Secure Asset Transfer Protocol
Internet-Draft
Intended status: Standards Track
Expires: 17 March 2026

N. Smith
Independent

13 September 2025

A SATP Core Binding for vLEI Identities
draft-smith-satp-vlei-binding-00

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

Copyright Notice

Table of Contents

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 liveliness 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.

3. Identities

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 differennt 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] bound to a cryptographic key is also known as a principal [ACM-Calculus].

A legal entity is defined by [ISO17442-1_2020] section 1 (scope).

vLEIs [ISO17442-3] use Autonomic Identifiers (AID) to name legal entities and to bind cryptographic keys, to form vLEI principals. AIDs are contained within an Authentic Chained Data Contain (ACDC) [ACDC-Spec] credential. AIDs link to Key Event Logs (KEL) that are form of key attestation. KELs change periodically as key event receipts are added to the log, thus key state could have security implications. The state of the vLEI credential may change between SATP stages or whenever a key is used. The state of an ACDC is locked to keystate at issuance. A cryptographic hash of an ACDC credential and its initial key state can be referenced using a Self-Addressing Identifier (SAID) [CESR-Spec].

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 during asset exchange. Ideally, SATP principals (including key state) are unchanging during complete asset exchange (or full rollback). However, if key-state can’t be locked as part of a SATP ACID exchange, key state verification at each SATP stage may be needed.

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 furthur strengthen trustworthiness claims of SATP endpoints. Some SATP keys do not use vLEI credentals, but could still be based on ACDC credentials. Still other credential types

(e.g., X.509 [RFC5280])) could be used for non-natural person entities. Nevertheless, use of a Key Event Recipt Infrastructure (KERI) [KERI-Spec] key means these keys can benefit from KEL-based key attestation.

RFCthis assumes SATP identifiers and public keys are artifacts of a credential issued to a common entity. Nevertheless, the GatewayDeviceIdentityPublicKey could be associated with a different credential from the one belongin to the GatewaySignaturePublicKey. Consequently, there MAY be additional credentials issued to SATP principals that require additional verifier processing.

// Note1: Need to check if there is a KERI key encoding other than
// CESR and if ACDC is sufficient to describe the key.
//
// -- Ned Smith

3.1. 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 identifer (AID), which is semantically aligned with SATP IDs.

SATP Entity	SATP Message	Structure
Originator	OriginatorCredential -implied-	ACDC
	originatorPubkey	ACDC or other
	verifiedOriginatorEntityID	AID
Sender Gateway Owner	senderGatewayOwnerCredential -implied-	ACDC
	senderGatewayOwnerID	AID
Sender Gateway (G1)	senderGatewayCredential -implied-	ACDC
	senderGatewaySignaturePublicKey	ACDC or other

	senderGatewayId	AID
	senderGatewayDeviceIdentityCredential -implied-	ACDC
	senderGatewayDeviceIdentityPubkey	ACDC or other
	senderGatewayDeviceIdentityId -implied-	AID
Sender Network	senderNetworkCredential -implied-	ACDC
	senderGatewayNetworkId	AID
.....	.....	....
Beneficiary	BeneficiaryCredential -implied-	ACDC
	beneficiaryPubkey	ACDC or other
	verifiedBeneficiaryEntityID	AID
Receiver Gateway Owner	receiverGatewayOwnerCredential -implied-	ACDC
	senderGatewayOwnerID	AID
Receiver Gateway (G2)	receiverGatewayCredential -implied-	ACDC
	receiverGatewaySignaturePublicKey	ACDC or other
	receiverGatewayId	AID
	receiverGatewayDeviceIdentityCredential -implied-	ACDC
	receiverGatewayDeviceIdentityPubkey	ACDC or other
	receiverGatewayDeviceIdentityId -implied-	AID
Recipient Network	recipientNetworkCredential -implied-	ACDC

	recipientGatewayNetworkId	AID

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

// Note2: Need to describe how this draft approaches protocol binding
// where focus is on top-down, but not ignoring buttom up eg tls.
//
// -- Ned Smith

