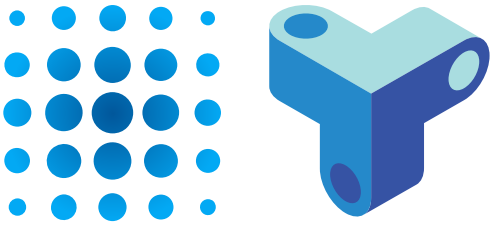
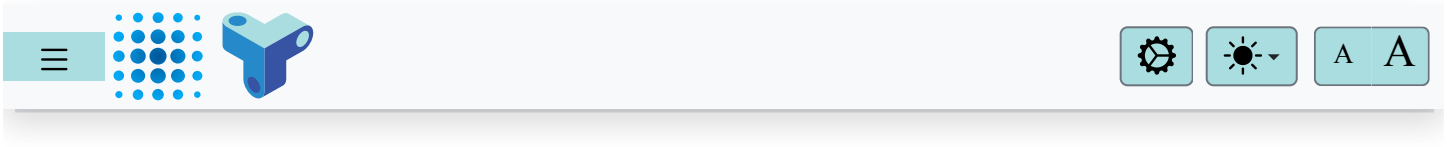


Spec-Up-T KERIsuite Glossary

Create technical specifications in markdown. Based on the original Spec-Up, extended with Terminology tooling

Contents

Powered By Spec-Up-T



– There are 332 terms –

A B C D E F G H I J K L M N O P Q R S T U V W X

0 matches

KERI Suite Glossary

Specification Status: Public Review Draft 01 (PR1)

Latest Draft:

- Github Repository
- Submit/View Issues
- Discussions

Editors:

- Samuel Smith, Gen
- Drummond Reed, Gen
- Henk van Cann

Contributors:

- Kor Dwarshuis

Participate:

- GitHub repo
- Commit history

Status

This is the first public review draft of the KERI Main Glossary. It is also the first version published using the Spec-Up-T specification editing utility based on Spec-Up specification editing utility developed by the Decentralized Identity Foundation.

Copyright Notice

| TBW Sam, please check to what extend you want to copy ToIP's terms |

This specification is subject to the **OWF Contributor License Agreement 1.0 - Copyright** available at https://www.openwebfoundation.org/the-agreements/the-owf-1-0-agreements-granted-claims/owf-contributor-license-agreement-1-0-copyright.

These terms are inherited from the KERI Suite Working Group at the Trust over IP (ToIP) Foundation. Working Group Charter

Terms of Use

These materials are made available under and are subject to the OWF CLA 1.0 - Copyright & Patent license. Any source code is made available under the Apache 2.0 license.

THESE MATERIALS ARE PROVIDED "AS IS." The Trust Over IP Foundation, established as the Joint Development Foundation Projects, LLC, Trust Over IP Foundation Series ("ToIP"), and its members and contributors (each of ToIP, its members and contributors, a "ToIP Party") expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to the materials. The entire risk as to implementing or otherwise using the materials is assumed by the implementer and user.

IN NO EVENT WILL ANY ToIP PARTY BE LIABLE TO ANY OTHER PARTY FOR LOST PROFITS OR ANY FORM OF INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THESE MATERIALS, ANY DELIVERABLE OR THE ToIP GOVERNING AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND

WHETHER OR NOT THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Introduction

The KERI Main Glossary is a deliverable of the ToIP KERI Suite Working Group. Its purpose is to promote shared understanding of terms and concepts across the many different working groups, communities, enterprises, and ecosystems who are collaborating to develop and deploy decentralized digital trust infrastructure.

Contributions and feedback are encouraged from any stakeholder in this area of terminology.

Linking to this Glossary

This glossary is designed to be both human and machine readable. All terms are listed alphabetically; acronyms are listed separately and linked to the fully expanded terms. Document authors can link directly to any term using standard web links and anchors following this syntax:

`https://weboftrust.github.io/kerisuite-glossary#term:xxxxx`

Where `xxxxx` is the term as it appears in the glossary, with any spaces are replaced by en-dashes (hyphens). For example, a link to the term `self-certifying identifer` would be:

`https://weboftrust.github.io/kerisuite-glossary#self-certifiying-identifier`

A specification document written using the Trustoverip's open source Spec-Up-T environment documented in the Spec-Up-T manual, originally based on Decentralized Identity Foundation's open source Spec-Up editor.

The tool may create special external references to terms in this glossary using the Spec-Up `xref` and the `tref` tags following this syntax:

`[ [xref: glossary, xxxxx] ]` and `[ [tref: glossary, xxxxx] ]`

Note: we've put spaces between brackets to be able to present this literally; remove the spaces in use.

Where `glossary` is the text label the document author assigns to the URL of a Web-accessible glossary, and `xxxxx` is the term as it appears in that glossary, with any spaces are replaced by en-dashes (hyphens). For example, a Spec-Up external reference to the term `self-certifying identifer` using the label `toip` for this glossary would look like this:

`[[xref: toip, self-certifying-identifier]]`

An item borrowed from an other glossary might look like this:

`[[xref: vlei, OOR]]`

Referenced Glossaries

These glossaries have been interlinked using `tref` and `xref` tags. We show both test and production environments. The `specs.json` is for proficient users to inspect the production settings.

Interlinked glossary summary

Glossary	TEST repo	Live TEST Glossary	Production repo	Live PRODUCTION Glossary	Specs.json PROD
KERIsuite	HenkvanCann	TEST	WebofTrust	PRODUCTION	Specs.json
vLEI	HenkvanCann				
ToIP **Main**	HenkvanCann	TEST	ToIP	PRODUCTION	Specs.json
ToIP **General IT**	HenkvanCann	TEST	ToIP	PRODUCTION	Specs.json

The following glossaries were used as sources for some of the definitions in the ToIP General Glossary. All source glossaries are cited in the definitions of each term.

Short Name	Source Glossary	URL
Wikipedia	Wikipedia	https://www.wikipedia.org/
eSSIF-Lab	eSSIF-Lab Glossary	https://essif-lab.github.io/framework/docs/essifLab-glossary
NIST-CSRC	NIST Computer Security Resource Center Glossary	https://csrc.nist.gov/glossary/

Short Name	Source Glossary	URL
W3C DID	W3C Decentralized Identifiers (DIDs) 1.0	https://www.w3.org/TR/did-core/#terminology
W3C VC	W3C VC Data Model 1.1	https://www.w3.org/TR/vc-data-model/#terminology

Terms and Definitions

KERI Suite Glossary

Specification Status: Public Review Draft 01 (PR1)

Latest Draft:

- Github Repository
- Submit/View Issues
- Discussions

Editors:

- Samuel Smith, Gen
- Drummond Reed, Gen
- Henk van Cann

Contributors:

- Kor Dwarshuis

Participate:

- GitHub repo
- Commit history

Status

This is the first public review draft of the KERI Main Glossary. It is also the first version published using the Spec-Up-T specification editing utility based on Spec-Up specification editing utility developed by the Decentralized Identity Foundation.

Copyright Notice

| TBW Sam, please check to what extend you want to copy ToIP's terms |

Terms of Use

Introduction

The KERI Main Glossary is a deliverable of the ToIP KERI Suite Working Group. Its purpose is to promote shared understanding of terms and concepts across the many different working groups, communities, enterprises, and ecosystems who are collaborating to develop and deploy decentralized digital trust infrastructure.

Contributions and feedback are encouraged from any stakeholder in this area of terminology.

Linking to this Glossary

This glossary is designed to be both human and machine readable. All terms are listed alphabetically; acronyms are listed separately and linked to the fully expanded terms. Document authors can link directly to any term using standard web links and anchors following this syntax:

`https://weboftrust.github.io/kerisuite-glossary#term:xxxxx`

Where `xxxxx` is the term as it appears in the glossary, with any spaces are replaced by en-dashes (hyphens). For example, a link to the term `self-certifying identifer` would be:

`https://weboftrust.github.io/kerisuite-glossary#self-certifiying-identifier`

A specification document written using the Trustoverip's open source Spec-Up-T environment documented in the Spec-Up-T manual, originally based on Decentralized Identity Foundation's open source Spec-Up editor.

The tool may create special external references to terms in this glossary using the Spec-Up `xref` and the `tref` tags following this syntax:

`[ [xref: glossary, xxxxx] ]` and `[ [tref: glossary, xxxxx] ]`

Note: we've put spaces between brackets to be able to present this literally; remove the spaces in use.

Where `glossary` is the text label the document author assigns to the URL of a Web-accessible glossary, and `xxxxx` is the term as it appears in that glossary, with any spaces are replaced by en-dashes (hyphens). For example, a Spec-Up external reference to the term `self-certifying identifer` using the label `toip` for this glossary would look like this:

`[[xref: toip, self-certifying-identifier]]`

An item borrowed from an other glossary might look like this:

`[[xref: vlei, OOR]]`

Referenced Glossaries

These glossaries have been interlinked using `tref` and `xref` tags. We show both test and production environments. The `specs.json` is for proficient users to inspect the production settings.

Interlinked glossary summary

Glossary	TEST repo	Live TEST Glossary	Production repo	Live PRODUCTION Glossary	Specs.json PROD
KERIsuite	HenkvanCann	TEST	WebofTrust	PRODUCTION	Specs.json
vLEI	HenkvanCann				
ToIP **Main**	HenkvanCann	TEST	ToIP	PRODUCTION	Specs.json
ToIP **General IT**	HenkvanCann	TEST	ToIP	PRODUCTION	Specs.json

The following glossaries were used as sources for some of the definitions in the ToIP General Glossary. All source glossaries are cited in the definitions of each term.

Short Name	Source Glossary	URL
Wikipedia	Wikipedia	https://www.wikipedia.org/
eSSIF-Lab	eSSIF-Lab Glossary	https://essif-lab.github.io/framework/docs/essifLab-glossary
NIST-CSRC	NIST Computer Security Resource Center Glossary	https://csrc.nist.gov/glossary/
W3C DID	W3C Decentralized Identifiers (DIDs) 1.0	https://www.w3.org/TR/did-core/#terminology
W3C VC	W3C VC Data Model 1.1	https://www.w3.org/TR/vc-data-model/#terminology

Terms and Definitions

abandoned-identifier

An AID is abandoned when either the inception-event or a subsequent rotation-event rotates to an empty next key digest list (which means the next threshold must also be 0).

access-controlled-interaction

Access controlled actions like submitting a report. If you already have that report then load balancer needs a mechanism to drop repeated requests.

