__old

Created by Drummond Reed, last modified by Kevin Griffin 4 minutes ago

This page contains the meeting agendas and notes for the ACDC Task Force. Note that for expediency it is a single running page of notes (vs. separate Meeting Notes pages for each meeting as is typical of other ToIP Working Groups and Task Forces). Meetings are in reverse chronological order.

- 2023-05-09
- 2023-04-25
- 2023-04-11
- 2023-03-28
- 2023-03-14
- 2023-02-28
- 2023-02-14
- 2023-01-31
- 2023-01-17
- 2023-01-03
- 2022-12-20
- 2022-12-06
- 2022-11-22
- 2022-11-08
- 2022-10-25
- 2022-10-11
- 2022-09-27
- 2022-09-13
- 2022-08-30
- 2022-08-16
- 2022-08-02
- 2022-07-19
- 2022-07-05
- 2022-06-21
- 2022-06-07
- 2022-05-24
- 2022-05-10
- 2022-04-26
- 2022-04-12
- 2022-03-29
- 2022-03-15
- 2022-03-01
- 2022-02-14
- 2022-01-31
- 2022-01-17
- 2022-01-03
- 2021-12-20
- 2021-12-06
- 2021-11-22
- 2021-11-08
- 2021-10-25
- 2021-10-11
- 2021-09-27
- 2021-09-13
- 2021-08-30

- 2021-08-16
- 2021-08-02
- 2021-07-19
- 2021-06-28
- 2021-06-21
- 2021-06-07
- 2021-05-17
- 2021-05-10
- 2021-03-26
- 2021-03-01
- 2021-03-01
- 2021-02-15
- 2021-02-01
- 2021-01-18
- 2021-01-04

Future Topics

Graduated disclosure in ACDCs
IPEX Specification
How ACDCs can be included with the Linux Foundation Open Wallet
Linux Foundation Open Wallet Initiative https://github.com/openwallet-foundation
AnonCreds as a separate library
SKWA Signify ACDC authorizations access control
EGF of vLEI
ACDC Validation Bundling - From validating signature, chains and schema all the way up the business logic stack
IOT and KERI and ACDC
Revisit BADA-RUN
Next IIW - tickets/game for next IIW
Revocation approach
Adoption of VC-ACDC

From Drummond Reed:

- There is a very active thread on the DID Core spec right now discussing the issues around DID subjects being different from DID key controllers.

I'd love to get the ACDC TF's view on if and how KERI addresses those issues. https://github.com/w3c/did-core/issues/83

Zoom Meeting Link

https://zoom.us/j/92692239100?pwd=UmtSQzd6bXg1RHRQYnk4UUEyZkFVUT09

2023-05-09

Attendees:

@ Samuel Smith

@ Kevin Griffin

@ Phil Feairheller

@ Kent Bull

@ Lance Byrd

@ Henk van Cann

@ Jason Colburne

@ Trent Larson

@ Steven Milstein

@ Nuttawut Kongsuwan

@ Arshdeep Singh

@Harif

@Alex Andrei

@ P Subrahmanyam

@ Ruth Choueka

@ Rodolfo Miranda

@ Neil Thomson

Click here for → Meeting Recording

Agenda / Notes

- Introductions
- Announcements
- Reports
  - W3C VCWG2
    - 1100 and 1101 PRs Read and comment on these threads
  - Signify
    - Trezor Ed25519 SHIM Python (Rodolpho)
  - vLEI
    - Tentatively accepted proposed path for US Customs as consumer of vLEI backed data. vLEI to provenance a JSON-LD version of the data. ECDSA Secp256r1 FIPS approved
    - LEI could be incorperated into the CCG Tracebaility Vocab
  - CESRide Rust got partial rotation working
    - Edge operators in ACDC
- Discussion
  - Adoption of VC-ACDC
    - https://github.com/WebOfTrust/vc-acdc
  - Proposal:
    Move VC-ACDC under ToIP - Resolved passed unanimously
  - Next proposal ask working group
  - Edge Operators in ACDC
  - Graduated Disclosure in ACDC

2023-04-25

Attendees:

