLEIF IT Team vlel-support@gleif.org (mailto:vlei-support@gleif.org)

Change controller:

* IETF / GLEIF

8.2. CoAP Content-Format ID Assignments

IANA is requested to assign the following Content-Format numbers in the "CoAP Content-Formats" sub-registry, within the "Constrained RESTful Environments (CoRE) Parameters" Registry [IANA.core-parameters]:

Content-Type	Content Coding	ID	Reference
application/cesr+json	-	TBA1	RFCthis
application/cesr+cbor	-	TBD2	RFCthis

application/cesr+msgpk	-	TBD3	RFCthis
application/cesr	-	TBD4	RFCthis
application/ cesr+json;profile=urn:vlei:leid	-	TBA10	RFCthis
application/ cesr+json;profile=urn:vlei:ecr	-	TBA11	RFCthis
application/ cesr+json;profile=urn:vlei:oor	-	TBA12	RFCthis
application/ cesr+json;profile=urn:vlei:oor	-	TBA13	RFCthis
application/ cesr+json;profile=urn:vlei:qvi	-	TBA14	RFCthis
application/ cesr+json;profile=urn:vlei:ecra	-	TBA15	RFCthis
application/ cesr+cbor;profile=urn:vlei:leid	-	TBA20	RFCthis
application/ cesr+cbor;profile=urn:vlei:ecr	-	TBA21	RFCthis
application/ cesr+cbor;profile=urn:vlei:oor	-	TBA22	RFCthis
application/ cesr+cbor;profile=urn:vlei:oor	-	TBA23	RFCthis
application/ cesr+cbor;profile=urn:vlei:qvi	-	TBA24	RFCthis
application/ cesr+cbor;profile=urn:vlei:ecra	-	TBA25	RFCthis
application/ cesr+msgpk;profile=urn:vlei:leid	-	TBA30	RFCthis
application/ cesr+msgpk;profile=urn:vlei:ecr	-	TBA31	RFCthis
application/	-	TBA32	RFCthis

cesr+msgpk;profile=urn:vlei:oor				
+-----+-----+-----+-----+				
application/ cesr+msgpk;profile=urn:vlei:oor	-	TBA33	RFCthis	
+-----+-----+-----+-----+				
application/ cesr+msgpk;profile=urn:vlei:qvi	-	TBA34	RFCthis	
+-----+-----+-----+-----+				
application/ cesr+msgpk;profile=urn:vlei:ecra	-	TBA35	RFCthis	
+-----+-----+-----+-----+				
application/ cesr;profile=urn:vlei:leid	-	TBA40	RFCthis	
+-----+-----+-----+-----+				
application/ cesr;profile=urn:vlei:ecr	-	TBA41	RFCthis	
+-----+-----+-----+-----+				
application/ cesr;profile=urn:vlei:oor	-	TBA42	RFCthis	
+-----+-----+-----+-----+				
application/ cesr;profile=urn:vlei:oor	-	TBA43	RFCthis	
+-----+-----+-----+-----+				
application/ cesr;profile=urn:vlei:qvi	-	TBA44	RFCthis	
+-----+-----+-----+-----+				
application/ cesr;profile=urn:vlei:ecra	-	TBA45	RFCthis	
+-----+-----+-----+-----+				

Table 6: New Content-Formats

9. References

9.1. Normative References

[REQ-LEVEL]

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>>.

- [I-D.ietf-satp-core]
Hargreaves, M., Hardjono, T., Belchior, R., Ramakrishna, V., and A. Chiriac, "Secure Asset Transfer Protocol (SATP) Core", Work in Progress, Internet-Draft, draft-ietf-satp-core-11, 7 August 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-satp-core-11>>.
- [RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <<https://www.rfc-editor.org/rfc/rfc7159>>.
- [RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <<https://www.rfc-editor.org/rfc/rfc7517>>.
- [RFC2585] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", RFC 2585, DOI 10.17487/RFC2585, May 1999, <<https://www.rfc-editor.org/rfc/rfc2585>>.
- [RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <<https://www.rfc-editor.org/rfc/rfc4648>>.
- [STD96] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <<https://www.rfc-editor.org/rfc/rfc9052>>.
- [STD91] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <<https://www.rfc-editor.org/rfc/rfc6838>>.
- [RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <<https://www.rfc-editor.org/rfc/rfc7252>>.
- [RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <<https://www.rfc-editor.org/rfc/rfc8610>>.

[GLEIF-vLEI-Part1]

Global Legal Entity Identifier Foundation, "Technical Requirements Part 1: KERI Infrastructure", GLEIF vLEI-EGF-TechReq-Part1-v1.3, 16 April 2025, <https://www.gleif.org/organizational-identity/introducing-the-verifiable-lei-vlei/introducing-the-vlei-ecosystem-governance-framework/2025-04-16_vlei-egf-v3.0-technical-requirements-part-1-keri-infrastructure-2024_v1.3_final.pdf>.