ACDC

authentic-chained-data-container

ADC

authentic-data-container

AID

autonomic-identifier

ambient-verifiability

Verifiable by anyone, anywhere, at anytime. Although this seems a general term, it was first used in the context of KERI by Sam Smith.

ample

The minimum required number of participants in an event to have a supermajority so that one and only one agreement or consensus on an event may be reached. This is a critical part of the KAACE agreement algorithm (consensus) in KERI for establishing consensus between witnesses on the key state of a KERI identifier.

APC

authentic-provenance-chain

authentic-chained-data-container

a directed acyclic graph with properties to provide a verifiable chain of proof-of-authorship. See the full specification

authentic-data-container

A mechanism for conveying data that allows the authenticity of its content to be proved.

authentic-provenance-chain

Interlinked presentation-exchange of evidence that allow data to be tracked back to its origin in an objectively verifiable way.

authoritative

Established control authority over an identifier, that has received attestations to it, e.g. control over the identifier has been verified to its root-of-trust. So the (control over the) identifier is 'authoritative' because it can be considered accurate, renowned, honourable and / or respected.

authorized-vlei-representative

Also 'AVR'. This a representative of a Legal Entity that are authorized by the DAR of a Legal Entity to request issuance and revocation of:

autonomic-identifier

a self-managing cryptonymous identifier that must be self-certifying (self-authenticating) and must be encoded in CESR as a qualified Cryptographic primitive.

autonomic-trust-basis

When we use an AID as the root-of-trust we form a so-called *autonomic trust basis*. This is diagrammed as follows:

AVR

authorized-vlei-representative

backer

an alternative to a traditional KERI based Witness commonly using Distributed Ledger Technology (DLT) to store the KEL for an identifier.

BADA

best-available-data-acceptance-mechanism

base-media-type

`credential` plus `ld` plus `json`.

bespoke-credential

It's an issuance-event of the disclosure or presentation of other ACDCs. *Bespoke* means *Custom* or *tailor made*.

best-available-data-acceptance-mechanism

The BADA security model provides a degree of replay-attack protection. The attributate originator (issuer, author, source) is provided by an attached signature couple or quadruple. A single reply could have multiple originators. When used as an authorization the reply attributes may include the identifier of the authorizer and the logic for processing the associated route may require a matching attachment.

bexter

The class variable length text that is used in CESR and preserves the round-trip transposability using Base64 URL safe-only encoding even though the text variable length.

bis

bis = backed vc issue, registry-backed transaction event log credential issuance

bivalent

A nested set of layered delegations in a delegation tree, wraps each layer with compromise recovery protection of the next higher layer. This maintains the security of the root layer for compromise recovery all the way out to the leaves in spite of the leaves using less secure key management methods.

blind-oobi

A blind OOBI means that you have some mechanisms in place for verifying the AID instead of via the OOBI itself. A blind OOBI is essentially a URL. It's called "blind" because the witness is not in the OOBI itself. You haves other ways of verifying the AID supplied.

blinded-revocation-registry

The current state of a transaction-event-log (TEL) **may be hidden or blinded** such that *the only way* for a potential verifier of the state to observe that state is *when the controller of a designated AID discloses it* at the time of presentation.

bran

A cryptographic string used as a primary input, a seed, for creating key material for and autonomic-identifier.

brv

brv = backed vc revoke, registry-backed transaction event log credential revocation

cesr-proof-signatures

CESR Proof Signatures is an extension to the Composable Event Streaming Representation [CESR] that provides transposable cryptographic signature attachments on self-addressing data SAD. Any SAD, such as an Authentic Chained Data Container (ACDC) Verifiable Credential [ACDC], for example, may be signed with a CESR Proof Signature and streamed along with any other CESR content. In addition, a signed SAD can be embedded inside another SAD, and the CESR proof signature attachment can be transposed across envelope boundaries and streamed without losing any cryptographic integrity.

CESR-version

the CESR Version is provided by a special Count Code that specifies the Version of all the CESR code tables in a given Stream or Stream section.

CESR

composable-event-streaming-representation

cesride

is concerned with parsing CESR primitives.

chain-link-confidential-disclosure

contractual restrictions and liability imposed on a recipient of a disclosed ACDC that contractually link the obligations to protect the disclosure of the information contained within the ACDC to all subsequent recipients as the information moves downstream. The Chain-link Confidential Disclosure provides a mechanism for protecting against un-permissioned exploitation of the data disclosed via an ACDC.

chain-link-confidentiality

Chains together a sequence of disclosee which may also include a set of constraints on data usage by both second and third parties expressed in legal language such that the constraints apply to all recipients of the disclosed data thus the phrase “chain link” confidentiality. Each Disclosee in the sequence in turn is the discloser to the next Disclosee.

cigar

An ***un***indexed-signature.

CLC

chain-link-confidentiality

code-table-selector

the first character in the text code of composable-event-streaming-representation that determines which code-table to use, either a default code table or a code table selector character when not the default code table. Thus the 1 character text code table must do double duty. It must provide selectors for the different text code tables and also provide type codes for the most popular primitives that have a pad size of 1 that appear is the default code table.

cold-start-stream-parsing

After a reboot (or cold start), a stream processor looks for framing information to know how to parse groups of elements in the stream.

compact-disclosure

a disclosure of an ACDC that discloses only the SAID(s) of some or all of its field maps. Both Partial and Selective Disclosure rely on Compact Disclosure.

compact-variant

Either a most-compact version of an ACDC or the fully-compact version of an ACDC. An issuer commitment via a signature to any variant of ACDC (compact, full, etc) makes a cryptographic commitment to the top-level section fields shared by all variants of that ACDC because the value of a top-level-section is either the SAD or the SAID of the SAD of the associated section.

composability

short for text-binary concatenation composability. An encoding has Composability when any set of Self-Framing concatenated Primitives expressed in either the Text domain or Binary domain may be converted as a group to the other Domain and back again without loss.

composable-event-streaming-representation

Also called 'CESR'. This compact encoding scheme fully supports both textual and binary streaming applications of attached crypto material of all types. This approach includes composability in both the textual and binary streaming domains. The primitive may be the minimum possible but still composable size.

composable

composability

configuration-traits

a list of specially defined strings representing a configuration of a KEL. See #configuration-traits-field.

contingent-disclosure

Contingent disclosure is a privacy-preserving mechanism where only specific information or attributes are disclosed under defined conditions. It enables the selective sharing of data

such that only the required information is revealed to a relying party, without exposing other unrelated or sensitive details. chain-link-confidentiality is a form of contingent disclosure.

contractually-protected-disclosure

a discloser of an ACDC that leverages a Graduated Disclosure so that contractual protections can be put into place to minimize the leakage of information that can be correlated. A Contractually Protected Disclosure partially or selectively reveals the information contained within the ACDC in the initial interaction with the recipient and discloses further information only after the recipient agrees to the terms established by the discloser. More information may be progressively revealed as the recipient agrees to additional terms.

controller

an entity that can cryptographically prove the control authority over an AID and make changes on the associated KEL. A controller of a multi-sig AID may consist of multiple controlling entities.

cooperative-delegation

The way KERI addresses the security-cost-performance-architecture-trade-off is via delegation of identifier prefixes. Delegation includes a delegator and a delegate. For this reason we may call this a cooperative delegation. This is a somewhat **novel form of delegation**.

correlation

In our scope this is an identifier used to indicate that external parties have observed how wallet contents are related.

count-code

group-framing-code

credential

Evidence of authority, status, rights, entitlement to privileges, or the like.

current-threshold

represents the number or fractional weights of signatures from the given set of current keys required to be attached to a Message for the Message to be considered fully signed.

custodial-agent

An agent owned by an individual who has granted signing-authority to a custodian who is usually also the host of the running agent software. Using partial-rotation to facilitate custodial key management the owner of the identifier retains rotation-authority and thus the ability to “fire” the custodian at any time without requiring the cooperation of the custodian.

custodial-rotation

Rotation is based on control authority that is split between two key sets. The first for signing authority and the second (pre-rotated) for rotation authority, the associated thresholds and key list can be structured so that a designated custodial agent can hold signing authority, while the original controller can hold exclusive rotation authority.

dead-attack

an attack on an establishment-event that occurs after the Key-state for that event has become stale because a later establishment event has rotated the sets of signing and pre-rotated keys to new sets.

decentralized-identity

`KERI`s definition of decentralization (centralization) is about *control* not *spatial distribution*. In our definition *decentralized* is not necessarily the same as *distributed*. By distributed we mean that activity happens at more than one site. Thus decentralization is about *control* and distribution is about *place*. To elaborate, when we refer to decentralized infrastructure we mean infrastructure under decentralized (centralized) control no matter its spatial distribution. Thus *decentralized infrastructure* is infrastructure sourced or controlled by more than one `entity`.

DEL

duplicitous-event-log

delegated-identifier

Matches the act of delegation with the appropriate digital twin. Consequently when applied recursively, delegation may be used to compose arbitrarily complex trees of hierarchical (delegative) key management event streams. This is a most powerful capability that may provide an essential building block for a generic universal decentralized key management infrastructure (DKMI) that is also compatible with the demand of generic event streaming applications.

derivation-code

To properly extract and use the public-key-infrastructure embedded in a self-certifying-identifier we need to know the cryptographic *signing scheme* used by the key-pair. KERI includes this very compactly in the identifier, by replacing the pad character (a character used to fill a void to able to always end up with a fixed length public key) with a special character that encodes the derivation process. We call this the *derivation code*.

designated-aliases

An AID controller can designate aliases which are AID controlled identifiers such as a did:keri, did:webs, etc. The AID controller issues a designated aliases attestation (no issuee) that lists the identifiers and manages the status through a registry anchored to their KEL. See the designated aliases docs

designated-authorized-representative

Also 'DAR'. These are representatives of a Legal Entity that are authorized by the Legal Entity to act officially on behalf of the Legal Entity. DARs can authorize:

diger

A *primitive* that represents a digest. It has the ability to verify that an input hashes to its raw value.

dip

dip = delcept, delegated inception

direct-mode

Two primary trust modalities motivated the KERI design, One of these is the *direct* (one-to-one) mode, in which the identity controller establishes control via verified signatures of the

controlling key-pair. The direct mode doesn't use witnesses nor key-event-receipt-logs, but has direct (albeit intermittent) network contact with the validator.

disclosee

a role of an entity that is a recipient to which an ACDC is disclosed. A Disclosee may or may not be the Issuee of the disclosed ACDC.

discloser

a role of an entity that discloses an authentic-chained-data-container. A Discloser may or may not be the Issuer of the disclosed ACDC.

dnd

Do Not Delegate is a flag/attribute for an AID, and this is default set to "you can delegate."

domain

a representation of a primitive either Text (T), Binary (B) or Raw binary ®.

drt

drt = deltate, delegated rotation

dual-indexed-codes

a context-specific coding scheme, for the common use case of thresholded multi-signature schemes in CESR.

dual-text-binary-encoding-format

An encoding format that allows for both text and binary encoding format, which is fully interchangeable. The composability property enables the round trip conversion en-masse of concatenated primitives between the text domain and binary domain while maintaining the separability of individual primitives.

duplicitous-event-log

This is a record of inconsistent event messages produced by a given controller or witness with respect to a given key-event-receipt-log. The duplicitous events are indexed to the corresponding event in a KERL.

duplicity-detection

A mechanism to detect duplicity in cryptographically secured event logs.

duplicity

the existence of more than one version of a Verifiable key-event-log for a given AID.