@ Samuel Smith

@ Phil Feairheller

@ Rodolfo Miranda

@ Lance Byrd

@ Steven Milstein

@ Kevin Griffin

@cole davis

@ Jason Colburne

@ Ruth Choueka

@ Nuttawut Kongsuwan

@ Kent Bull

@Harif

@ Neil Thomson

@ Mark Scott

@ Joseph Lee Hunsaker

@alex Andrei

@ Daniel Hardman

@ Randy Warshaw

Click here for → Meeting Recording

Agenda / Notes

- Introductions
    - Welcome Cole from Switchchord.
- Announcements
    - Qui issuing dev ACDCs verified with KERIpy
    - RootsID/Lance consulting with GLEIF
- Reports
    - Qui issuing dev ACDCs verified with KERIpy
    - IIW Demo by Phil for KASSH
    - Provenant starting trails with KEIR/ACDC
- Discussion Items
    - What happened at IIW
        - SSH presentation (KASSH)
            - Organiation credentials for securing SFTP with ACDCs/KERI
        - Observations
            - more interest in KERI/ACDC vs challenging why KERI/ACDC
            - more non-GLEIF presentations (Randy, Kent, Jason, Nuttawut, and more!)
            - potential to add an official KERI 101! (following a current theme of OpenID Connect etc)
            - Yay for IPR, old repos have been archived
            - KERI/ACDC BDFL Benevolent Dictator For Life (Linux/Python)
            - Lance covered the sessions on LinkedIn
                - https://www.linkedin.com/in/2byrds/recent-activity/shares/
            - KERIA session was well received.
            - AI / Content provenance a major theme
    - ACDC Privacy mechanisms

Discussion

Randy: People are going to get over the excitement of having a vLEI in about two weeks. After that we need more engagement, even if It is just small utilities we use.

Kevin: It would be cool if this community would put ACDCs in some form of wallet.

Jason: That is what we are doing, all of these sorts of things. We want it to be used for tickets for events and many similar things.

Lance: Jason, what platforms are you seeking to support?

Jason: Since it is in Rust we want to support iOS, Android, and others. We are also offering a multi-tenant vault. We have built stuff on mobile now. We are going for an MVP in about 5 weeks.

... more discussion

Sam: With all this new interest in KERI and ACDC it is likely a good idea at the next IIW to have an ACDC 101, 201, and 301

2023-04-11

Attendees:

@ Samuel Smith

@ Phil Feairheller

@ Kevin Griffin

@ Kent Bull

@ Henk van Cann

@ Ruth Choueka

@ Lance Byrd

Click here for → Meeting Recording

Agenda

- Announcements
  - Waiting for IIW!
  - Provenant continues issue vLEIs!
- Reports
  - vLEI
    - https://github.com/w3c/vc-data-model/issues/1048
    - https://github.com/w3c/vc-specs-dir/pull/14
  - ToIP spanning layer
    - work shop this week
- Discussion Items
  - How to bind an AID to other key material (RSA Key)
    - Add a seal to the KEL point to the new key matieral or
    - Create a TEL to manage the state of the new key material or
    - Use BADA (Best Available Data Acceptance) policy, mechanism for signing data that inputs the key state of the signer as part of the state for replay attack detection
    - any recipient of a signed statement needs to know if it's a replay attack include key state
  - How would you do this in keripy?
    - Anchoring is easy, do an IXN event using the `kli`
    - No generic mechanism for TELs in keripy (we accept PRs)
    - Reply messages same ^^ (see end point code in keripy)
  - BADA (Best Available Data Acceptance) RUN (Read Update Nullify) articles
    - https://github.com/WebOfTrustInfo/rwot11-the-hague/blob/master/final-documents/taking-out-the-crud-five-fabulous-did-attacks.pdf
    - https://hackmd.io/@SamuelMSmith/Sy_g84sDK
    - https://github.com/trustoverip/acdc/wiki/best-available-data-acceptance-mechanism this is one the HackMDs?
    - https://weboftrust.github.io/ietf-oobi/draft-ssmith-oobi.html
  - IIW
    - - IIW Topics Sessions
      - KERI 101 Session - Nuttawut/Phil Introducing KERI