[GLEIF-vLEI-Part2]

Global Legal Entity Identifier Foundation, "Technical Requirements Part 2: vLEI Credentials", GLEIF vLEI-EGF-TechReq-Part2-v1.1, 15 December 2023, <https://www.gleif.org/media/pages/organizational-identity/introducing-the-verifiable-lei-vlei/introducing-the-vlei-ecosystem-governance-framework/7040021178-1759312105/2023-12-15_vlei-egf-v3.0-technical-requirements-part-2-vlei-credentials_v1.1-final.pdf>.

[GLEIF-vLEI-Part3]

Global Legal Entity Identifier Foundation, "Technical Requirements Part 3: vLEI Credential Schema Registry", GLEIF vLEI-EGF-TechReq-Part3-v1.1, 15 December 2023, <https://www.gleif.org/media/pages/organizational-identity/introducing-the-verifiable-lei-vlei/introducing-the-vlei-ecosystem-governance-framework/7040021178-1759312105/2023-12-15_vlei-egf-v3.0-technical-requirements-part-2-vlei-credentials_v1.1-final.pdf>.

[ISO17442-3]

International Organization for Standardization, "Financial services — Legal entity identifier (LEI) — Part 3: Verifiable LEIs (vLEIs)", ISO 17442-3:2024, 2024, <<https://www.iso.org/standard/85628.html>>.

[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>>.

[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>>.

[IANA.media-types]
IANA, "Media Types",
<<https://www.iana.org/assignments/media-types>>.

[IANA.core-parameters]
IANA, "Constrained RESTful Environments (CoRE)
Parameters",
<<https://www.iana.org/assignments/core-parameters>>.

9.2. Informative References

[I-D.ietf-satp-architecture]
Hardjono, T., Hargreaves, M., Smith, N., and V.
Ramakrishna, "Secure Asset Transfer (SAT) Interoperability
Architecture", Work in Progress, Internet-Draft, draft-
ietf-satp-architecture-08, 31 July 2025,
<<https://datatracker.ietf.org/doc/html/draft-ietf-satp-architecture-08>>.

[ISO17442-1]
International Organization for Standardization, "Financial
services — Legal entity identifier (LEI) — Part 1:
Assignment", ISO 17442-1:2020, 2020,
<<https://www.iso.org/standard/59771.html>>.

[KERI-Spec]
Trust Over IP Foundation, "Key Event Receipt
Infrastructure (KERI) Specification, v0.9, Draft", TOIP
TSWG-KERI-2023, 2023,
<<https://trustoverip.github.io/tswg-keri-specification/>>.

[KERI-glossary]
Trust Over IP Foundation, "KERI Suite Glossary, Draft 01",
n.d., <<https://trustoverip.github.io/kerisuite-glossary/>>.

[ACDC-Spec]
Trust Over IP Foundation, "Authentic Chained Data
Containers (ACDC) Specification, v0.9, Draft", TOIP TSWG-
ACDC-2023, 2023,
<<https://trustoverip.github.io/tswg-acdc-specification>>.

[CESR-Spec]
Trust Over IP Foundation, "Composable Event Streaming
Representation (CESR) Proof Format Specification, v0.9,
Draft", TOIP TSWG-CESR-2023, 2023,
<<https://trustoverip.github.io/tswg-cesr-specification/>>.

[GLEIF-vLEI-EGF]

Global Legal Entity Identifier Foundation, "Verifiable LEI (vLEI) Ecosystem Governance Framework v3.0: Primary and Controlled Documents", GLEIF vLEI-EGF-v3.0, 16 April 2025, <<https://www.gleif.org/en/vlei/introducing-the-vlei-ecosystem-governance-framework>>.

[vLEI-glossary]

Global Legal Entity Identifier Foundation, "Verifiable LEI (vLEI) Ecosystem Governance Framework 3.0: Glossary", GLEIF v1.3, 15 December 2023, <https://www.gleif.org/organizational-identity/introducing-the-verifiable-lei-vlei/introducing-the-vlei-ecosystem-governance-framework/2023-12-15_vlei-egf-v3.0-glossary_v1.3-final.pdf>.

[ACM-Calculus]

Abadi, M., Burrows, M., Lampson, B., and G. Plotkin, "A Calculus for Access Control in Distributed Systems", ACM TOPLAS 15(4), pp. 706734, October 1993, <<https://dl.acm.org/doi/10.1145/155183.155225>>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/rfc/rfc4949>>.

[ISO17442-1_2020]

International Organization for Standardization, "Financial services — Legal entity identifier (LEI) — Part 1: Assignment", ISO 17442-1:2020, 2020, <<https://www.iso.org/standard/78829.html>>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/rfc/rfc5280>>.

[STD94] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <<https://www.rfc-editor.org/rfc/rfc8949>>.

[MSGPCK] MessagePack Community, "MessagePack Specification", 2023, <<https://github.com/msgpack/msgpack/blob/master/spec.md>>.

