GLEIF

did:keri DID Method Resolver

Introducing did:keri Did Method Resolver

January 27, 2023

Presentation to Customs Border Protection/Department of Homeland Security

Agenda

1. First Step Towards Interoperability
2. Data Model: KERI Support for DID Doc Data
3. The Problem is Discovery
4. 3 Approaches to did:keri
5. did:keri with Introductions
6. did:keri-lite… The Magical DID
7. did:keri with Watcher Integration
8. Next Steps

First Step Towards Interoperability

First Steps Toward Interoperability

- Collaboration with members of many communities
  - Collaborative session at IIW
  - BC Gov (Stephan Curran)
  - Universal Resolver (Markus Sabadelo)
  - DIDComm community (Daniel Hardman, Sam Curran)
  - Current and prospective QVIs (Provenant)
  - RootsID working on PoC
- Providing interoperability with anyone using DIDComm
- Any KERI AID can become a KERI DID (AID is method specific identifier)
- Easily integrated into existing infrastructure
  - Python library integration
  - HTTPS REST API integration
- Planned integration with ACA-Py
- Community provided PoC and reference implementation

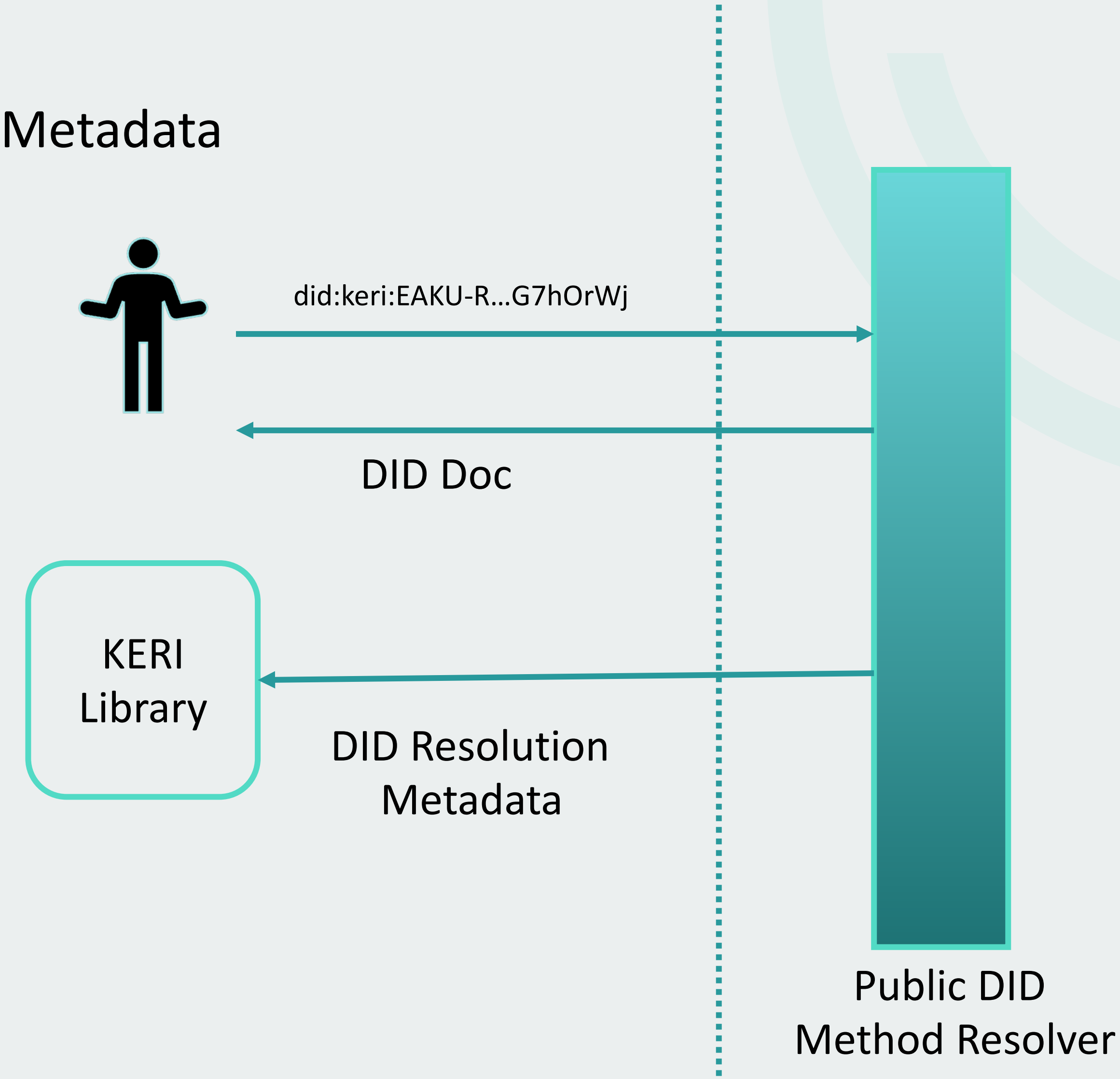
Data Model: KERI Support for DID Doc Data