- Fit into the IIW 101 Series they hold every session
- KERI for Dummies
  - Stable Identifiers with underlying Dynamic Key State
  - - KERI 201 Session - Kent (an accelerated developer introduction to KERI and ACDC)
    - Possibly move to demo hour
    - Qui Identity - demo hour
    - Break out hour on getting KERI / decentralization adopted.
    - RootID participating in DIDComm 2 hack-a-thon - chat, issuance
    - did:keri - Watcher variant
    - Logging into SSH with KERI
    - CESRide/Parside/Signifide white boarding session
    - VC-ACDC talk around how to create other Proof Formats for W3C VCs
    - Sam possibly doing talk about SPAC Paper / ESSR (Meta-Cryptographic Systems)
    - Randy (Provenant) doing vLEI in Telecom, cross boarder KYC problems.
    - Binding actors to actions, making communications authentic
    - Salty Nonce drinking game
    - Signify / KERIA planning session (third day session)
    - Create a Google sheet for planning sessions - Phil
    - Sam session on reputation how to use AI against AI
  - So you want to be a QVI (GLEIF)
- ACDC Privacy Mechanisms
  - https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/SPAC_Message.md
  - https://weboftrust.github.io/ietf-acdc/draft-ssmith-acdc.html#name-unpermissioned-exploitation

2023-03-28

Attendees:
@ Samuel Smith
@ Phil Feairheller

@ Kevin Griffin

@ Kent Bull

@ P Subrahmanyam

@ Rodolfo Miranda

@ Henk van Cann

@ Arshdeep Singh

Click here for → Meeting Recording

Agenda

- Announcements
  - vc-acdc continues work
  - trust spanning protocol work continues - new white paper from @ Samuel Smith
    - https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/SPAC_Message.md
    - https://github.com/trustoverip/trust-spanning-protocol/discussions
  - Qui will be at IIW and is progressing work on ACDC creation in Rust
  - XBRL Digital signature working group, draft requirements complete
    - next steps are technical specification
    - any mechanism for signing an xbrl report package
    - signing visual components is included...
    - How do acdc and xbrl relate?
      - in the pilot we issued acdc role credentials and chained off that a data attestation
      - we provided that input to the xbrl group
- Reports

- vLEI
    - W3C direction of VC implementations. vLEI will be one of those as a transformation into the base media type
    - Schema directory
        - Kent: will make a PR once my KERI Tutorial is out at the end of this week, by March 31, 2023
    - We should move KASL (https://github.com/TetraVeda/kaslcred) under there (@ Kent Bull 🙂
- Discussion Items
    - May I ask if anyone here has experimented with signing PAdES (PDF Advanced Electronic Signature) with KERI?
        - No one explicitly but a good route for adoption
            - How would you go about integration into acrobat etc
            - currently signed with x509
    - Graduated disclosure
        - Append to extend
            - chain additional material to existing acdcs
            - no dynamically changing of existing material
            - hashes further up the chain remain verifiable
            - metadata acdc would be the first step in a graduated disclosure
                - Eg you're showing someone more personal information
                - here are my terms regarding the presentation
                - the disclosee they sign their metadata acdc with a blinded hash of the attribute block and the rules of the disclosure
    - IIW "thoughts"

2023-03-14

Attendees:

@ Samuel Smith

@ Kevin Griffin

@ Phil Feairheller

@ Kent Bull

@ Henk van Cann

@ Jason Colburne

@ Lance Byrd

Click here for → Meeting Recording

Agenda

- Announcements
    - W3C WI re-proposal 3/15 please support the work
    - KERI gone to 1.0 PyPi release upcoming.
    - ToIP TF trust spanning layer work continues (includes KERI/ACDC)
    - P256 support being added to keripy/cesride
    - ToIP Datamodelling and representation
        - Sam to present on authentic data chains
        - Data Modelling & Representation WG
          Tuesday, March 21·12:00 – 1:00pm ET
          https://zoom.us/j/99186768208?pwd=TUwxOUIvYW5xL0JHaEJTRlp5ZnNlUT09
    - Roots ID vLEI credentials received from Provenant!
    - KASLCred - saidifies a map of schema
        - https://github.com/tetraveda/kaslcred
        - additional blog post for issuing and verifiying an acdc

        - RootsID working on a hands on education "notebook" for SSI including KERI/ACDC

- Reports
    - vLEI
        - VC schema using JSON Schema for VC Data Model make ACDC schema compatible?
        - https://w3c-ccg.github.io/vc-json-schemas/
    - ViRA charter expanded to allow signing individual facts