ECR

engagement-context-role

edge

a top-level field map within an ACDC that provides edges that connect to other ACDCs, forming a labeled property graph (LPG).

end-role

An end role is an authorization for one AID to serve in a role for another AID.

engagement-context-role

A person that represents the legal-entity in a functional or in another context role and is issued an ECR vlei-credential.

escrow-state

The current state of all the temporary storage locations (what events are waiting for what other information) that KERI protocol needs to keep track of, due to its fully asynchronous nature.

establishment-event

a key-event that establishes or changes the key state which includes the current set of authoritative keypairs (key state) for an AID.

exn

exn = exchange

exp

exp = expose, sealed data exposition

field-map

A traditional `key:value` pair renamed to avoid confusing with the cryptographic use of the term 'key'.

first-seen

refers to the first instance of a message received by any witness or watcher. The first-seen event is always seen, and can never be unseen. It forms the basis for duplicity detection in KERI-based systems.

frame-code

framing-code

framing-code

a code that delineates a number of characters or bytes, as appropriate, that can be extracted atomically from a stream.

full-disclosure

a disclosure of an ACDC that discloses the full details of some or all of its field maps. In the context of selective-disclosure, Full Disclosure means detailed disclosure of the selectively disclosed attributes, not the detailed disclosure of all selectively disclosable attributes. In the context of partial-disclosure, Full Disclosure means detailed disclosure of the field map that was so far only partially disclosed.

fully-compact

The most compact form of an ACDC. This is the only signed variant of an ACDC and this signature is anchored in a transaction-event-log (TEL) for the ACDC.

fully-expanded

The most user-friendly version of an ACDC credential. It doesn't need to be signed and typically is not signed since the most compact version which is signed can be computed from this form and then the signature can be looked up in the TEL of the ACDC in question.

GAR

gleif-authorized-representative

ghost-credential

Is a valid credential within in a 90 days grace period (the revocation transaction time frame before it's booked to revocation registry).

gleif-authorized-representative

A representative of GLEIF authorized to perform the identity verifications requirements needed to issue the QVI vLEI Credential.

GLEIS

Global Legal Entity Identifier System

graduated-disclosure

a disclosure of an ACDC that does not reveal its entire content in the initial interaction with the recipient and, instead, partially or selectively reveals only the information contained within the ACDC necessary to further a transaction with the recipient. A Graduated disclosure may involve multiple steps where more information is progressively revealed as the recipient satisfies the conditions set by the discloser. compact-disclosure, partial-disclosure, selective-disclosure, and full-disclosure are all Graduated disclosure mechanisms.

graph-fragment

An ACDC is a verifiable data structure and *part of a graph*, consisting of a node property and one or two edge proporties.

group-code

group-framing-code

group-framing-code

special Framing Codes that can be specified to support groups of Primitives which make them pipelinable. Self-framing grouping using Count Codes is one of the primary advantages of composable encoding.

hab

A Hab is a keystore for one identifier. The Python implementation in keripy, also used by keria uses LMDB to store key material and all other data.

habery

'Hab' comes from 'Habitat'. It's a place where multi-sigs and AIDs are linked. Habery manages a collection of hab. A Hab is a data structure (a Python object).

hierarchical-composition

Encoding protocol that is composable in a hierarchy and enables pipelining (multiplexing and de-multiplexing) of complex streams in either text or compact binary. This allows management at scale for high-bandwidth applications.

icp

icp = incept, inception

inception-event

an establishment-event that provides the incepting information needed to derive an AID and establish its initial Key state.

inception

The operation of creating an AID by binding it to the initial set of authoritative keypairs and any other associated information. This operation is made verifiable and duplicity evident upon acceptance as the inception event that begins the AID's KEL.

indexed-signature

Also called *siger*. An indexed signature attachment is used when signing anything with a multi-key autonomic identifier. The index is included as part of the attachment, so a verifier knows which of the multiple public keys was used to generate a specific signature.

indirect-mode

Two primary trust modalities motivated the KERI design, One of these is the *indirect* (one-to-many) mode, which depends on witnessed key event receipt logs (KERL) as a secondary root-of-trust for validating events. This gives rise to the acronym KERI for key event receipt infrastructure.

inquisitor

In the ACDC context it's a general term for someone (in a validating role) that launches an inquiry at some KERI witness.

integrity

~In KERI's "security first" approach Authenticity includes *technical integrity* of data involved. This includes:

interaction-event

Non-establishment Event that anchors external data to the key-state as established by the most recent prior establishment event.

interactive-authentication-design

A group of approaches having an interactive mechanism that requires a set of requests and responses or challenge responses with challenge response replies for secure authentication.

interceptor

a keria class that allows to push events that are happening inside the cloud agent to other backend processes.

interleaved-serialization

Serializations of different types interleaved in an overarching format

IPEX

issuance-and-presentation-exchange-protocol

iss

iss = vc issue, verifiable credential issuance

issuance-and-presentation-exchange-protocol

provides a uniform mechanism for the issuance and presentation of ACDCs in a securely attributable manner.

issuance-event

The initial transaction event log event anchored to the issuing AID's key event log that represents the issuance of an ACDC credential.

issuance-exchange

A special case of a presentation-exchange where the discloser is the issuer of the origin (Primary) ACDC of the directed-acyclic-graph formed by the set of chained authentic-chained-data-containers so disclosed.

issuee

a role of an entity to which the claims of an ACDC are asserted.

issuer

a role of an entity that asserts claims and creates an ACDC from these claims.

ixn

JSON field name (attribute) for Interaction Event; its content (value) contains a hash pointer. All transaction-event-log events are anchored in a key-event-log in either ixn (interaction-event) or rot (rotation-events). This is the foundation enabling a verifiable credential protocol to be built on top of KERI.

judge

A judge is an entity or component that examines the entries of one or more key-event-receipt-log and DELs of a given identifier to validate that the event history is from a non-duplicity controller and has been witnessed by a sufficient number of non-duplicitous witness such that it may be trusted or conversely not-trusted by a validator.

juror

A juror has the basic task of performing duplicity detection on events and event receipts.

jury

The jury is the set of entities or components acting as juror.

KA2CE

keri-agreement-algorithm-for-control-establishment

KAACE

keri-agreement-algorithm-for-control-establishment

KAPI

Application programmer interfaces (APIs) for the various components in the KERI ecosystem such as Controllers, Agents, Witnesses, Watchers, Registrars etc need by which they can share information. The unique properties of the KERI protocol require APIs that preserve those properties. We call the set of APIs the KERI API.

KAWA

keri's-algorithm-for-witness-agreement

keep

Is KERI's and ACDC's user interface that uses the keripy agent for its backend. It uses the REST API exposed from the keripy agent.

KEL

A Key Event Log.

keri-agreement-algorithm-for-control-establishment

Agreement on an event in a key event log KEL means each witness has observed the exact version of the event and each witness' receipt has been received by every other witness.

keri-command-line-interface

Command line tool used to create identifiers, manage keys, query for KELs and participate in delegated identifiers or multi-signature group identifiers. It also includes operations for running witnesses, watchers and cloud agents to establish a cloud presence for any identifier.

keri-event-stream

A stream of verifiable KERI data, consisting of the key-event-log and other data such as a transaction-event-log. This data is a CESR event stream (TODO: link to IANA application/cesr media type) and may be serialized in a file using composable-event-streaming-representation encoding. We refer to these *CESR stream resources* as KERI event streams to simplify the vocabulary.

keri-improvement-doc

These docs are modular so teams of contributors can independently work and create PRs of individual KIDs; KIDs answer the question "how we do it". We add commentary to the indivudual KIDs that elaborate on the why. It has been split from the how to not bother implementors with the why.

keri-ox

The RUST programming-language implementation of the KERI protocol.

keri-request-authentication-method

All requests from a web client must use KRAM (KERI Request Authentication Method) for replay attack protection. The method is essentially based on each request body needing to include a date time string field in ISO-8601 format that must be within an acceptable time window relative to the server's date time. See the KRAM Github repo

keri-suite-search-engine

KERISSE is the Docusaurus self-education site of Web-of-Trust GitHub repo with Typesense search facilities. Because of its focus on well-versed developers in the field of SSI and the support of their journey to understand the structure of the code and how things work in the keri-suite it's more a search engine that drills down on documentation.

keri-suite

The *KERI suite* is the set of inter-related developments (KERI, ACDC, OOBI, CESR, IPEX, etc) under the Web-of -Trust user on Github

KERI

key-event-receipt-infrastructure

keri's-algorithm-for-witness-agreement

a type of Byzantine Fault Tolerant (byzantine-fault-tolerance) algorithm.

KERIA-agent

An agent in keria terms, is an instance of a keystore (hab) that runs in a given instance of the KERIA agent server.

KERIA

KERI Agent in the cloud. The KERIA service will expose 3 separate HTTP endpoints on 3 separate network interfaces.

keride

is a *Rust* programming language library for key-event-receipt-infrastructure. Among its features

keridemlia

It is a contraction of key-event-receipt-infrastructure and Kademlia. It's the distributed database of Witness IP-addresses based on a distributed-hash-table. It also does the CNAME - stuff that domain-name Services (DNS) offers for KERI: the mapping between an identifier and it's controller AID stored in the KEL to its current wittness AID and the wittness AID to the IP address.

kerific

kerific is a front plugin or extension that currently only works for Chrome and Brave. It matches words in any text on the web that is parseable for kerific and offers buttons to various glossaries and definitions in the self-sovereign-identity field.

KERIMask

A wallet similar to *MetaMask*, the manifestation will be a browser extension and it will connect to KERIA servers in order for a person to control AIDs from their browser.

keripy

The Python programming-language implementation of the KERI protocol.