Data Model: KERI Support for DID Doc Data

- DID Subject, DID Controller – KERI AID DID
- Verification Methods:
  - KERI public signing keys
  - Other keys committed to by AID
    - Keys derived from public signing keys (encryption)
    - Anchored in KEL (using cryptographic digest)
    - BADA (Best Available Data Acceptance) Policy
- Verification Relationships:
  - Authentication and assertion assigned to KERI public keys
  - Other types represented by key role BADA data
- Services:
  - KERI Services already defined and stored as BADA data
  - New Roles needed to map to external endpoint types (e.g. DIDComm)

Data Model: DID Resolution Metadata

- Securing the Last Mile
- KERI artifacts returned in DID Resolution Metadata
  - Key Event Log
  - Signed Key Commitments
  - Signed Service Endpoints
- Provides end-verifiability for consumers
- Allows for Public did:keri DID Resolvers
- Ensures Zero Trust



The Problem is Discovery

User Permissioned Percolated Discovery

Insight: Need-to-know just-in-time discovery (NTK-JIT)

Issuer may provide upon demand at issuance all information an Issuee (*Holder) needs to verify the issuance. Now Holder has discovered by percolation what it needs-to-know (NTK) just-in-time (JTK) to verify.*

Holder now may provide upon demand at presentation all information any verifier needs to to verify the presentation. Now verifier has discovered by percolation what it needs-to-know (NTK) just-in-time (JTK) to verify. This includes all the percolated discovery from Issuer to Holder.

Likewise the Verifier may imbue on a NTK-JIT basis any subsequent use of that information with all the percolated discovery information it already received from the Holder plus any other information the Verifier needs to contribute.

KERI End-Verifiability means zero-trust in the percolation path.
Discovery becomes an availability not a security problem.

User Permissioned Percolated Discovery

SPED (Speedy Percolated Endpoint Discovery)

Privacy preserving or public discovery as needed
User permissioned & totally decentralized

Watcher Network may provide super Nodes for aggregated discovery if desirable

End-to-end verifiability means any discovery source is as good as any other.
End verifiable “truth” is still true from whatever source it may have come.

This enables secure bootstrap of discovery from any source on a NTK JIT basis.

No need for a globally trusted discovery bootstrap resolver

OOBI (Out-of-Band-Introduction)

How to use DNS safely! Vacuous discovery of service endpoints.

OOBI = Url and AID   Simple enough for QR Code

```
http://8.8.5.6:8080/oobi/EaU6JR2nmwyZ-i0d8JZAoTNZH3ULvYAfSVPzhzS6b5CM
```

Variant: Use query string to label endpoint to be discovered.

```
http://8.8.5.6:8080/oobi/EaU6JR2nmwyZ-i0d8JZAoTNZH3ULvYAfSVPzhzS6b5CM?role=watcher&name=eve
https://example.com/oobi/EaU6JR2nmwyZ-i0d8JZAoTNZH3ULvYAfSVPzhzS6b5CM?role=witness
```

Well-Known Variant:

```
/.well-known/keri/oobi/EaU6JR2nmwyZ-i0d8JZAoTNZH3ULvYAfSVPzhzS6b5CM
```

Result of well-known request is target URL or redirection

```
https://example.com/witness/witmer  (redirection)
http://8.8.5.5:8080/witness/witmer  (public IP)
http://10.0.5.15:8088/witness/witmer  (private IP)
```

Any OOBI may forward to another OOBI.