- Discussion Items
    - Do we want to go to 1.0 for ACDC
    - Informal page within the repo "scrapbook"
        - summarize minor changes
        - markdown file within the IETF Draft ACDC repo
        - date | item
    - Milestones for ACDC/1.0
        - do we have any open github issues?
        - formaly publish a draft spec with IETF
        - ACDC went to production via KERIpy
    - Update ACDC readme to point to KERIpy 1.0
        - submission to IETF update the verion and IETF will pick it up
        - @ Kevin Griffin will look at GitHub issues

Graduated disclosure

- Minimum disclosure first
- only disclose what you need to further the transaction
- progression of least disclosures
    - progress next disclosure or stops
- disclosure transactions can provide protections, such as terms of disclosure/contractual obligations to minimize risk
    - "Chain-Link Confidentiality" paper by Woodrow Hartzog is a seminal work on the topic.
        - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045818
    - Woodrow Hartzog is one of the major legal privacy rights legal minds in this space.
    - legally we can protect privacy in terms of "data rights"
    - current vLEI implementation only has usage in the rules section
    - compact disclosure
        - disclose a hash of the data that can be used later to verify the data
    - partial disclosure
        - not disclosing everything you could disclose
        - disclosure hash/schema
    - selective disclosure
    - full disclosure would be the final step in graduated disclosure
- Public ACDCs have no UUID
- Private ACDCs have a UUID (salty nonce with sufficient entropy it can't be guessed) which means that you can selectively/partially disclose sections and the data you're disclosing cannot be guessed.
- Continue from section five

2023-02-28

Attendees:

@ Samuel Smith

@ Kevin Griffin

@ Kent Bull

@ Phil Feairheller

@ Lance Byrd

@ Rodolfo Miranda

@ P Subrahmanyam
@ Henk van Cann

Click here for → Meeting Recording

Agenda

- Announcements
  - Publishing requirements for data signatures inside XBRL and inclusion of ACDC Data Attestations.
    - Technical working group next step
  - Roots ID 6 month effort with Cardarno Foundation (supply chain, KERI, ACDC)
    - EGF Working group as a suggestion to get started with supply chain governance
  - Looking to get examples for CESR, for parsing events
    - Creating events and KELS to start
  - ToIP TSWG Trust spanning layer task force continuing meetings, looking to adopt KERI (ACDC)

Reports implementation of ACDCs

- vLEI
  - work items to update schema
  - RootsID vLEI from Provenant
    - Legal Entity vLEI and Offical Organization Role vLEI credentials for Rodolfo and Lance et al
- ViRA
  - See above on the XBRL
- HCF
- Provenant upcoming announcements
  - MWC conference on Mobile World Congress
- RootsID
- QUI Identity
  - KERI first then ACDC 🙂

Discussion Items

- W3C Face to Face outcomes
  - Scope to try resolve @context issues present within the W3C VC DM (multiple lengthy github issues)
    - ACDC can become a verifiable proof (external) with a uni-directional transform to the base media type of `credential+ld+json`
      - https://weboftrust.github.io/vc-acdc/
      - Hopefully approved by March feature freeze of the w3c vc data model
        - Requires three sponsors (GLEIF, ProSapien, one more)
        - Additional sponser (Shawn)
    - Similar approach from w3c/`vc-jwt` (https://github.com/w3c/vc-jwt)
    - Help appreciated with review/comments/questions
    - uni vs bi directional
      - receiver can process an ACDC, transform produces a valid JSON-LD object that can be used for RDF
      - vc-acdc will be unidirectional
        - default @context is open to discussion
      - more complex example would be a vLEI transformation
      - vc dm is payload of an acdc
      - Issue for addition of `payload` in ACDC up for discussion (https://github.com/trustoverip/tswg-acdc-specification/issues/74)
    - embedded proof follow similar pattern to how SAIDs work
      - adding proof inside the vc
    - external proof act as a container for the vc, the container contains the proof (Proof is on the ACDC)

- Also presentations on VC Data Integrity Proofs and Holder Binding

2023-02-14

Was postponed due to W3C CCG face to face meeting in Miami. This debate calls for VC Data Model arena match.