KERISSE

keri-suite-search-engine

KERL

key-event-receipt-log

kever

Kever is a key event verifier.

key-event-log

a Verifiable data structure that is a backward and forward chained, signed, append-only log of key events for an AID. The first entry in a KEL must be the one and only Inception event of that AID.

key-event-message

Message whose body is a key event and whose attachments may include signatures on its body.

key-event-receipt-infrastructure

or the KERI protocol, is an identity system-based secure overlay for the Internet.

key-event-receipt-log

a key event receipt log is a kel that also includes all the consistent key event receipt messages created by the associated set of witnesses. See annex key-event-receipt-log.

key-event-receipt

message whose body references a Key event and whose attachments must include one or more signatures on that Key event.

key-event

See the more general TrustoverIP concept of key-event: key-event

KID

keri-improvement-doc

kli

keri-command-line-interface

KRAM

keri-request-authentication-method

ksn

ksn = state, key state notice

ledger-backer

A witness in KERI that is ledger-registered. It's a type of backer that proof its authenticity by a signing key anchored to the public key of a data item on a (public) blockchain.

legal-entity-engagement-context-role-vlei-credential-governance-framework

A document that details the requirements for vlei-role-credential **issued to** representatives of a Legal Entity *in other than official roles* but in functional or other context of engagement.

legal-entity-official-organizational-role-vlei-credential-governance-framework

A document that details the requirements for vlei-role-credential **issued to** official representatives of a Legal Entity.

legal-entity-vlei-credential-governance-framework

A *document* that details the requirements for vLEI Credential **issued by** a qualified-vlei-issuer to a legal-entity.

listed-identifier

Is a list in an authentic-chained-data-container of authorised did:webs identifier + method; the list appears in the metadata of the did:webs DID-doc.

live-attack

an attack that compromises either the current signing keys used to sign non-establishment events or the current pre-rotated keys needed to sign a subsequent establishment event. See (Security Properties of Prerotation)[#live-attacks].

locked-state

The default status a KERI data store is in once it has been created using a passcode; it is by default encrypted.

management-TEL

management-transaction-event-log

management-transaction-event-log

A 'management transaction-event-log' will signal the creation of the *Virtual Credential Registry VCR* and track the list of *Registrars* that will act as *backer* for the individual _ transaction event logs (TELs)_ for each virtual-credential (VC).

moobi

Multi OOBI would allow to share a bunch of different end-points (oobis) all at once. A way for a single store to share multiple endpoints for that store.

most-compact

An ACDC that, for a given level of disclosure, is as compact as it can be, which means

multi-valent

A delegator may have multiple delegate, thereby enabling elastic horizontal scalability. Multiple delegates from a single delegator. Furthermore, each delegate may act as a delegator for its own delegates to form a *nested delegation tree*.

naive-conversion

Non-CESR Base64 conversion. How people are used to using the Base64 encode and decode. Without pre-padding etc all the stuff CESR does to ensure aligns on 24 bit boundaries so CESR never uses the '=' pad character. But naive base64 will pad if the length is not 24 bit aligned.

ndigs

Digests of public keys, not keys themselves. The reason to use ndigs is to prove control over public keys or to hide keys. It's used in Keripy and consists of a list of qualified base64

digests of public rotation key derivations.

nested-cooperative-delegated-identifiers

In KERI delegations are cooperative, this means that both the delegator and delegate must contribute to a delegation. The delegator creates a cryptographic commitment in either a rotation or interaction event via a seal in a delegated establishment event. The delegate creates a cryptographic commitment in its establishment event via a seal to the delegating event.

next-threshold

represents the number or fractional weights of signatures from the given set of next keys required to be attached to a Message for the Message to be considered fully signed.

non-establishment-event

a Key event that does not change the current Key state for an AID. Typically, the purpose of a Non-establishment event is to anchor external data to a given Key state as established by the most recent prior Establishment event for an AID.

non-interactive-authentication-design

A group of approaches having non-interactive mechanisms that pose unique problems because they do not allow a challenge response reply handshake. A request is submitted that is self-authenticating without additional interaction.

official-organizational-role

Also 'OOR'. A person that represents the Legal Entity in an official organizational role and is issued an OOR vLEI Credential.

OOBI

out-of-band-introduction

opcode

Opcodes are meant to provide stream processing instructions that are more general and flexible than simply concatenated primitives or groups of primitives.

operator

an optional field map in the Edge section that enables expression of the edge logic on edge subgraph as either a unary operator on the edge itself or an m-ary operator on the edge group.

out-of-band-introduction

Out-of-band Introductions (OOBIs) are discovery and validation of IP resources for key-event-receipt-infrastructure autonomic identifiers. **Discovery via URI, trust via KERI.**

parside

is a bunch of generators. Responsible for pulling out a stream of bits from a CESR stream and parse it.

partial-disclosure

a disclosure of an ACDC that partially discloses its field maps using Compact Disclosure. The Compact Disclosure provides a cryptographically equivalent commitment to the yet-to-be-disclosed content, and the later exchange of the uncompacted content is verifiable to an earlier Partial Disclosure. Unlike Selective disclosure, a partially disclosable field becomes correlatable to its encompassing block after its Full Disclosure.

partial-pre-rotation

partial-rotation

partial-rotation

The pre-rotation mechanism supports partial pre-rotation or **more exactly partial rotation of pre-rotated keypairs**. It's a rotation operation on a set of pre-rotated keys that may keep some keys in reserve (i.e unexposed) while exposing others as needed.

pathing

It was designed to sign portions of a credential aimed at complex cases like

percolated-discovery

a discovery mechanism for information associated with an AID or a SAID, which is based on Invasion Percolation Theory. Once an entity has discovered such information, it may in turn share what it discovers with other entities. Since the information so discovered is end-verifiable, the percolation mechanism and percolating intermediaries do not need to be trusted.

percolated-information-discovery

In the OOBI protocol, a discovery mechanism for the KERI and the ACDC protocols is provided by a bootstrap that enables Percolated Information Discovery (PID), which is based on Invasion Percolation Theory.

PID

percolated-information-discovery

pre-rotation

Cryptographic commitment to next rotated key set in previous rotation or inception-event.

prefix

A prefix that is composed of a basic Base-64 (URL safe) derivation code pre-pended to Base-64 encoding of a basic public digital signing key.

presentation-exchange

An exchange that provides disclosure of one or more authentic-chained-data-containers between a Discloser and a Disclosee.

primary-root-of-trust

In KERI a root-of-trust that is cryptographically verifiable all the way to its current controlling key pair in a PKI.

proem

A “proem” is an introductory statement, preamble, or preface. It sets the stage for the content that follows, often providing context, framing the discussion, or outlining the

purpose and scope of the material.

promiscuous-mode

It is the mode a watcher runs in. A watcher uses the same code as a witness. However a watcher does so “lacking standards of selection; acting without careful judgment; indiscriminate”. Or “Showing little forethought or critical judgment; casual.”

proof-of-authorship

Proof that somebody or something has originally created certain content. It’s about *data*’s inception. Whereas proof-of-authority is about *rights* attached to this data.

provenanced

The act of verifying authenticity or quality of documented history or origin of something.

PTEL

public-transaction-event-log

public-transaction-event-log

is a public hash-linked data structure of transactions that can be used to track state anchored to a key-event-log.

public-verifiable-credential-registry

is a form of a Verifiable Data Registry that tracks the issuance/revocation state of credentials issued by the controller of the key-event-log. Two types of TELs will be used for this purpose: management-transaction-event-log and virtual-credential-transaction-event-log.

qry

qry = query

quadlet

a group of 4 characters in the T domain and equivalently in triplets of 3 bytes each in the B domain used to define variable size.

qualified-vlei-issuer-vlei-credential-governance-framework

A *document* that details the requirements to enable this Credential to be **issued by** GLEIF **to** qualified-vlei-issuer which allows the Qualified vLEI Issuers to issue, verify and revoke legal-entity-vlei-credential-governance-framework, legal-entity-official-organizational-role-vlei-credential-governance-framework, and legal-entity-engagement-context-role-vlei-credential-governance-framework.

qualified-vlei-issuer

The contracting party to the vLEI Issuer Qualification Agreement that has been qualified by GLEIF as a Qualified vLEI Issuer.

qualified

When qualified, a cryptographic primitive includes a prepended derivation code (as a proem), that indicates the cryptographic algorithm or suite used for that derivation.

qvi-authorized-representative

A designated representative of a QVI authorized, to conduct QVI operations with GLEIF and legal-entity. Also referring to a person in the role of a QAR.

rct

rct = receipt

read-update-nullify

Read, update, nullify are a set of actions you (or a server) can take on data. “Read” means to view it, “update” means to change it, and “nullify” means to invalidate it, but not “Delete” it. Mind you, there’s also no “Create”.

receipt-log

ordered record of all key event receipts for a given set of witnesses.

receipt

event message or reference with one or more witness signatures.

reconciliation

Reconciliation is the process in which you decide to accept a fork of the key-event-log or not.

redundant-credential

Multiple credentials issued by the same issuer (e.g. a QVI). They do not have anything to do with each other. They are independently valid.

registrar

identifiers that serve as backers for each transaction-event-log (TEL) under its provenance. This list of Registrars can be rotated with events specific to a certain type of TEL. In this way, a Registrar is analogous to a Backer in KERI KELs and Registrar lists are analogous to Backer lists in KERI KELs.

registration-interaction

Setup/Registration interaction, new AID and authorization to establish access control. You present a (vLEI) credential. You don't want that captured and misused. Narrowing the scope to a certain role (e.g. Document Submitter) is a pre-registration via delegation authority.

reputation

Consistent behaviour over time on the basis of which anyone else makes near-future decisions.

reserve-rotation

One important use case for partial-rotation is to enable pre-rotated key pairs designated in one establishment-event **to be held in reserve and not exposed** at the next (immediately subsequent) establishment event.

rev

rev = vc revoke, verifiable credential revocation

revocation-event

An event that revokes control-authority over an identifier. From that point in time the authoritative key-pairs at hand are not valid anymore.