This is safe because the eventual endpoint is end-verifiable (authenticated).

3 Approaches to did:keri

3 Approaches to did:keri

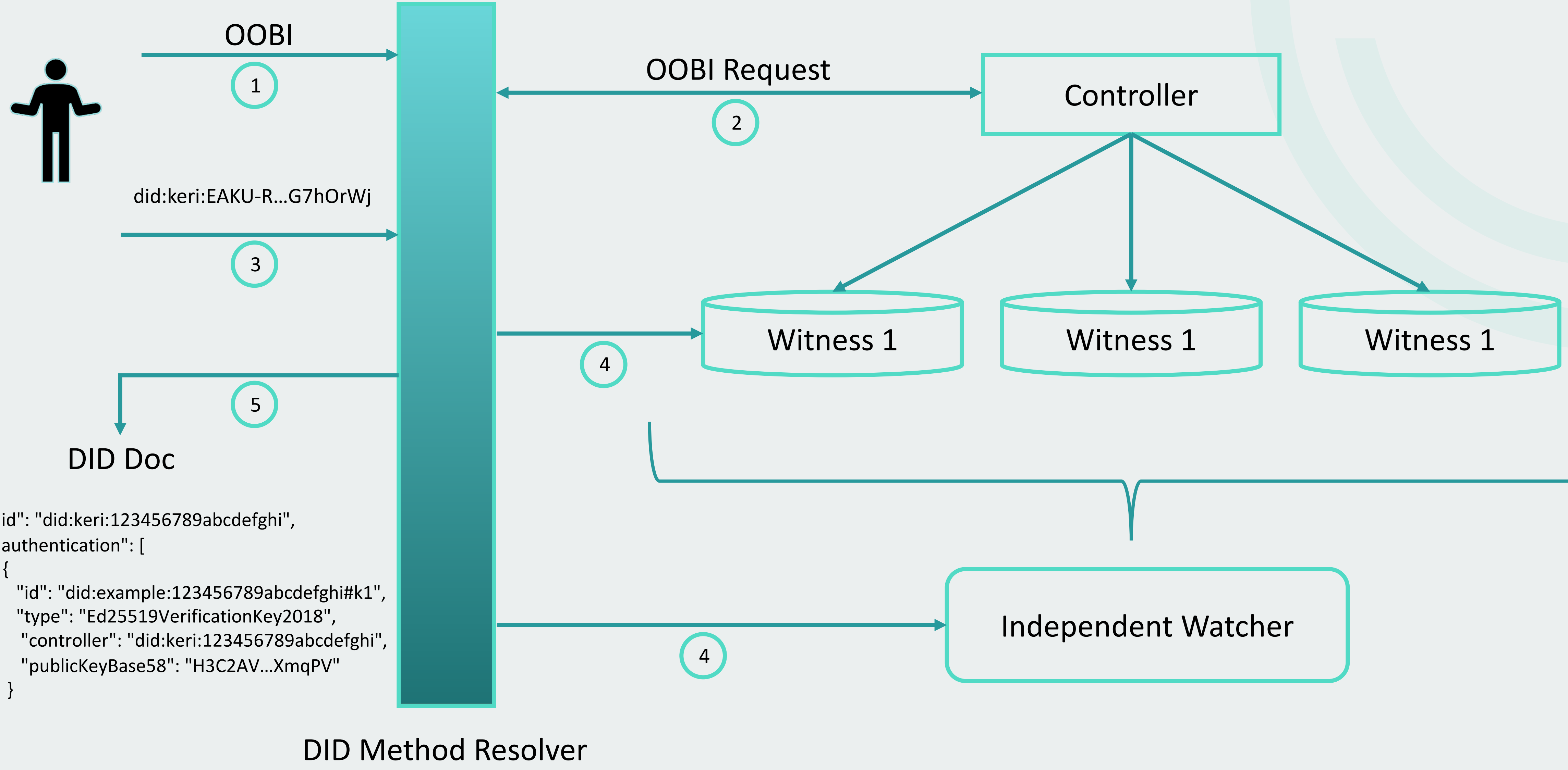
- **did:keri with Introductions**
  - —Leveraging native KERI discovery (OOBI & Percolated Discovery)
- **did:keri-lite – The Magical DID**
  - —Ephemeral DID support
- **did:keri with Watcher Integration**
  - —Multiple configuration options with local or Ecosystem Super Watchers