2023-01-31

Attendees:

@ Phil Feairheller

@ Samuel Smith

@ Henk van Cann

@ Kevin Griffin

@ Randy Warshaw

@ Ruth Choueka

@ Lance Byrd

Jason Colburn

@ Trent Larson

@ Rodolfo Miranda

@ Daniel Hardman

@ Scott Whitmire

@ Peter McCormick

@ Neil Thomson

@ Mark Scott

Click here for → Meeting Recording

Agenda

- Announcements
  - Daniel Hardman
    - https://cesrview.provenant.net/
    - Demo of CESR Viewer
  - W3CVC WG2
    - https://www.w3.org/2017/vc/WG/Meetings/F2F/Miami
  - ToIP Spanning Layer Group
  - GUT Meeting
    - outcome to help people use a simple/small subset of KERI

Reports implementation of ACDCs

- vLEI
  - upcoming backwards compatible changes to the vLEI OOR codes etc Rules.
  - Provenant vLEI issuances.
- ViRA
- HCF
- Provenant upcoming announcements

- RootsID
- QUI Identity

Discussion Items

- Schema definitions and publication
    - Potential permissionless registry of schema
        - schema is immutable (SAID), any changes get a new SAID
        - avoids namespace collision / name squat
        - Schema discovery (percolated discovery)
        - Questions about how to use schema, governance
            - How do we want to aggregate schema/community wide repo
        - Schema registration on witnesses
            - GitHub repo for submission of new schema
            - WebOfTrust (@ Kevin Griffin will create WebOfTrust/schema)
            - PRs welcome to submit a schema (not a shared governance trust registry)
            - Use GitHub pages for submission, and then build/publish, suggestion from @ Phil Feairheller
                - vLEI test schema
            - Description field / Metadata additions for human readble documentation
            - Add to ACDC spec to commit to metadata relevant to the schema.
                - Relevant metadata is a JSON SAD with its own SAID and the SAID is included in the Schema as the value of a description field in the schema.
        - Add guidelines via readme.md for kli commands to saidify a schema etc
        - Expansion of SAIDs with concat of two saids (Namespacing?)

2023-01-17

@ Phil Feairheller

@ Samuel Smith

@ Kent Bull

@ Henk van Cann

@ Rodolfo Miranda

@ Steven Milstein

@ Nuttawut Kongsuwan

@ Mark Scott

@ Joseph Lee Hunsaker

@ Peter McCormick

@ Arshdeep Singh

@ Scott Whitmire

Agenda

- Announcements
    - Trust Over IP Calendar needs to be updated, again. Calendar invite needs updated Zoom link.
    - Jason Colburne: QuiIdentity blog post incoming about why they are choosing KERI.
    - vLEI is in Production and Provenant is the first ever Qualified vLEI Issuer.

Reports implementation of ACDCs

- vLEI
    - Working on production roadmap for Q1
        - Will include QVI SDK
        - Will include Watcher Network
- ViRA
    - XBRL signatures group join meeting
- GS1
- HCF

Items

- Review "Future topics"
    - Clean up
        - Discovery Web-of-trust ecosystem trust anchors - comparison to did:peer: Discussed in KERI meeting, brief summary here.
        - Root of Trust / Trust Anchor also serves as a Discovery mechanism for pre-discovering KELs for the AIDs in a given ecosystem.
    - add summary of expectations for the discussion
    - do we need a third party (LF Open Wallet for example)
- ACDC Validation Bundling - From validating signature, chains and schema all the way up the business logic stack
    - Structural validation: Schema, signatures, chains, content (as constrained by the schema)
    - Business Logic Validation: Does this credential meet the requirements and needs of given business logic
    - GLEIF Reporting API Verifcation Service:
        - https://github.com/GLEIF-IT/sally
    - Is there a place for interleaving the structural validation with business logic validation?
        - Could we have call-outs from the structural validation at various stages in the process to perform step-wise business logic
    - How does caching of ACDC/KEL/TEL information affect forensic investigations of data
        - For example, "Did this driver have a valid license at the time (in the past) of an accident.
        - Having to constantly check for revocation status introduces possible network latency.
            - Polling or pushing can mitigate these problems

2023-01-03

@ Samuel Smith @ Kent Bull @ Henk van Cann @ Kevin Griffin @ Ruth Choueka @ P Subrahmanyam @ Mark Scott @ Nuttawut Kongsuwan @ Rodolfo Miranda @ Joseph Lee Hunsaker @ Trent Larson Michal Pietrus

Agenda

- Announcements

Reports implementation of ACDCs

- vLEI
    - Cardano?
    - Provenant
    - ECR Provenant issues
        - Slack channel vLEI
        - Schema
    - vLEI EGF Issues
        - action to add or decide on repot to host vLEI EGF issues @ Kevin Griffin
        - Community support from Henk to help with vLEI issues EGF
            - need more of a How To with vLEI EDF
    - Pending updates to Schema vLEI to add change required fields
- ViRA
- GS1
- HCF