RID

root-autonomic-identifier

root-autonomic-identifier

An entity may provide the root-of-trust for some ecosystem (with delegation)via its root AID. Let's call this the *RID* for "root AID". The RID must be protected using the highest level of security in its key-management.

rot

JSON field name (attribute) for Rotation Event; its content (value) contains a hash pointer. All transaction-event-log events are anchored in a key-event-log in either ixn (interaction-event) or rot (rotation-events). This is the foundation enabling a verifiable credential protocol to be built on top of KERI.

rotation-authority

The (exclusive) right to rotate the authoritative key pair and establish changed control authority.

rotation-event

an Establishment Event that provides the information needed to change the Key state, which includes a change to the set of authoritative keypairs for an AID.

rotation

The operation of revoking and replacing the set of authoritative key-pair for an AID. This operation is made verifiable and duplicity evident upon acceptance as a rotation event that is appended to the AID's KEL.

rpy

rpy = reply

rules

a top-level field map within an ACDC that provides a legal language as a Ricardian Contract, which is both human and machine-readable and referenceable by a cryptographic digest.

run-off-the-crud

RUN off the CRUD is an alternative to the traditional CRUD approach to defining basic operations on resources in data management systems (e.g., databases, APIs). RUN stands for Read, Update, Nullify and bears a nuanced approach to deletion.

RUN

The acronym for the new peer-to-peer end-verifiable monotonic update policy is RUN (**Read, Update, Nullify**).

SAD

self-addressing-data

SAID

self-addressing-identifier

sally

is an implementation of a verification service and acting as a reporting server. It is purpose-built software for the vLEI ecosystem to allow participants in the vLEI ecosystem present credentials, so the GLEIF Reporting API can show what vLEI are; issued to legal-entity.

salter

A primitive that represents a seed. It has the ability to generate new signers.

salty-nonce-blinding-factor

For ease of sharing a secret and hiding information with this secret of Blindable State TELs we use a Salty Nonce Blinding Factor. You'd like to hide the state of certain credentials to some verifiers in the future, while keeping the state verifiable for others.

schema

the said of a JSON schema that is used to issue and verify an ACDC.

SCID

self-certifying-identifier

secondary-root-of-trust

In KERI its a root-of-trust that, for its secure attribution, depends on another verifiable data structure (VDS) which MUST be a primary-root-of-trust.

secure-asset-transfer-protocol

An IETF protocol (and working group) in the making (as of mid 2022) for moving assets between blockchains.

secure-private-authentic-confidentiality

ToIP Trust Spanning Layer Group realized we do have a secure authentication layer (KERI) but we don't have a secure confidentiality and privacy mechanism. Sam Smith proposes SPAC paper to define this.

security-cost-performance-architecture-trade-off

The degree of protection offered by a key management infrastructure usually forces a trade-off between security, cost, and performance.

security

'secure' is free from or not exposed to danger or harm; safe. For identifiers *security* typically means secure from *exploit* or *compromise*. More specifically an identifier is secure with respect to an entity if there is a mechanism by which that entity may prove it has controller over the identifier.

selective-disclosure

a disclosure of an ACDC that selectively discloses its attributes using Compact Disclosure. The set of selectively disclosable attributes is provided as an array of blinded blocks where each attribute in the set has its own dedicated blinded block. Unlike Partial Disclosure, the selectively disclosed fields are not correlatable to the so far undisclosed but selectively disclosable fields in the same encompassing block.

self-addressed-data

a representation of data content from which a SAID is derived. The SAID is both cryptographically bound to (content-addressable) and encapsulated by (self-referential) its SAD said.

self-addressing-data

an identifier that is content-addressable and self-referential. A SAID is uniquely and cryptographically bound to a serialization of data that includes the SAID as a component in that serialization said.

self-addressing-identifier

any identifier that is deterministically generated out of the content, or a digest of the content.

self-certifying-identifier

a type of Cryptonym that is uniquely cryptographically derived from the public key of an asymmetric signing keypair (public, private).

self-framing

a textual or binary encoding that begins with type, size, and value so that a parser knows how many characters (when textual) or bytes (when binary) to extract from the stream for a given element without parsing the rest of the characters or bytes in the element is Self-Framing.

server-sent-event

Mailbox notifications; a streaming service for the agent U/I, to get notifications from the KERI system itself.

siger

indexed-signature

signer

A primitive that represents a private key. It has the ability to create Sigers and Cigars (signatures).

signify-keria-request-authentication-protocol

SKRAP is a client to the KERIA server. Mobile clients will be using SKRAP to connect to KERI AIDs via agents in the new, multi-tenant Mark II Agent server, keria.

signify

Signify is a web client key-event signing - and key pair creation app that minimizes the use of KERI on the client.

signing-authority

The authority to sign on behalf of the controller of the authoritative key pair. Often in situation where delegation has taken place, e.g. a custodial agent. These are limited rights because rotation-authority is not included.

simple-keri-for-web-auth

A KERI implementation that sacrifices performance or other non-security feature for usability. In general a narrow application of KERI may not require all the features of KERI but those features that it does support must still be secure.

SKRAP

signify-keria-request-authentication-protocol

SKWA

simple-keri-for-web-auth

sniffable

A stream is *sniffable* as soon as it starts with a group code or field map; in fact this is how our parser (parside) works. and detects if the CESR stream contains a certain datablock.

sniffer

The *sniffer* is part of parside and detects if the CESR stream contains CESR binary, CESR Text, JSON, CBOR, MGPK.

solicited-issuance

The issuance of a Legal Entity vLEI Credentials, OOR vLEI Credentials and ECR vLEI Credentials upon receipt by the QAR of a Fully Signed issuance request from the AVR(s) of the legal-entity.

SPAC

secure-private-authentic-confidentiality

spurn

To *reject*. In KERI, "spurn" refers to a cryptographic or protocol-based act of rejecting an invalid or untrusted event. This rejection is deliberate and purposeful, ensuring the system's integrity by disregarding information that does not meet the necessary validation criteria. The verb 'spurn' is first used in the IPEX specification.

ssi-system

The SSI Infrastructure consists of the technological components that are deployed all over the world for the purpose of providing, requesting and obtaining data for the purpose of negotiating and/or executing electronic transactions.

stable

Refers to the state of cryptographic verifiability across a network or system. It generally implies that a particular identifier, event, or data set is consistent, fully verified, and cannot be contested within KERI.

stale-event

A stale key event is an outdated or irrelevant (key) event involving an stale-key that may compromise security.

stale-key

A stale key is an outdated or expired encryption key that should no longer be used for securing data

stream

a CESR Stream is any set of concatenated Primitives, concatenated groups of Primitives, or hierarchically composed groups of primitives.

streamer

A convenience class for supporting stream parsing, including nested (tunneled, encrypted) CESR streams. Streams can be a mixture/combination of different primitive, including other streams. A stream is a concatenation of primitives.

strip-parameter

tells us what part of the CESR stream will be parsed by which code.

targeted-acdc

an ACDC with the presence of the Issuee field in the attribute or attribute aggregate sections.

TEL

transaction-event-log

text-binary-concatenation-composability

An encoding has *composability* when any set of self-framing concatenated primitives expressed in either the text domain or binary domain may be converted as a group to the other domain and back again without loss.

tholder

t-holder object that supports fractionally-weighted signing-threshold

threshold-of-accountable-duplicity

The threshold of accountable duplicity (TOAD) is a threshold number `M` that the controller declares to accept accountability for an event when any subset `M` of the `N` witnesses confirm that event. The threshold `M` indicates the minimum number of confirming witnesses the controller deems sufficient given some number `F` of potentially faulty witnesses, given that `M >= N - F`. This enables a controller to provide itself with any degree of protection it deems necessary given this accountability.

threshold-signature-scheme

or TSS; is a type of digital signature protocol used by Mutli-party Computation (MPC) wallets to authorize transactions or key state changes.

TOAD

threshold-of-accountable-duplicity

top-level-section

The fields of an ACDC in compact-variant. The value of a top level section field is either the SAD or the SAID of the SAD of the associated section.

transaction-event-log

The set of transactions that determine registry state form a log called a Transaction Event Log (TEL). The TEL provides a cryptographic proof of registry state by reference to the corresponding controlling key-event-log. Any validator may therefore cryptographically verify the authoritative of the registry.

transfer-off-ledger

The act of transferring control authority over an identifier from a ledger (or blockchain) to the native verifiable KERI data structure Key Event Log.

trust-domain

A trust domain is the ecosystem of interactions that rely on a trust basis. A trust basis binds controllers, identifiers, and key-pairs. *For example the Facebook ecosystem of social interactions is a trust domain that relies on Facebook's identity system of usernames and passwords as its trust basis.*

trust-spanning-protocol

Protocol using verifiable-identifiers that signs every single message on the internet and makes them verifiable.

TSP

trust-spanning-protocol

univalent

In identifier systems, univalent means having a unique and non-ambiguous identifier for each entity or resource. This means that there is a *one-to-one correspondence* between the identifiers and the entities, and that no two different entities share the same identifier.

unpermissioned-correlation

a correlation established between two or more disclosed ACDCs whereby the discloser of the ACDCs does not permit the disclosee to establish such a correlation.

unsolicited-issuance

Issuance of a Legal Entity vLEI Credential upon notice by a QAR to the AVR(s) of the Legal Entity that a Legal Entity vLEI Credential has been solicited on the legal-entity's behalf.

untargeted-acdc

an ACDC without the presence of the Issuee field in the attribute or attribute aggregate sections.

vcp

vcp = vdr incept, verifiable data registry inception

VCTEL

virtual-credential-transaction-event-log

vdr

verifiable-data-registry

verfer

A primitive that represents a public key. It has the ability to verify signatures on data.

verifiable-credential

Verifiable credentials (VCs) are an open standard for digital credentials. They can represent information found in physical credentials, such as a passport or license, as well as new things that have no physical equivalent, such as ownership of a bank account.

verifiable-legal-entity-identifier

Verifiable credentials are issued by authorized validation agents (QVI) under the governance of GLEIF, who delegate tasks to these agents. They provide cryptographic proof that the information about a legal entity, as linked to its Legal Entity Identifier (LEI), is verifiably authentic, accurate, and up-to-date.

verifiable

a condition of a KEL: being internally consistent with the integrity of its backward and forward chaining digest and authenticity of its non-repudiable signatures.

verification

An action an agent (of a principal) performs to determine the authenticity of a claim or other digital object using a cryptographic key.

verify

The act, by or on behalf of a party, of determining whether that data is authenticity (i.e. originates from the party that authored it), timely (i.e. has not expired), and conforms to other specifications that apply to its structure.

version-code

tells you which set of tables to load, it tells the table state. It's a unique code. what version of the table is going to load.

version-string

the first field in any top-level KERI field map in which it appears.

version

an instance of a KEL for an AID in which at least one event is unique between two instances of the kel.

virtual-credential-transaction-event-log

will track the issued or revoked state of each virtual credential (VC) and will contain a reference to its corresponding *management transaction event log (management TEL)*.

vrt

vrt = vdr rotate, verifiable data registry rotation

watcher

an *entity* or *component* that keeps a copy of a kerl for an identifier but that is not designated by the *controller* of the identifier as one of its witnesses. See annex watcher.

weight-of-weights

There are 2 levels in the multi-sign weighted thresholds of multisig in KERI because the solution only needs to focus on *tightly cooperating teams*.

weight

an optional field map in the Edge section that provides edge weight property that enables directed weighted edges and operators that use weights.

well-known-witnesses

Witness identifier creation by using *salts* to initialize their key stores so that you can predict what identifiers will be created. For testing purposes only!

witness

a witness is an entity or component designated (trusted) by the controller of an identifier. The primary role of a witness is to verify, sign, and keep events associated with an identifier. A witness is the controller of its own self-referential identifier which may or may not be the same as the identifier to which it is a witness. See also keri's-algorithm-for-witness-agreement.

xip

A XIP message allows a transaction set to be a mini peer to peer exchange to become a verifiable data structure. It makes the transaction become duplicity evident.

agent

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	910006489e6ae5ebd79ca096682e2ec8fac5bc65

An actor that is executing an action on behalf of a party (called the principal of that actor). In the context of decentralized digital trust infrastructure, the term "agent" is most frequently used to mean a digital agent.