did:keri with Introductions

did:keri with Introductions

- Out-of-band mechanism to boot strap the communication
  - Initial KEL and service endpoints loaded
  - Similar to did:peer requirement to have Genesis DIDDoc
  - KERI OOBI protocol as opposed to DIDComm OOBI and DID Exchange
- Resolver runs local KERI and stores all needed data to generate DID Doc
- Updates are handled by standard KERI mechanisms
  - Polling updates
  - Gossip updates
  - Watcher Integration

did:keri with Introductions



DID Doc

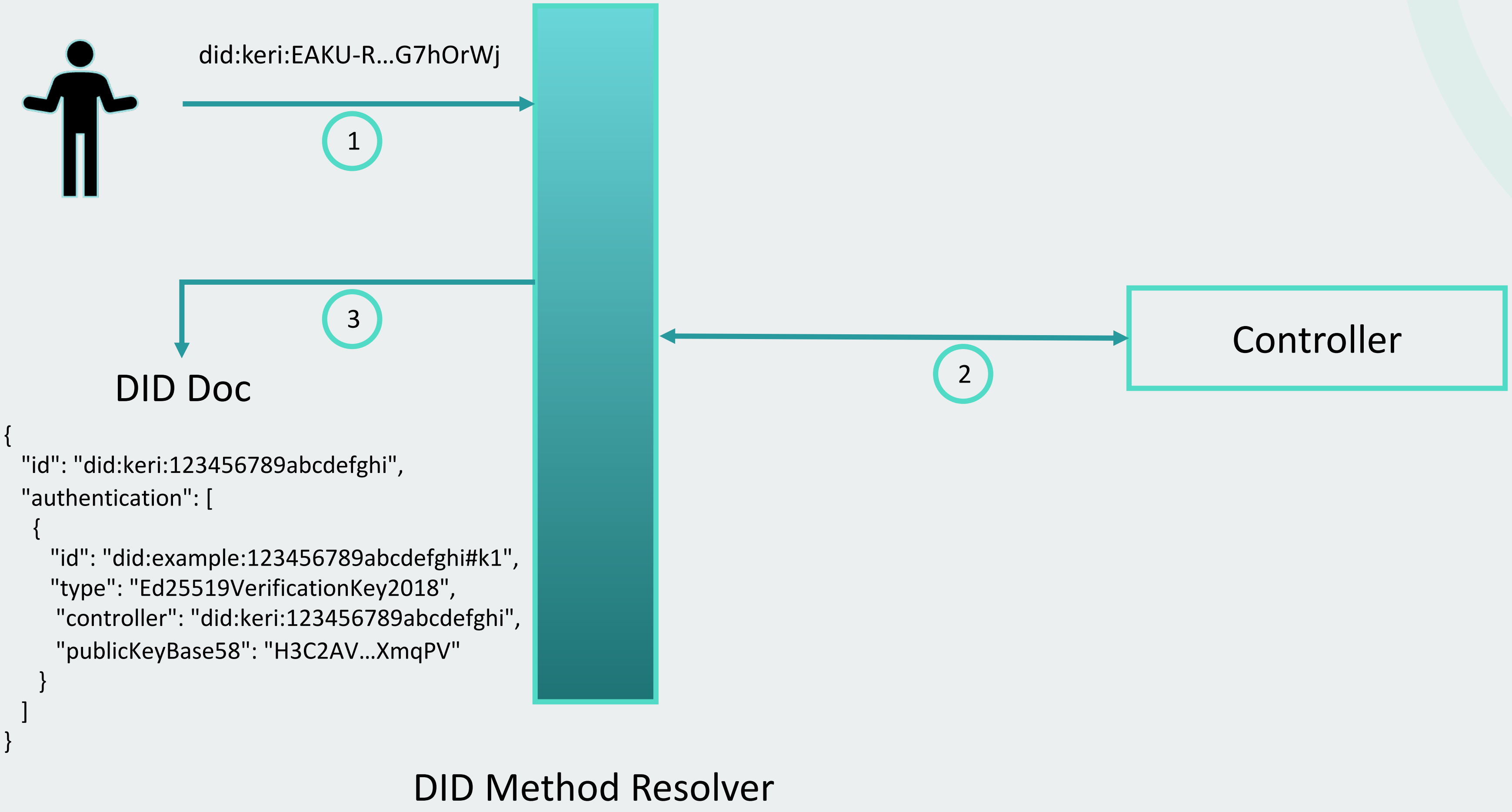
```
{
  "id": "did:keri:123456789abcdefghi",
  "authentication": [
    {
      "id": "did:example:123456789abcdefghi#k1",
      "type": "Ed25519VerificationKey2018",
       "controller": "did:keri:123456789abcdefghi",
       "publicKeyBase58": "H3C2AV…XmqPV"
    }
  ]
}
```