3.2. 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	OORA
LegalEntityOfficialOrganizationalRolevLEICredential	OOR
ECRAuthorizationvLEICredential	ECRA
LegalEntityEngagementContextRolevLEICredential	ECR

Table 2: vLEI Ecosystem Roles

vLEI defines a role architecdture that is hierarchical. A QVI role oversees lifecycle of LEID, OORA, and ECRA roles. The OORA role oversees lifecycle of OOR roles and the ECRA role oversees the lifecycle of ECR roles. The LEID, OOR, and ECR roles could oversee lifecycle of non-vLEI credentials; which are classified as non-natural person credentials by [ISO17442-1_2020].

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 8.

// Note3: 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, X.509).
//
// -- 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 stages.

Table 3 maps SATP entities to specific vLEI roles.

#	SATP Entity	vLEI Role
1	Originator, Beneficiary, Gateway Owner	LEID
2	GatewaySignature, GatewayNetwork, GatewayDeviceIdentity	non-natural person credential
3	Gateway Admin, Network Admin, Gateway Operations Manager, Network Operations Manager	ECR

Table 3: Mapping SATP Entity to vLEI Role

// Note4: The various xxxID messages are tstr values - the
// stringified representation of the vLEI credential identifer should
// be used here. This is probably an SAID. For a SATP-JSON binding,
// the SAID MUST use the text form of the CESR derivation code. For

```
// a SATP-CBOR or other binary binding the SAID MUST use the binary
// form of the CESR derivation code.
//
// -- Ned Smith
```

4.1.1. LegalEntityIdentityvLEICredential Credentials

The SATP Messages in row 1 of Table 3 is a LegalEntityvLEICredential as defined by the LEvLEIC (https://github.com/GLEIF-IT/vLEI-schema/blob/main/legal-entity-vLEI-credential.json) schema.

These messages are realized using a Legal Entity vLEI Credential (LEvLEIC) because these message identify legal entities. Gateway owner identities area form of legal entity as they identify the owner of a gateway rather than the gateway itself.

4.1.2. 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.

4.1.3. Other 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 3 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...

4.2. Key Structures

Keys embedded in hardware or firmware may not easily be converted to an interoperablel 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 ACDC [ACDC-Spec] credentials.

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 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 follwing 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 Optonal 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:oora
LegalEntityOfficialOrganizationalRolevLEICredential (OOR)	profile=urn:vlei: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 Optonal 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 Optonal 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-TechReq-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-TechReq-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 vlei-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 vlei-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-TechReq-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 vlei-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 vlei-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-TechReq-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 vlei-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 vlei-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-TechReq-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 vlei-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 vlei-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:lar	-	TBA13	RFCthis
application/ cesr+json;profile=urn:vlei:qvi	-	TBA14	RFCthis
application/ cesr+json;profile=urn:vlei:vra	-	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:lar	-	TBA23	RFCthis
application/ cesr+cbor;profile=urn:vlei:qvi	-	TBA24	RFCthis
application/ cesr+cbor;profile=urn:vlei:vra	-	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:lar	-	TBA33	RFCthis
application/ cesr+msgpk;profile=urn:vlei:qvr	-	TBA34	RFCthis
application/ cesr+msgpk;profile=urn:vlei:vra	-	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:lar	-	TBA43	RFCthis
application/ cesr;profile=urn:vlei:qvr	-	TBA44	RFCthis
application/ cesr;profile=urn:vlei:vra	-	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-TechReq-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-TechReq-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/en/vlei/introducing-the-vlei-ecosystem-governance-framework>.

[GLEIF-vLEI-TechReq-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/en/vlei/introducing-the-vlei-ecosystem-governance-framework>.

[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/>.

[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: Primary and Controlled Documents", GLEIF vLEI-EGF-v3.0, 16 April 2025, <https://www.gleif.org/en/vlei/introducing-the-vlei-ecosystem-governance-framework>.

[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>.

