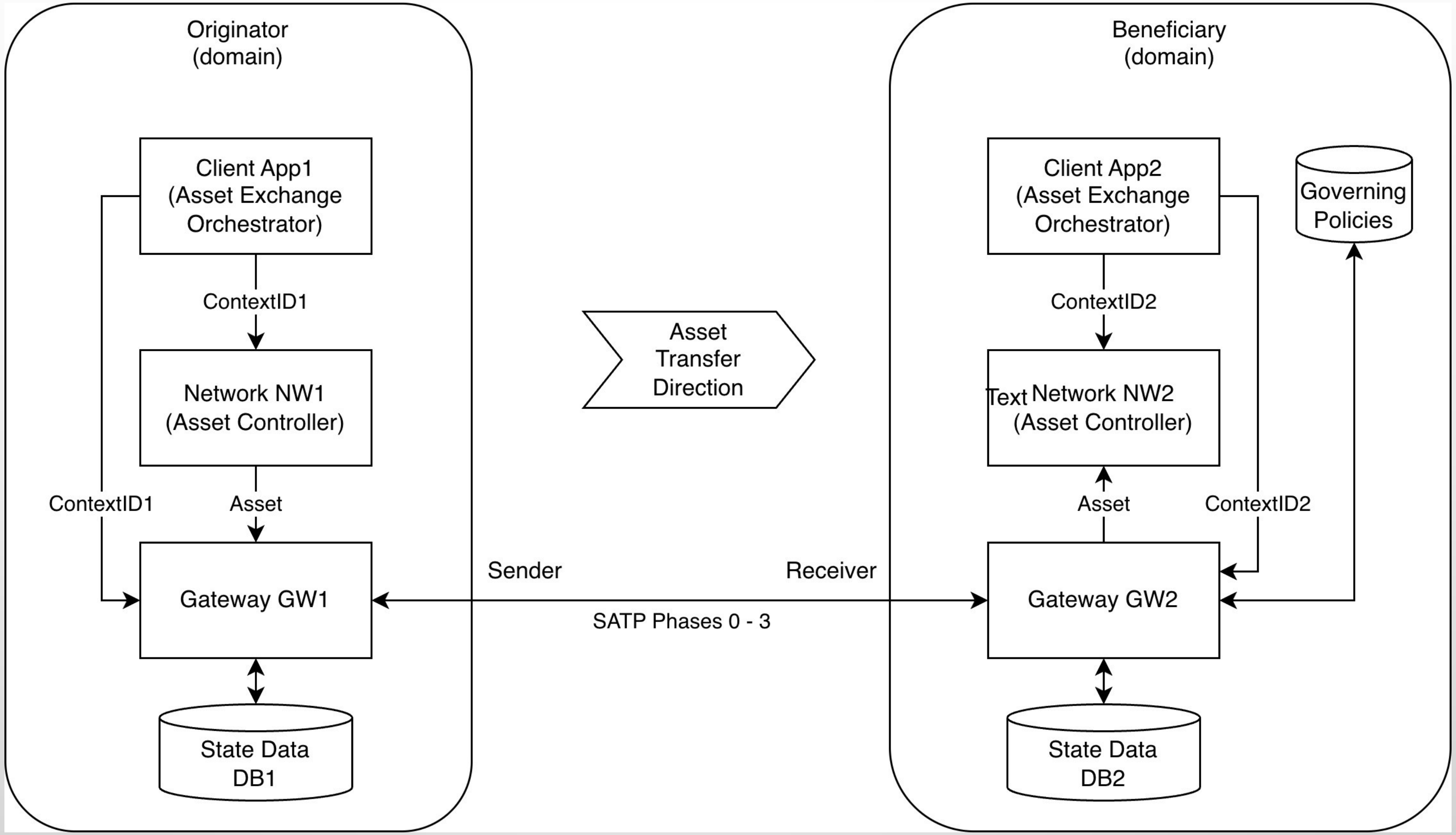
SATP-VLEI BINDING

NED SMITH

IETF124

SATP ARCHITECTURE OVERVIEW



Phase 0 Objectives:

- ContextID Establishment (G1, G2)
- Asset Identification (G1)
- Asset Ownership Validation (G1)
- Authorization To Transfer (G1)
- Exchange Of Travel Rule (G1, G2)
- Validation Of Gateway Ownership (G1, G2)
- Mutual Attestation (G1, G2)
- Negotiate Transfer Protocol (G1, G2)
- Asset Class Verification (G2)

SATP DOMAIN ENTITIES

Entities:

- **Originator / Beneficiary**: Legal entity financially and legally responsible for actions of the domain
- **Orchestrator Owner:** Legal entity responsible for asset exchange orchestration and Orchestrator management
- **Network Owner:** Legal entity responsible for network operation and Network management
- **Gateway Owner:** Legal entity responsible for asset exchange gateway operation and Gateway management
- **Orchestrator:** Host controlling asset exchange orchestration
- **Network:** Host controlling domain assets
- **Gateway:** Host controlling asset exchange

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 (humans) except where they act as sole proprietors recognized as legal entities

VLEI ROLES AND ENTITIES

Global Legal Entity Authority (GLEA)

- **Role**: Root Namespace Authority.
- **Instance:** GLEIF (the one and only entity in this role).
- **Duties**: Manages the globally rooted LEI namespace and issues QVI Authorization Credentials.