Source: eSSIF-Lab.

See also: wallet.

Note: In a ToIP context, an agent is frequently assumed to have privileged access to the wallet(s) of its principal. In market parlance, a mobile app performing the actions of an agent is often simply called a wallet or a digital wallet.

attribute

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	910006489e6ae5ebd79ca096682e2ec8fac5bc65

An identifiable set of data that describes an entity, which is the subject of the attribute.

See also: property.

Supporting definitions:

eSSIF-Lab: Data that represents a characteristic that a party (the owner of the attribute) has attributed to an entity (which is the subject of that attribute).

Note: An identifier is an attribute that uniquely identifies an entity within some context.

attributional-trust

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

contextual-linkability

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

control-authority

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

delegation

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	910006489e6ae5ebd79ca096682e2ec8fac5bc65

The act of a first party authorizing a second party to perform a set of actions for or on behalf of the first party. Delegation may be performed by the first party (the delegator) issuing a delegation credential that gives a certain set of capabilities to the second party (the delegatee).

discovery

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

identity-assurance

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

legitimized-human-meaningful-identifier

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

non-repudiable

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

non-transferable-identifier

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary

Property	Value
Commit hash	not found

This term was not found in the external repository.

persistent-identifier

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

reputational-trust

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

secure-attribution

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

self-sovereign-identity

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

SSI

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	910006489e6ae5ebd79ca096682e2ec8fac5bc65

See: self-sovereign identity.

Note: In some contexts, such as academic papers or industry conferences, this acronym has started to replace the term it represents.

transferable-identifier

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

verifiable-identifier

Property	Value
Owner	henkvancann
Repo	ctwg-main-glossary
Commit hash	not found

This term was not found in the external repository.

transferable

DAR

OOR

QAR

QVI

vlei credential

vlei-ecosystem-governance-framework

vlei-role-credential

vLEI

agency

More in extended KERI glossary

ledger-backer

A witness in KERI that is ledger-registered. It's a type of backer that proof its authenticity by a signing key anchored to the public key of a data item on a (public) blockchain.

More in extended KERI glossary

legal-entity-engagement-context-role-vlei-credential-governance-framework

A document that details the requirements for vlei-role-credential **issued to** representatives of a Legal Entity *in other than official roles* but in functional or other context of engagement.

Source: Draft vLEI Ecosystem Governance Framework Glossary.

More in extended KERI glossary

legal-entity-official-organizational-role-vlei-credential-governance-framework

A document that details the requirements for vlei-role-credential **issued to** official representatives of a Legal Entity.

Source: Draft vLEI Ecosystem Governance Framework Glossary.

More in extended KERI glossary

legal-entity-vlei-credential-governance-framework

A *document* that details the requirements for vLEI Credential **issued by** a qualified-vlei-issuer to a legal-entity.

More in extended KERI glossary

legitimized-human-meaningful-identifier

listed-identifier

Is a list in an authentic-chained-data-container of authorised did:webs identifier + method; the list appears in the metadata of the did:webs DID-doc.

Source: paraphrased Samuel Smith, Zoom meeting *KERI dev* Thursday Nov 9 2023

More in extended KERI glossary

live-attack

an attack that compromises either the current signing keys used to sign non-establishment events or the current pre-rotated keys needed to sign a subsequent establishment event. See (Security Properties of Prerotation)[#live-attacks].

Source: Dr. S.Smith

More in extended KERI glossary

locked-state

The default status a KERI data store is in once it has been created using a passcode; it is by default encrypted.

More in extended KERI glossary

management-TEL

management-transaction-event-log

More in extended KERI glossary

management-transaction-event-log

A 'management transaction-event-log' will signal the creation of the *Virtual Credential Registry VCR* and track the list of *Registrars* that will act as *backer* for the individual _ transaction event logs (TELs)_ for each virtual-credential (VC).

More in extended KERI glossary

moobi

Multi OOBI would allow to share a bunch of different end-points (oobis) all at once. A way for a single store to share multiple endpoints for that store.

More in extended KERI glossary

most-compact

An ACDC that, for a given level of disclosure, is as compact as it can be, which means

- it has the SAIDs for each section that are not disclosed
- it has expanded sections that are disclosed

More in extended KERI glossary

multi-valent

A delegator may have multiple delegate, thereby enabling elastic horizontal scalability. Multiple delegates from a single delegator. Furthermore, each delegate may act as a delegator for its own delegates to form a *nested delegation tree*.

More in extended KERI glossary

naive-conversion

Non-CESR Base64 conversion. How people are used to using the Base64 encode and decode. Without pre-padding etc all the stuff CESR does to ensure aligns on 24 bit boundaries so CESR never uses the '=' pad character. But naive base64 will pad if the length is not 24 bit aligned.

Source: Samuel Smith in issue 34

More in extended KERI glossary

ndigs

Digests of public keys, not keys themselves. The reason to use ndigs is to prove control over public keys or to hide keys. It's used in Keripy and consists of a list of qualified base64 digests of public rotation key derivations.

More in extended KERI glossary

nested-cooperative-delegated-identifiers

In KERI delegations are cooperative, this means that both the delegator and delegate must contribute to a delegation. The delegator creates a cryptographic commitment in either a rotation or interaction event via a seal in a delegated establishment event. The delegate creates a cryptographic commitment in its establishment event via a seal to the delegating event.

More in extended KERI glossary

next-threshold

represents the number or fractional weights of signatures from the given set of next keys required to be attached to a Message for the Message to be considered fully signed.

More in extended KERI glossary

non-establishment-event

a Key event that does not change the current Key state for an AID. Typically, the purpose of a Non-establishment event is to anchor external data to a given Key state as established by the most recent prior Establishment event for an AID.

Source: Dr. S. Smith

More in extended KERI glossary

non-interactive-authentication-design

A group of approaches having non-interactive mechanisms that pose unique problems because they do not allow a challenge response reply handshake. A request is submitted that is self-authenticating without additional interaction.

More in extended KERI glossary

non-repudiable

non-transferable-identifier

official-organizational-role

Also ‘OOR’. A person that represents the Legal Entity in an official organizational role and is issued an OOR vLEI Credential.

Source Draft vLEI Ecosystem Governance Framework Glossary.

More in extended KERI glossary

opcode

Opcodes are meant to provide stream processing instructions that are more general and flexible than simply concatenated primitives or groups of primitives.

More in extended KERI glossary

operator

an optional field map in the Edge section that enables expression of the edge logic on edge subgraph as either a unary operator on the edge itself or an m-ary operator on the edge group.

Source: Dr. S.Smith

More in extended KERI glossary

out-of-band-introduction

Out-of-band Introductions (OOBIs) are discovery and validation of IP resources for key-event-receipt-infrastructure autonomic identifiers. **Discovery via URI, trust via KERI.**

The simplest form of a KERI OOBI is a namespaced string, a tuple, a mapping, a structured message, or structured attachment that contains both a KERI AID and a URL. The OOBI associates the URL with the AID.

More in extended KERI glossary

parside

is a bunch of generators. Responsible for pulling out a stream of bits from a CESR stream and parse it.

Sam Smith suggested for Parside to not iterate stuff, only parse chunks delimited by the count-code. (Source Cesride: meeting Feb 2 2023)

More in extended KERI glossary

partial-disclosure

a disclosure of an ACDC that partially discloses its field maps using Compact Disclosure. The Compact Disclosure provides a cryptographically equivalent commitment to the yet-to-be-disclosed content, and the later exchange of the uncompacted content is verifiable to an earlier Partial Disclosure. Unlike Selective disclosure, a partially disclosable field becomes correlatable to its encompassing block after its Full Disclosure.

Source: Dr. S. Smith

More in extended KERI glossary

partial-pre-rotation

partial-rotation

More in extended KERI glossary

partial-rotation

The pre-rotation mechanism supports partial pre-rotation or **more exactly partial rotation of pre-rotated keypairs**. It's a rotation operation on a set of pre-rotated keys that may keep some keys in reserve (i.e unexposed) while exposing others as needed.

More in extended KERI glossary

pathing

It was designed to sign portions of a credential aimed at complex cases like

- a credential embedded in another credential
- multiple signers, only signing portions of a credential (partial signing)

More in extended KERI glossary

percolated-discovery

a discovery mechanism for information associated with an AID or a SAID, which is based on Invasion Percolation Theory. Once an entity has discovered such information, it may in turn share what it discovers with other entities. Since the information so discovered is end-verifiable, the percolation mechanism and percolating intermediaries do not need to be trusted.

Source: Dr. S. Smith

percolated-information-discovery

More in extended KERI glossary

percolated-information-discovery

In the OOBI protocol, a discovery mechanism for the KERI and the ACDC protocols is provided by a bootstrap that enables Percolated Information Discovery (PID), which is based on Invasion Percolation Theory.

After related information for discovery and verification is bootstrapped from the OOBI, subsequent authorization is non-interactive, thus making it highly scalable. This provides what we call zero-trust percolated discovery or speedy percolated discovery.

More in extended KERI glossary

persistent-identifier

pre-rotation

Cryptographic commitment to next rotated key set in previous rotation or inception-event.

More in extended KERI glossary

prefix

A prefix that is composed of a basic Base-64 (URL safe) derivation code pre-pended to Base-64 encoding of a basic public digital signing key.

Including the derivation code in the prefix binds the derivation process along with the public key to the resultant identifier.

More in extended KERI glossary

presentation-exchange

An exchange that provides disclosure of one or more authentic-chained-data-containers between a Discloser and a Disclosee.