Appendix A. Full CDDL

```
start = satp-message

non-empty<M> = (M) .and ({ + any => any })

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
}


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

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"
```

```
   }>


   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
   }

   vlei-media-type =
     "application/cesr+json;profile=urn:vlei:leid" /
     "application/cesr+json;profile=urn:vlei:ecr" /
     "application/cesr+json;profile=urn:vlei:ecr;charset=utf-16le" /
     "application/cesr+json;profile=urn:vlei:oor" /
     "application/cesr+json;profile=urn:vlei:ecra" /
     "application/cesr+json;profile=urn:vlei:qvi" /
     "application/cesr+json;profile=urn:vlei:oora" /
     "application/cesr+json;profile=urn:vlei:oora;encoding=base64uri" /
     "application/cesr+cbor;profile=urn:vlei:leid" /
     "application/cesr+cbor;profile=urn:vlei:leid;encoding=text" /
     "application/cesr+cbor;profile=urn:vlei:ecr" /
     "application/cesr+cbor;profile=urn:vlei:ecr;encoding=base64uri" /
     "application/cesr+cbor;profile=urn:vlei:ecr;encoding=text" /
     "application/cesr+cbor;profile=urn:vlei:oor" /
     "application/cesr+cbor;profile=urn:vlei:oor;encoding=text" /
     "application/cesr+cbor;profile=urn:vlei:ecra" /
     "application/cesr+cbor;profile=urn:vlei:ecra;encoding=text" /
     "application/cesr+cbor;profile=urn:vlei:qvi" /
     "application/cesr+cbor;profile=urn:vlei:qvi;encoding=text" /
     "application/cesr+cbor;profile=urn:vlei:oora" /
     "application/cesr+cbor;profile=urn:vlei:oora;encoding=text" /
     "application/cesr+msgpk;profile=urn:vlei:leid" /
```

```
     "application/cesr+msgpk;profile=urn:vlei:leid;encoding=text" /
     "application/cesr+msgpk;profile=urn:vlei:ecr" /
     "application/cesr+msgpk;profile=urn:vlei:ecr;encoding=text" /
     "application/cesr+msgpk;profile=urn:vlei:oor" /
     "application/cesr+msgpk;profile=urn:vlei:oor;encoding=text" /
     "application/cesr+msgpk;profile=urn:vlei:ecra" /
     "application/cesr+msgpk;profile=urn:vlei:ecra;encoding=text" /
     "application/cesr+msgpk;profile=urn:vlei:qvi" /
     "application/cesr+msgpk;profile=urn:vlei:qvi;encoding=text" /
     "application/cesr+msgpk;profile=urn:vlei:oora" /
     "application/cesr+msgpk;profile=urn:vlei:oora;encoding=text" /
     "application/cesr;profile=urn:vlei:leid" /
     "application/cesr;profile=urn:vlei:leid;encoding=binary" /
     "application/cesr;profile=urn:vlei:leid;encoding=base64uri" /
     "application/cesr;profile=urn:vlei:leid;charset=utf-16le" /
     "application/cesr;profile=urn:vlei:ecr" /
     "application/cesr;profile=urn:vlei:ecr;encoding=binary" /
     "application/cesr;profile=urn:vlei:oor" /
     "application/cesr;profile=urn:vlei:oor;encoding=binary" /
     "application/cesr;profile=urn:vlei:ecra" /
     "application/cesr;profile=urn:vlei:ecra;encoding=binary" /
     "application/cesr;profile=urn:vlei:qvi" /
     "application/cesr;profile=urn:vlei:qvi;bencoding=binary" /
     "application/cesr;profile=urn:vlei:oora" /
     "application/cesr;profile=urn:vlei:oora;encoding=binary"
```

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": "QUNEQzEwQ0JPUkJhc2U2NEVuY29kZWQvLi4u"
    // 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": "oWJ0ZXN0LWVjci1jcmVkZW50aWFs..."
    // 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

TODO acknowledge.

Author’s Address

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