Items

- ToIP ACDC Meeting Recordings are not available until 4 weeks after meeting. Need more timely availability.
    - @ Kevin Griffin action item need to talk to ToIP automate
- GLEIF Root-of-Official-Trust well known structure and formation details
    - GLEIF RoOT comprised of seven individuals and five "escrowed" participants used in creation of a multisig AID.
        - Uses establishment only events
        - Escrow participants are used in the eventuality that the root participants are unavailable (a designated survivor situation)
    - *Establishment only* means has no *non-establishment events*: https://github.com/trustoverip/acdc/wiki/non-establishment-event
    - GLEIF then created two additional multisig AIDs "Internal" and "External"
        - GLEIF RoOT then approved delegation of the internal and external AIDs, this delegation adds the first link in the chain of authority being established.
        - The "External" AID is how GLEIF manages its interactions with pending and existing QVIs (https://github.com/trustoverip/acdc/wiki/qualified-vlei-issuer)
            - This multisig AID is then used to issue the Qualified vLEI Issuer vLEI Credential to a QVI that has completed the GLEIF qualification process.
        - The Internal AID is how GLEIF acts as a Legal Entity in the vLEI ecosystem.
            - https://search.gleif.org/#/record/506700GE1G29325QX363/verifiable_credentials
- vLEI Schema Versioning EGF Doc: https://github.com/WebOfTrust/vLEI/blob/dev/docs/Schema_Registry.md
- When the version of the schema changes the SAID of the schema will change. A new credential based on the new scheme, will be a different credential (because the semantics might have changed) ... An old credential based on an old schema (version) will still validate. "Do I enforce the latest version of a schema for all the credentials or just their own version at the time of issuance?" → This has become a business logic decision.
- We don't have to have a protection against mutable schemas, like access control, because every mutated schema will lead to a new credential.
- GLEIF decides what goes into a vLEI; this is a governance design decision. So other identifier systems might have different governance designs; e.g. a committee voting on what goes into a vLEI-like data structure.

2022-12-20

@ Samuel Smith

@ Phil Feairheller

@ Lance Byrd

@ Kevin Dean

@ Rodolfo Miranda

@ Neil Thomson

Agenda

- Announcements
    - GLEIF Issuing Production vLEIs this week
        - Press Release
            - https://www.gleif.org/en/newsroom/press-releases/first-suite-of-vlei-services-to-enable-digital-signing-and-automated-verification-of-corporate-caller-ids
        - GLEIF Reporting API
            - https://search.gleif.org/#/record/506700GE1G29325QX363/verifiable_credentials
            - https://search.gleif.org/#/record/984500983AD71E4FBC41/verifiable_credentials
        - Ecosystem Governance Framework documents published
            - https://www.gleif.org/en/vlei/introducing-the-vlei-ecosystem-governance-framework
    - RootsID Demo'ed a Cardano Ledger Backer used to create an inception and several rotation events
    - XBRL International Digital Signatures working group meeting
- Reports Immplementation of ACDCs

        - vLEI
        - ViRA (verifiable iXBRL Report Attestation)
        - GS1 looking to implement in 2023
        - HCF was older implementation but more work in future
    - Items
        - TLS with ACDCs
            - Soon to be support for over the wire encryption for CESR
                - We need to add support for variable length code for encrypted primitive
                - Bare metal encrypted protocol for gossip protocol, over UDP for example
                - Once we have codes for variable length encrypted primitives, they can be embedded in ACDCs or DIDComm messages
            - DIDComm or TLS are options to use right now.
                - With CESR we could have a scalable UDP streaming protocol
            - Scalability and performance are the main reasons to use something other than DIDComm or TLS
            - Authenticity, confidentiality and privacy are the three trade offs of the CAP theorem
            - Encrypted at motion vs encrypted at rest
                - DIDComm and TLS solve the encrypted channel (at motion) problem. But once received, the encryption are thrown away.
                - With TLS alone and passwords you are vulnerable to attacks that can steal your password
                - With KERI over TLS a TLS attack can make you vulnerable to loss of confidentiality because they can see the content but not loss of any secrets because there are no shared secrets with KERI
                    - Good tradeoff to use KERI over TLS now.
                - In January we'll have codes for symmetric and asymmetric encrypted primitives.
            - How about OIDC4VC & OIDC4VP?
                - you can't have zero-trust with identity providers
                - identity providers can become super aggregators
                - Neil: The main use for VCs for OIDC is for Enterprise environments - not general internet
                - Many websites are converting from passwords to passkeys which will allow to bypass OpenID
            - What happened to DIDComm v3
                - Daniel Hardman will be starting that work in January to define v3, heavily KERI influenced. Tentatively for January 9th 9pm CET
                - Stripped down to what DIDComm does best
                - Daniel: There is a DIDComm gossip protocol
                    - https://github.com/dhh1128/didcomm.org/blob/gossyp/gossyp/README.md
                - Lance: Should agents that have implemented DIDComm v1 transition to DIDComm v2 or wait for v3?
                    - Daniel- go ahead and move to v2 because that will get you closer to v3.
        - GLEIF well-known root-of-trust