did:keri-lite… The Magical DID

did:keri-lite… The Magical DID

- Self contained DID with embedded inception event
  - Appended Base64 or CESR encoded event
  - Service endpoint embedded in inception event
- Maps to KERI Non-transferable identifier variant (effectively NT)
  - AID with inception event but no next keys
- Useful for ephemeral DIDs
  - Similar to static peer DIDs

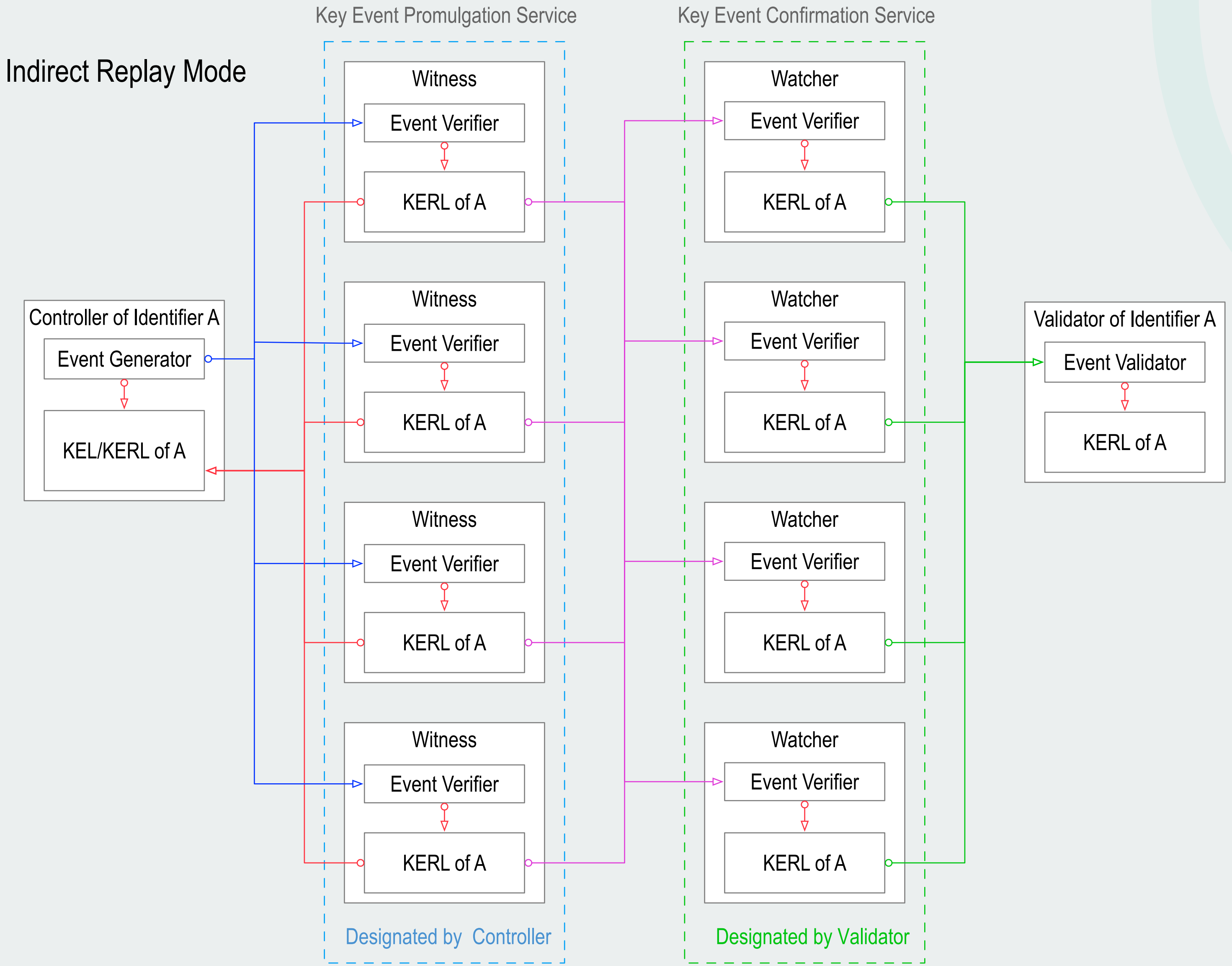
did:keri-lite… The Magical DID



```
{
  "id": "did:keri:123456789abcdefghi",
  "authentication": [
   {
     "id": "did:example:123456789abcdefghi#k1",
     "type": "Ed25519VerificationKey2018",
      "controller": "did:keri:123456789abcdefghi",
      "publicKeyBase58": "H3C2AV…XmqPV"
    }
  ]
}
```