Qualified vLEI Issuer (QVI)

- **Role**: Accredited legal entity authorized by GLEA.
- **Duties**: Issues Legal Entity Credentials (LEID) to organizations.

Legal Entity (LEID holder)

- **Role**: Credentialed organization.
- **Duties**: Authorized to issue Official Organizational Role (OOR) and Engagement Context Role (ECR) credentials.
- **Delegation**: May delegate issuance authority via OORA (for OORs) and ECRA (for ECRs).

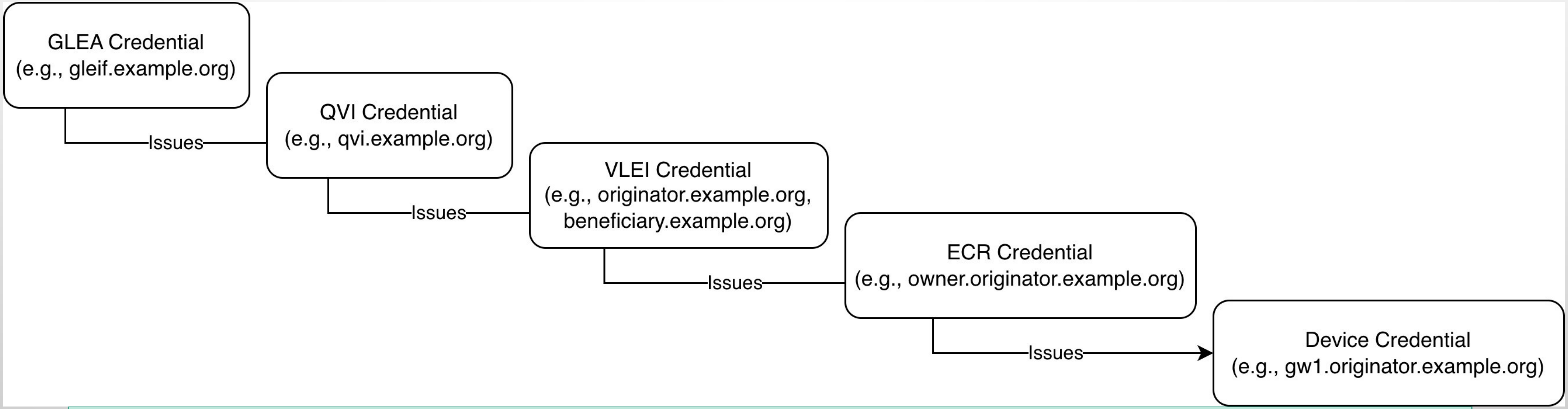
Official Organizational Role (OOR)

- **Role**: Individual bound to a formally recognized, legally accountable position within the entity (e.g., CEO, CIO, CFO).
- **Duties**: Acts in an official, persistent capacity on behalf of the organization.
- **Delegation**: Issuance of OOR credentials may be delegated via an OORA.

Engagement Context Role (ECR)

- **Role:** Individual bound to a context-specific role (e.g., auditor, consultant, project manager).
- **Duties**: Acts in a scoped, engagement-bound capacity.
- **Delegation**: Issuance of ECR credentials may be delegated via an ECRA.