A presentation exchange is the process by which authenticity information may be exchanged between two parties, namely, the discloser and disclosee.

More in extended KERI glossary

primary-root-of-trust

In KERI a root-of-trust that is cryptographically verifiable all the way to its current controlling key pair in a PKI.

The characteristic *primary* is one-on-one related to the **entropy** used for the creation of (the seed of) the private keys.

More in extended KERI glossary

proem

A “proem” is an introductory statement, preamble, or preface. It sets the stage for the content that follows, often providing context, framing the discussion, or outlining the purpose and scope of the material.

More in extended KERI glossary

promiscuous-mode

It is the mode a watcher runs in. A watcher uses the same code as a witness. However a watcher does so “lacking standards of selection; acting without careful judgment; indiscriminate”. Or “Showing little forethought or critical judgment; casual.”

Source

More in extended KERI glossary

proof-of-authorship

Proof that somebody or something has originally created certain content. It’s about *data*’s inception. Whereas proof-of-authority is about *rights* attached to this data.

More in extended KERI glossary

provenanced

The act of verifying authenticity or quality of documented history or origin of something.

More in extended KERI glossary

public-transaction-event-log

is a public hash-linked data structure of transactions that can be used to track state anchored to a key-event-log.

More in extended KERI glossary

public-verifiable-credential-registry

is a form of a Verifiable Data Registry that tracks the issuance/revocation state of credentials issued by the controller of the key-event-log. Two types of TELs will be used for this purpose: management-transaction-event-log and virtual-credential-transaction-event-log.

More in extended KERI glossary

qry

qry = query

More in extended KERI glossary

quadlet

a group of 4 characters in the T domain and equivalently in triplets of 3 bytes each in the B domain used to define variable size.

Source: Dr. S. Smith

More in extended KERI glossary

qualified-vlei-issuer-vlei-credential-governance-framework

A *document* that details the requirements to enable this Credential to be **issued by** GLEIF **to** qualified-vlei-issuer which allows the Qualified vLEI Issuers to issue, verify and revoke legal-entity-vlei-credential-governance-framework, legal-entity-official-organizational-role-vlei-credential-governance-framework, and legal-entity-engagement-context-role-vlei-credential-governance-framework.

More in extended KERI glossary

qualified-vlei-issuer

The contracting party to the vLEI Issuer Qualification Agreement that has been qualified by GLEIF as a Qualified vLEI Issuer.

Source: Draft vLEI Ecosystem Governance Framework Glossary.

More in extended KERI glossary

qualified

When qualified, a cryptographic primitive includes a prepended derivation code (as a proem), that indicates the cryptographic algorithm or suite used for that derivation.

More in extended KERI glossary

qvi-authorized-representative

A designated representative of a QVI authorized, to conduct QVI operations with GLEIF and legal-entity. Also referring to a person in the role of a QAR.

Paraphrased by @henkvancann from source Draft vLEI Ecosystem Governance Framework Glossary.

More in extended KERI glossary

rct

rct = receipt

More in extended KERI glossary

read-update-nullify

Read, update, nullify are a set of actions you (or a server) can take on data. “Read” means to view it, “update” means to change it, and “nullify” means to invalidate it, but not “Delete” it. Mind you, there’s also no “Create”.

More in extended KERI glossary

receipt-log

ordered record of all key event receipts for a given set of witnesses.

More in extended KERI glossary

receipt

event message or reference with one or more witness signatures.

See Also:

key-event-receipt

More in extended KERI glossary

reconciliation

Reconciliation is the process in which you decide to accept a fork of the key-event-log or not.

Source: Samuel Smith, Zoom meeting Jan 2 2024.

More in extended KERI glossary

redundant-credential

Multiple credentials issued by the same issuer (e.g. a QVI). They do not have anything to do with each other. They are independently valid.

More in extended KERI glossary

registrar

identifiers that serve as backers for each transaction-event-log (TEL) under its provenance. This list of Registrars can be rotated with events specific to a certain type of TEL. In this way, a Registrar is analogous to a Backer in KERI KELs and Registrar lists are analogous to Backer lists in KERI KELs.

More in extended KERI glossary

registration-interaction

Setup/Registration interaction, new AID and authorization to establish access control. You present a (vLEI) credential. You don’t want that captured and misused. Narrowing the scope to a certain role (e.g. Document Submitter) is a pre-registration via delegation authority.

More in extended KERI glossary

reputation

Consistent behaviour over time on the basis of which anyone else makes near-future decisions.

Source: Samuel Smith at IIW37.

Also see TrustoverIP definition: reputation

More in extended KERI glossary

reputational-trust

reserve-rotation

One important use case for partial-rotation is to enable pre-rotated key pairs designated in one establishment-event **to be held in reserve and not exposed** at the next (immediately subsequent) establishment event.

Source IETF-KERI draft 2022 by Samual Smith.

More in extended KERI glossary

rev

rev = vc revoke, verifiable credential revocation

More in extended KERI glossary

revocation-event

An event that revokes control-authority over an identifier. From that point in time the authoritative key-pairs at hand are not valid anymore.

More in extended KERI glossary

root-autonomic-identifier

An entity may provide the root-of-trust for some ecosystem (with delegation)via its root AID. Let's call this the *RID* for "root AID". The RID must be protected using the highest level of security in its key-management.

More in extended KERI glossary

rot

JSON field name (attribute) for Rotation Event; its content (value) contains a hash pointer. All transaction-event-log events are anchored in a key-event-log in either ixn (interaction-event) or rot (rotation-events). This is the foundation enabling a verifiable credential protocol to be built on top of KERI.

Source Kent Bull 2023

More in extended KERI glossary

rotation-authority

The (exclusive) right to rotate the authoritative key pair and establish changed control authority.

More in extended KERI glossary

rotation-event

an Establishment Event that provides the information needed to change the Key state, which includes a change to the set of authoritative keypairs for an AID.

Source: Dr. S.Smith

More in extended KERI glossary

rotation

The operation of revoking and replacing the set of authoritative key-pair for an AID. This operation is made verifiable and duplicity evident upon acceptance as a rotation event that is appended to the AID's KEL.

Source Sam Smith

More in extended KERI glossary

rpy

rpy = reply

More in extended KERI glossary

rules

a top-level field map within an ACDC that provides a legal language as a Ricardian Contract, which is both human and machine-readable and referenceable by a cryptographic digest.

Source: Dr. S. Smith

More in extended KERI glossary

run-off-the-crud

RUN off the CRUD is an alternative to the traditional CRUD approach to defining basic operations on resources in data management systems (e.g., databases, APIs). RUN stands for Read, Update, Nullify and bears a nuanced approach to deletion.

More in extended KERI glossary

sally

is an implementation of a verification service and acting as a reporting server. It is purpose-built software for the vLEI ecosystem to allow participants in the vLEI ecosystem present credentials, so the GLEIF Reporting API can show what vLEI are; issued to legal-entity.

More in extended KERI glossary

salter

A primitive that represents a seed. It has the ability to generate new signers.

Source by Jason Colburne

More in extended KERI glossary

salty-nonce-blinding-factor

For ease of sharing a secret and hiding information with this secret of Blindable State TELs we use a Salty Nonce Blinding Factor. You'd like to hide the state of certain credentials to some verifiers in the future, while keeping the state verifiable for others.

More in extended KERI glossary

schema

the said of a JSON schema that is used to issue and verify an ACDC.

Source: Dr. S.Smith

More in extended KERI glossary

secondary-root-of-trust

In KERI its a root-of-trust that, for its secure attribution, depends on another verifiable data structure (VDS) which MUST be a primary-root-of-trust.

By its nature and cryptographic anchoring via seal to a primary root-of-trust, a secondary root-of-trust still has a high level of trustability and can be automatically verified.

More in extended KERI glossary

secure-asset-transfer-protocol

An IETF protocol (and working group) in the making (as of mid 2022) for moving assets between blockchains.

More in extended KERI glossary

secure-attribution

secure-private-authentic-confidentiality

ToIP Trust Spanning Layer Group realized we do have a secure authentication layer (KERI) but we don't have a secure confidentiality and privacy mechanism. Sam Smith proposes SPAC paper to define this.

Related:

https://www.usenix.org/system/files/sec22-cohen.pdf

More in extended KERI glossary

security-cost-performance-architecture-trade-off

The degree of protection offered by a key management infrastructure usually forces a trade-off between security, cost, and performance.

Typically, key generation happens relatively infrequently compared to event signing. But highly secure key generation may not support highly performant signing. This creates an architecture trade-off problem.

Paraphrased from source Universal Identifier Theory by Samuel Smith

More in extended KERI glossary

security

'secure' is free from or not exposed to danger or harm; safe. For identifiers *security* typically means secure from *exploit* or *compromise*. More specifically an identifier is secure with respect to an entity if there is a mechanism by which that entity may prove it has controller over the identifier.

Also see TrustoverIP security-policy

More in extended KERI glossary

selective-disclosure

a disclosure of an ACDC that selectively discloses its attributes using Compact Disclosure. The set of selectively disclosable attributes is provided as an array of blinded blocks where each attribute in the set has its own dedicated blinded block. Unlike Partial Disclosure, the selectively disclosed fields are not correlatable to the so far undisclosed but selectively disclosable fields in the same encompassing block.

Source: Dr. S. Smith

More in extended KERI glossary

self-addressed-data

a representation of data content from which a SAID is derived. The SAID is both cryptographically bound to (content-addressable) and encapsulated by (self-referential) its SAD said.

Source: Dr. S.Smith

More in extended KERI glossary

self-addressing-data

an identifier that is content-addressable and self-referential. A SAID is uniquely and cryptographically bound to a serialization of data that includes the SAID as a component in that serialization said.

Source: Dr. S. Smith

More in extended KERI glossary

self-addressing-identifier

any identifier that is deterministically generated out of the content, or a digest of the content.

Source: Dr. S. Smtih

More in extended KERI glossary

self-certifying-identifier

a type of Cryptonym that is uniquely cryptographically derived from the public key of an asymmetric signing keypair (public, private).

Source: Dr. S. Smith

Also see the TrustoverIP scope definition: self-certifying identifier

More in extended KERI glossary

self-framing

a textual or binary encoding that begins with type, size, and value so that a parser knows how many characters (when textual) or bytes (when binary) to extract from the stream for a given element without parsing the rest of the characters or bytes in the element is Self-Framing.

More in extended KERI glossary

self-sovereign-identity

server-sent-event

Mailbox notifications; a streaming service for the agent U/I, to get notifications from the KERI system itself.