2022-12-06

@ Samuel Smith

Agenda

- Announcements
    - PoC Backer on Cardano Demo Next week in KERI Mtg
    - GLEIF Issuing Production vLEIs this week
- Items
    - Blinded Revocation Registries - addition to ACDC spec
    - TLS with ACDCs

2022-11-22

@ Samuel Smith

@ Phil Feairheller

@ Kent Bull

@ Lance Byrd

@ Rodolfo Miranda

@Alex Andrei

Agenda

- Announcements
  - What is EDP1vHcw_wc4M__Fj53-cJaBnZZASd-aMTaSyWEQ-PC2 ?
    - The GLEIF RoOT AID!
    - https://gleif-it.github.io/.well-known/keri/oobi/EDP1vHcw_wc4M__Fj53-cJaBnZZASd-aMTaSyWEQ-PC2
    - https://weboftrust.github.io/.well-known/keri/oobi/EDP1vHcw_wc4M__Fj53-cJaBnZZASd-aMTaSyWEQ-PC2
    -
```
{
  "v": "KERI10JSON00049d_",
  "t": "icp",
  "d": "EDP1vHcw_wc4M__Fj53-cJaBnZZASd-aMTaSyWEQ-PC2",
  "i": "EDP1vHcw_wc4M__Fj53-cJaBnZZASd-aMTaSyWEQ-PC2",
  "s": "0",
  "kt": [
    "1/3",
    "1/3",
    "1/3",
    "1/3",
    "1/3",
    "1/3",
    "1/3"
  ],
  "k": [
    "DFkI8OSUd9fnmdDM7wz9o6GT_pJIvw1K_S21AKZg4VwK",
    "DA-vW9ynSkvOWv5e7idtikLANdS6pGO2IHJy7v0rypvE",
    "DLWJrsKIHrrn1Q1jy2oEi8Bmv6aEcwuyIqgngVf2nNwu",
    "DD6JYvXBsVAmEtirgwKPQBHFwVQfX4f_CZQmBsOh_1hT",
    "DOOyxiELz2xqQCebeimJC4PW9Xv_5xgRkW7q_TC2lToN",
    "DGoS9UZrs0u2jiCMlMGAG5xpUwQQ66NyqEoxmq8OiFUT",
    "DBaAts7zYaRUNMkWIgWN5TL85cp61mHk_wlWzsIM-cc_"
  ],
  "nt": [
    "1/3",
    "1/3",
    "1/3",
    "1/3",
```

```
      "1/3",
      "1/3",
      "1/3"
    ],
    "n": [
      "EB_KZDNru1dlUb_Nk0EpxbU1ZDSNUO790RAZ_-ehCwR6",
      "EHgOexUh8AvN7rXblsSr6MJE5Gn1HPq5Mv9KFpCpllKN",
      "ECH4pTtUI653ykKb_capPBkKF3RvBZRzyb5dPfuJCfOf",
      "ELXXiPwoaWOVOTLMOAmg4IKkjFHFs3q2hsL9tHvuuC2D",
      "EAcNrjXFeGay9qqMj96FIiDdXqdWjX17QXzdJvq58Zco",
      "ELzkbNYyJkwSa3HTua5eZwIeqiDmJBbUEgQ1a0sHtld_",
      "EPoly9Tq4IPx41U-AGDShLDdtbFVzt7EqJUHmCrDxBdb"
    ],
    "bt": "4",
    "b": [
      "BNfDO63ZpGc3xiFb0-jIOUnbr_bA-ixMva5cZb3s4BHB",
      "BDwydI_FJJ-tvAtCl1tIu_VQqYTI3Q0JyHDhO1v2hZBt",
      "BGYJwPAzjyJgsipO7GY9ZsBTeoUJrdzjI2w_5N-Nl6gG",
      "BM4Ef3zlUzIAIx-VC8mXziIbtj-ZltM8Aor6TZzmTldj",
      "BLo6wQR73-eH5v90at_Wt8Ep_0xfz05qBjM3_B1UtKbC"
    ],
    "c": [
      "EO"
    ],
    "a": []
  }
```