did:keri with Watcher Integration

did:keri with Ecosystem Super Watchers

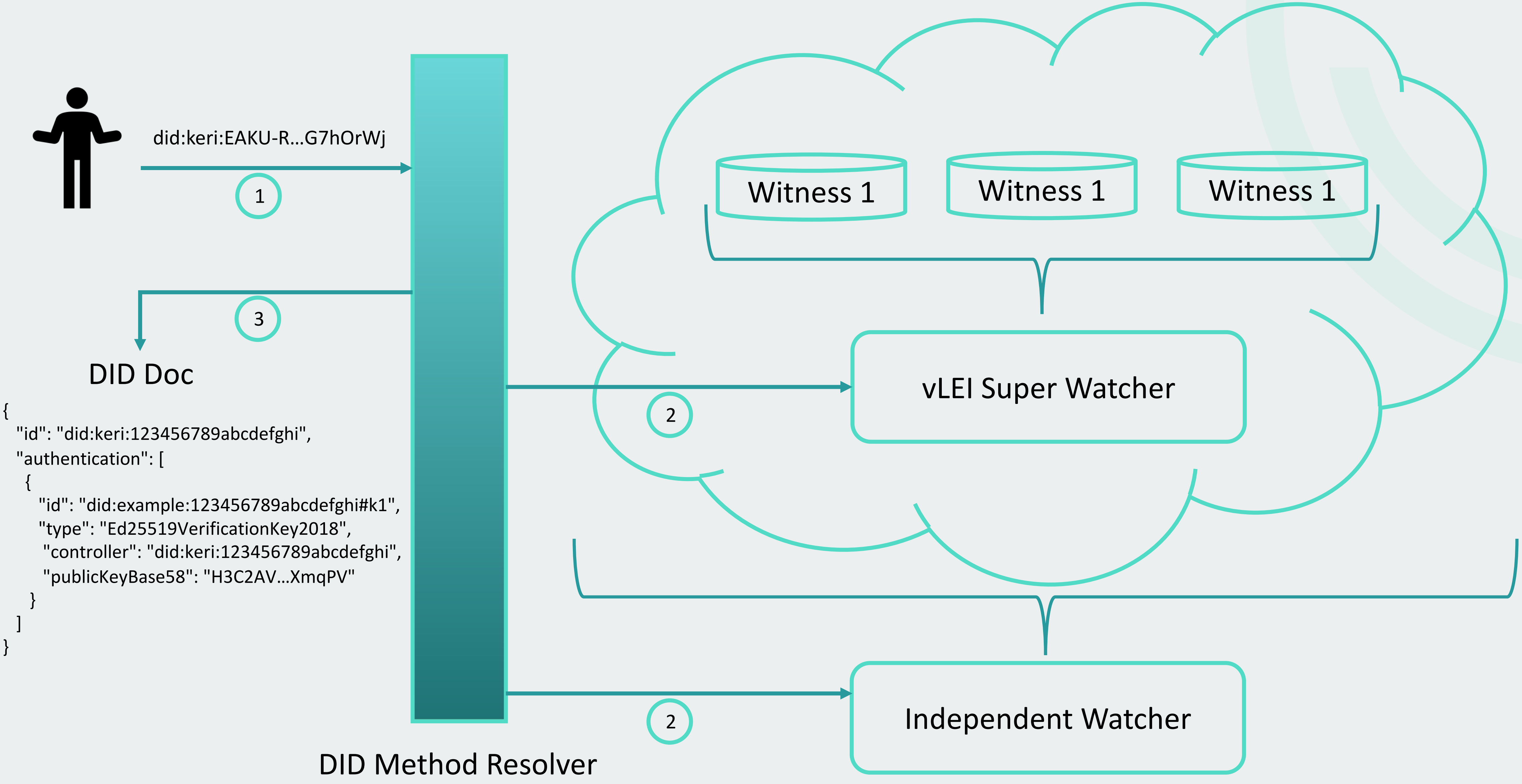


did:keri with Watcher Integration

- Public ecosystem Trust Anchors for well known decentralized discovery
- vLEI for example events published via GLEIF and QVI witnesses
- 2 Options for DID Method Configuration:
  - Launch independent Watcher to monitor ecosystem witnesses
  - Ecosystem “Super Watcher” made available by stewards of ecosystem
    - GLEIF plans for vLEI Super Watcher
- DID Method Resolver polls or receives gossip notifications from Super Watcher
  - DID Method Resolver runs local KERI to end-verify all KEL and TEL information
- DID Namespace Expansion:
  - Additional Super Watchers can be added or discovered
  - Additional DID Resolvers can be added for other ecosystems that can gossip with each other
- DID Resolution Metadata available for non-trusted DID Resolver use

did:keri with Ecosystem Super Watchers

vLEI EcoSystem



```
{
  "id": "did:keri:123456789abcdefghi",
  "authentication": [
   {
     "id": "did:example:123456789abcdefghi#k1",
     "type": "Ed25519VerificationKey2018",
      "controller": "did:keri:123456789abcdefghi",
      "publicKeyBase58": "H3C2AV…XmqPV"
    }
  ]
}
```

Next Steps

Next Steps

- Augment KERI data model for Keys and Endpoint Types (Q1 2023)
- vLEI Public Ecosystem Watchers (Q1 2023)
- Specification with watcher resolver variant (Q1 2023)
- Implementation of watcher resolver variant (Q2 2023)
- Specification and Implementation of Peer-like variants
  - Dependent on community involvement
  - PoC already available for did:keri-lite from RootsID

Limitations

- This presentation contains confidential and proprietary information and/or trade secrets of the Global Legal Entity Identifier Foundation (GLEIF) and/or its affiliates, and is not to be published, reproduced, copied, or disclosed without the express written consent of Global Legal Entity Identifier Foundation.
- Global Legal Entity Identifier Foundation, the Global Legal Entity Identifier Foundation logo are service marks of Global Legal Entity Identifier Foundation.