Appendix A. Full CDDL

(Artwork only available as CDDL: see <https://www.ietf.org/archive/id/draft-smith-satp-vlei-binding-01.html>)

Appendix B. Examples in JSON

The following SATP wrapper examples show synthetic vLEI data:

```
{
  "verifiedOriginatorEntityId": {
    "content": {
      "mt": "application/cesr+json;profile=urn:vlei:leid"
      // JSON serialization of an ACDC credential (LEID profile)
    },
    "payload": "ACDC10JSON...SAID...i:did:keri:..."
    // literal ACDC JSON text, not base64
  }
}

{
  "verifiedBeneficiaryEntityId": {
    "content": {
      "mt": "application/cesr;profile=urn:vlei:leid;encoding=binary"
    },
    "payload": "QUNEQzEwQ0JPUkVhc2U2NEVuY29kZWQvLi4u"
    // base64 of binary CESR serialization of SAID credential (LEID profile)
  }
}

{
  "senderGatewayOwnerId": {
    "content": {
      "mt": "application/cesr+msgpk;profile=urn:vlei:leid"
      // cf, cbt, oid omitted here — optional in schema
    },
    "payload": "ACDC10MSGP...SAID...i:did:keri:..."
    // MessagePack serialization of an ACDC credential (LEID profile)
  }
}
```

```
{
  "receiverGatewayOwnerId": {
    "content": {
      "mt": "application/cesr;profile=urn:vlei:leid;encoding=base64uri"
      // could also include cf, cbt, oid if known
    },
    "payload": "QUNEQzEwQ0VTUkJhc2U2NEVuY29kZWQvLi4u"
    // Base64 of binary CESR stream encoding of SAID credential
  }
}

{
  "senderGatewayId": {
    "content": {
      "mt": "application/cesr;profile=urn:vlei:ecr"
      // cf, cbt, oid omitted — optional in schema
    },
    "payload": "ACDC10CESR...SAID...i:did:keri:..."
    // CESR-encoded ACDC credential (ECR profile) as plain text
  }
}

{
  "recipientGatewayId": {
    "content": {
      "mt": "application/cesr+cbor;profile=urn:vlei:ecr", // from vlei-media-type enum
      "cf": 0,
      "oid": "1.2.3.4.6" // actual OID for this credential type
    },
    "payload": "ACDC10CBORTESTSAIDi:did:keri:EXAMPLERGWNETID"
    // raw CBOR bytes or base64/base64url string, but not CBOR-tagged
  }
}

{
  "senderGatewayNetworkId": {
    "content": {
      "mt": "application/cesr+cbor;profile=urn:vlei:ecr;encoding=base64uri",
      "cbt": false // no TN() CBOR tag; just base64 of raw CBOR
    },
    "payload": "oWJ0ZXN0LWVjciljcmVkJkZW50aWFs..."
    // base64 of the CBOR-encoded ACDC (ECR profile)
  }
}
```

```
{
  "senderGatewayNetworkId": {
    "content": {
      "mt": "application/cesr+cbor;profile=urn:vlei:ecr;encoding=base64uri",
      "cbt": false // no TN() CBOR tag; just base64 of raw CBOR
    },
    "payload": "gEEBAQ..."
  } // base64 of CBOR-encoded ACDC (ECR profile)
}
```

The following SATP wrapper examples show synthetic key data:

```
{
  "originatorPubkey": {
    "content": "application/jwk+json",
    "payload": "{ \"kty\": \"EC\", \"crv\": \"P-256\", \"x\": \"...\", \"y\": \"...\" }"
  },
  "beneficiaryPubkey": {
    "content": "application/cose;cose-type=cose-key",
    "encoding": "base64uri", // explicitly flagging representation
    "payload": "aEtNQnBRLi4u" // base64 of CBOR COSE_Key bytes
  },
  "senderGatewaySignaturePublicKey": {
    "content": "application/jwk+json",
    "payload": "{ \"kty\": \"RSA\", \"n\": \"...\", \"e\": \"AQAB\" }"
  },
  "receiverGatewaySignaturePublicKey": {
    "content": "application/cose;cose-type=cose-key",
    "encoding": "base64uri",
    "payload": "aEtNQ3BBLi4u"
  },
  "senderGatewayDeviceIdentityPubkey": {
    "content": "application/pkix-cert",
    "encoding": "PEM",
    "payload": "-----BEGIN CERTIFICATE-----\nMIIB...==\n-----END CERTIFICATE-----"
  },
  "receiverGatewayDeviceIdentityPubkey": {
    "content": "application/pkix-cert",
    "encoding": "DER",
    "payload": "MIIB..." // base64 DER
  }
}
```

Acknowledgments

Nicholas Racz for review, comments, and ecosystem alignment contributions.

Samuel Smith for review, comments, and KERI ACDC CESR and vLEI insights.

Author's Address

Ned Smith
Independent
Email: ned.smith.ietf@outlook.com