VLEI CREDENTIAL HIERARCHY WITH SATP ENTITIES

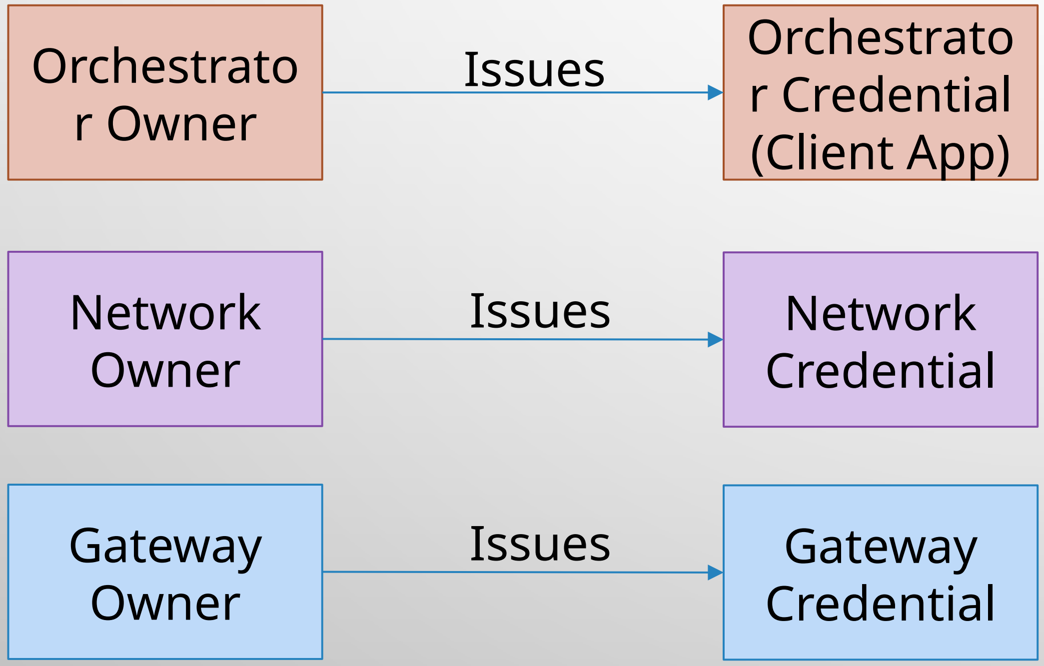


- *Originator*, and *Beneficiary* are LEID holders for their respective organizations / domains.
- *Orchestrator Owner*, *Network Owner*, and *Gateway Owner* are ECR holders.
- There may be officers of the organization / domain that are OOR holders.

vLEI authority hierarchy addresses Phase 0 objectives: Authorization to Transfer and Asset Ownership.

COMPLETING THE AUTHORIZATION ARCHITECTURE

- The ECR credential holders issue device credentials to the various SATP Architecture entities



Credentials could be any type:
- PKIX Certificates,
- OAuth2 Tokens,
- KERI Key Event Logs,
- Kerberos Tickets,

The current draft describes KERI and “other” (probably PKIX) credential types.

SATP Phase 1 anticipates using public keys (not symmetric)

BACKGROUND ON KEY EVENT RECEIPT INFRASTRUCTURE (KERI)

- Key-wielding entities are self-sovereign, meaning there isn’t a central authority vouching for end-entity key pairs.
- Trust in a key is determined by evaluating an entity’s key event log (KEL). This is a form of key attestation.
- KERI entities are identified by hashing the entity’s initial *key state* called *inception event called Autonomic ID (AID).*
- Inception key state contains:
  - current key(s),
  - Next (pre-rotated) keys(s),
  - the entities used to publish and verify key state,
  - configuration data.
- Interaction events associate application data with key state. Interaction events are logged in a KEL.
- KEL events are digitally signed using the key(s) wielded by the KERI entity.
- Verification walks a peer entity’s KEL verifying the application data is bound to the key state and that the key state is internally consistent.
- vLEI uses a type of application data called Authentic Chained Data Container (ACDC) that is bound to key state.
- The binding of application data to authorization data to key state is the basis for trusting application data.

VLEI BINDING TO SATP

- vLEI binding to SATP strategy is to identify SATP payloads containing vLEI content using media types or content format identifiers.
- This draft targets phase 1 transfer initialization claim artifacts:
  - **Public Keys**: originatorPubkey, beneficiaryPubkey, sender/receiverGatewaySignaturePublicKey, sender/receiverGatewayDeviceIdentityPubkey
  - **Identifiers**: verifiedOriginatorEntityId, verifiedBeneficiaryEntityId, sender/recipientGatewayId, sender/recipientGatewayNetworkId, sender/receiverGatewayOwnerId
- Since the artifacts originate from the outside, artifact payloads should be clearly disambiguated.
- This draft defines an artifact payload ”wrapper” consisting of a media type / CF ID and a payload.

```
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 ; CBOR tagged content
  ? oid: tstr
}>
```

MEDIA TYPE DEFINITION

- The draft anticipates registering media types for identifying wrapper payloads.
  - application/cesr+json
  - application/cesr+cbor
  - application/cesr+msgpk
  - application/cesr
- It also defines an optional *profile* parameter for vLEI use cases.
  - E.g., “application/cesr+json;profile=urn:vlei:qvi”

OPEN ISSUES

- draft-ietf-satp-core-11 doesn't appear to handle message payloads originating from outside. Does it make sense for satp core to define something like an artifact wrapper?
- *Public Keys* and *Identifiers* might be closely related given entity AIDs can discover associated KELs. And vLEI credentials contain issuer and issuee AIDs. Possibly, *originatorPubkey* and *verifiedOriginatorEntityId* are redundant when using KERI?
  - The core spec is somewhat quiet on how these artifacts are processed.
- *hashTransferInitClaim* is used to bind the transfer init context to other protocol messages. Given KERI key(s) sign satp messages, the GW key logs have self-addressing IDs (SAID) with transactional state that might be more secure than *hashTransferInitClaim*.

STATUS

- The current draft is at a -01 revision.
- It contains CDDL definition of artifact “wrapper” and media types.
- Additional authors welcome.
- The draft is a real-world binding of an identity and authorization framework that establishes asset ownership and authorization context.
- Key attestation and other ”trust” properties are built into underlying key management.
- ADOPT?