More in extended KERI glossary

siger

indexed-signature

More in extended KERI glossary

signer

A primitive that represents a private key. It has the ability to create Sigers and Cigars (signatures).

Source by Jason Colburne

More in extended KERI glossary

signify-keria-request-authentication-protocol

SKRAP is a client to the KERIA server. Mobile clients will be using SKRAP to connect to KERI AIDs via agents in the new, multi-tenant Mark II Agent server, keria.

More in extended KERI glossary

signify

Signify is a web client key-event signing - and key pair creation app that minimizes the use of KERI on the client.

More in extended KERI glossary

signing-authority

The authority to sign on behalf of the controller of the authoritative key pair. Often in situation where delegation has taken place, e.g. a custodial agent. These are limited rights because rotation-authority is not included.

More in extended KERI glossary

simple-keri-for-web-auth

A KERI implementation that sacrifices performance or other non-security feature for usability. In general a narrow application of KERI may not require all the features of KERI but those features that it does support must still be secure.

More on source Github Repo SKWA.

More in extended KERI glossary

sniffable

A stream is *sniffable* as soon as it starts with a group code or field map; in fact this is how our parser (parside) works. and detects if the CESR stream contains a certain datablock.

The datablock of CESR binary, CESR Text, JSON, CBOR, MGPK have an Object code or the Group code (binary or text) and it's always a recognizable and unique *three bit combination*.

More in extended KERI glossary

sniffer

The *sniffer* is part of parside and detects if the CESR stream contains CESR binary, CESR Text, JSON, CBOR, MGPK.

More in extended KERI glossary

solicited-issuance

The issuance of a Legal Entity vLEI Credentials, OOR vLEI Credentials and ECR vLEI Credentials upon receipt by the QAR of a Fully Signed issuance request from the AVR(s) of the legal-entity.

Source: Draft vLEI Ecosystem Governance Framework Glossary.

More in extended KERI glossary

spurn

To *reject*. In KERI, "spurn" refers to a cryptographic or protocol-based act of rejecting an invalid or untrusted event. This rejection is deliberate and purposeful, ensuring the system's integrity by disregarding information that does not meet the necessary validation criteria. The verb 'spurn' is first used in the IPEX specification.

More in extended KERI glossary

ssi-system

The SSI Infrastructure consists of the technological components that are deployed all over the world for the purpose of providing, requesting and obtaining data for the purpose of negotiating and/or executing electronic transactions.

Paraphrased by @henkvancann based on source eSSIF-lab

More in extended KERI glossary

stable

Refers to the state of cryptographic verifiability across a network or system. It generally implies that a particular identifier, event, or data set is consistent, fully verified, and cannot be contested within KERI.

More in extended KERI glossary

stale-event

A stale key event is an outdated or irrelevant (key) event involving an stale-key that may compromise security.

See also: stale-key

stale-key

A stale key is an outdated or expired encryption key that should no longer be used for securing data

See also: stale-event

stream

a CESR Stream is any set of concatenated Primitives, concatenated groups of Primitives, or hierarchically composed groups of primitives.

Source: Dr. S. Smith

More in extended KERI glossary

streamer

A convenience class for supporting stream parsing, including nested (tunneled, encrypted) CESR streams. Streams can be a mixture/combination of different primitive, including other streams. A stream is a concatenation of primitives.

Source: Kent Bull in chat Zoom meeting KERI Aug 6, 2024.

More in extended KERI glossary

strip-parameter

tells us what part of the CESR stream will be parsed by which code.

More in extended KERI glossary

targeted-acdc

an ACDC with the presence of the Issuee field in the attribute or attribute aggregate sections.

Source: Dr. S.Smith

untargeted-acdc

More in extended KERI glossary

text-binary-concatenation-composability

An encoding has *composability* when any set of self-framing concatenated primitives expressed in either the text domain or binary domain may be converted as a group to the other domain and back again without loss.

More in extended KERI glossary

tholder

t-holder object that supports fractionally-weighted signing-threshold

More in extended KERI glossary

threshold-of-accountable-duplicity

The threshold of accountable duplicity (TOAD) is a threshold number `M` that the controller declares to accept accountability for an event when any subset `M` of the `N` witnesses confirm that event. The threshold `M` indicates the minimum number of confirming witnesses the controller deems sufficient given some number `F` of potentially faulty witnesses, given that `M >= N - F`. This enables a controller to provide itself with any degree of protection it deems necessary given this accountability.

More in extended KERI glossary

threshold-signature-scheme

or TSS; is a type of digital signature protocol used by Mutli-party Computation (MPC) wallets to authorize transactions or key state changes.

Source Cryptoapis

More in extended KERI glossary

top-level-section

The fields of an ACDC in compact-variant. The value of a top level section field is either the SAD or the SAID of the SAD of the associated section.

An Issuer commitment via a signature to any variant of ACDC (compact, full, etc) makes a cryptographic commitment to the top-level section fields shared by all variants of that ACDC.

Paraphrased by @henkvancann based on source.

More in extended KERI glossary

transaction-event-log

The set of transactions that determine registry state form a log called a Transaction Event Log (TEL). The TEL provides a cryptographic proof of registry state by reference to the corresponding controlling key-event-log. Any validator may therefore cryptographically verify the authoritative of the registry.

More in extended KERI glossary

transfer-off-ledger

The act of transferring control authority over an identifier from a ledger (or blockchain) to the native verifiable KERI data structure Key Event Log.

More in extended KERI glossary

transferable-identifier

transferable

trust-domain

A trust domain is the ecosystem of interactions that rely on a trust basis. A trust basis binds controllers, identifiers, and key-pairs. *For example the Facebook ecosystem of social interactions is a trust domain that relies on Facebook's identity system of usernames and passwords as its trust basis.*

(Source whitepaper)

See also: trust-domain

More in extended KERI glossary

trust-spanning-protocol

Protocol using verifiable-identifiers that signs every single message on the internet and makes them verifiable.

Also see TrustoverIP toip-trust-spanning-protocol

univalent

In identifier systems, univalent means having a unique and non-ambiguous identifier for each entity or resource. This means that there is a *one-to-one correspondence* between the identifiers and the entities, and that no two different entities share the same identifier.

Source: Bing chat, Sept 2023

More in extended KERI glossary

unpermissioned-correlation

a correlation established between two or more disclosed ACDCs whereby the discloser of the ACDCs does not permit the disclosee to establish such a correlation.

Source: Dr. S. Smith

More in extended KERI glossary

unsolicited-issuance

Issuance of a Legal Entity vLEI Credential upon notice by a QAR to the AVR(s) of the Legal Entity that a Legal Entity vLEI Credential has been solicited on the legal-entity's behalf.

Source: Draft vLEI Ecosystem Governance Framework Glossary.

More in extended KERI glossary

untargeted-acdc

an ACDC without the presence of the Issuee field in the attribute or attribute aggregate sections.

Source: Dr. S. Smith

targeted-acdc

More in extended KERI glossary

vLEI

vcp

vcp = vdr incept, verifiable data registry inception

More in extended KERI glossary

vdr

verifiable-data-registry

More in extended KERI glossary

verfer

A primitive that represents a public key. It has the ability to verify signatures on data.

Source by Jason Colburne

More in extended KERI glossary

verifiable-credential

Verifiable credentials (VCs) are an open standard for digital credentials. They can represent information found in physical credentials, such as a passport or license, as well as new things that have no physical equivalent, such as ownership of a bank account.

See also: verifiable-credential

More in extended KERI glossary

verifiable-identifier

verifiable-legal-entity-identifier

Verifiable credentials are issued by authorized validation agents (QVI) under the governance of GLEIF, who delegate tasks to these agents. They provide cryptographic proof that the information about a legal entity, as linked to its Legal Entity Identifier (LEI), is verifiably authentic, accurate, and up-to-date.

More in extended KERI glossary

verifiable

a condition of a KEL: being internally consistent with the integrity of its backward and forward chaining digest and authenticity of its non-repudiable signatures.

Source: Dr. S. Smith

Explanation

Able to cryptographically verify a certain data structure on its inconsistency and its authenticity

More in extended KERI glossary

verification

An action an agent (of a principal) performs to determine the authenticity of a claim or other digital object using a cryptographic key.

Source: ToIP glossary, Jan 2024.

See also verification

More in extended KERI glossary

verify

The act, by or on behalf of a party, of determining whether that data is authenticity (i.e. originates from the party that authored it), timely (i.e. has not expired), and conforms to other specifications that apply to its structure.

Source eSSIF-lab in eSSIF-lab glossary

See also: verification

More in extended KERI glossary

version-code

tells you which set of tables to load, it tells the table state. It's a unique code. what version of the table is going to load.

More in extended KERI glossary

version-string

the first field in any top-level KERI field map in which it appears.

More in extended KERI glossary

version

an instance of a KEL for an AID in which at least one event is unique between two instances of the kel.

Source: Dr. S. Smith

More in extended KERI glossary

virtual-credential-transaction-event-log

will track the issued or revoked state of each virtual credential (VC) and will contain a reference to its corresponding *management transaction event log (management TEL)*.

More in extended KERI glossary

vlei credential

vlei-ecosystem-governance-framework

vlei-role-credential

vrt

vrt = vdr rotate, verifiable data registry rotation

More in extended KERI glossary

watcher

an *entity* or *component* that keeps a copy of a kerl for an identifier but that is not designated by the *controller* of the identifier as one of its witnesses. See annex watcher.

Source: Dr. S.Smith

More in extended KERI glossary

weight-of-weights

There are 2 levels in the multi-sign weighted thresholds of multisig in KERI because the solution only needs to focus on *tightly cooperating teams*.

- An individual using split keys over devices
- A team of teams

All other use cases can be solved by other means in KERI (e.g. delegation).

More in extended KERI glossary

weight

an optional field map in the Edge section that provides edge weight property that enables directed weighted edges and operators that use weights.

Source: Dr. S.Smith

More in extended KERI glossary

well-known-witnesses

Witness identifier creation by using *salts* to initialize their key stores so that you can predict what identifiers will be created. For testing purposes only!

More in extended KERI glossary

witness

a witness is an entity or component designated (trusted) by the controller of an identifier. The primary role of a witness is to verify, sign, and keep events associated with an identifier. A witness is the controller of its own self-referential identifier which may or may not be the same as the identifier to which it is a witness. See also keri's-algorithm-for-witness-agreement.

Source: Dr. S. Smith

More in extended KERI glossary

xip

A XIP message allows a transaction set to be a mini peer to peer exchange to become a verifiable data structure. It makes the transaction become duplicity evident.

Source KERI meeting 2024-03-12

More in extended KERI glossary