- Provenant has staging witnesses that can be used for developer experiments, as long as usage is light:
  - http://witness1.stage.provenant.net:5631/oobi/BDno6jGtzjMdf5jvlo1qvbM8qIy6bSYb5xTPm5-2exLE/controller?name=prstage-1
  - http://witness2.stage.provenant.net:5631/oobi/BKDAV5YjMdBChiNAGrWH4CK8qVp22O-wbxxwAmbPyhO_/controller?name=prstage-2
  - http://witness3.stage.provenant.net:5631/oobi/BKaAZ4LI5XI-0j0aLvV-w3sRs51Y4JaR0i5m9fvCfTY9/controller?name=prstage-3
- W3C VCWG
  - Ongoing discussion https://github.com/w3c/vc-data-model/issues/947#issuecomment-1323051496
  - IIW backroom conversations to build support for compromises.
  - Net outcome: The proposal to break the strong association with Linked Data will be denied
  - One proposal was to rename the current group to "VC-LD" which has been rejected without a vote.
    - They are name squatting on the phrase "Verifiable Credential"
  - Sam proposed that the VC spec should be layered with an authentication, authorization and presentation layers underneath the payload.
    - The payload could then be a "bag of triples" if that's what you want.
- IIW
  - Update
    - Authentic Web manifesto talk needs further discussion and fleshing out. Notes incoming from Neil.
    - Interacting with Markus Sabadello and Stephen Curren to integrate ACDCs and KERI into Aries and DID Ecosystems.
      - Fixing did:keri method and did:keri resolver
    - CESRox Session
    - CESR for First Years
    - Extending DIDComm for general data exchange
    - Tao of the Trust Spanning Layer
    - Interop Status session and DIDCom Interop session - Roots wallet was involved.
    - How to become a QVI. Using the KERI/ACDC software in live demonstration.

        - DID method Death Match: Did:KERI 0:1 scale .99999 for KERI
        - AnonCreds anchor in a KERI KELS
- System Design Tradeoffs
    - SKWA vs Signify - *where is this information captured? Time for a short doc expanding on the tradeoffs?*
        - SKWA - if you have your own infrastructure (on prem) you use SKWA to authenticate against those agents.
            - Signing happens in the cloud
            - Access control to the agent service
        - Signify - with infrastructure hosted (custodial) in the cloud you can do signing in the client and protect the keys in the cloud. (Provides protection for the key holder and the service provider)
            - The only place the keys are in the clear is in the client.
            - All event heavy lifting happens in the cloud.
            - Keys are stored encrypted in the cloud.
            - Key generation and signing in the client
            - Key Storage, Event generation/validation, event signing in the cloud

2022-11-08

@ Neil Thomson

@ Samuel Smith

@ Phil Feairheller

@ Ruth Choueka

@ Henk van Cann

@ Joseph Lee Hunsaker

@ Steven Milstein

@ Kent Bull

@ Trent Larson

@ Shawn Butterfield

Click here for → Zoom meeting Nov 8

Agenda

- Announcements
    - Linux Foundation Open Wallet Initiative https://github.com/openwallet-foundation
- W3C VCWG
    - New issue raised to create an outer envelope that would contain a JSON-LD payload inside. Leaving room for other formats for the payload.
    - https://github.com/w3c/vc-data-model/issues/972
- IIW
    - vLEI Update
    - CESR for Muggles
    - Authentic Web
    - Becoming a QVI for vLEI
    - Organizational Identity
    - iXBRL Pilot ACDC VIRA
    - Technical Session on CESR/CESRox
    - Technical Session of ACDC
    - Technical Session on KERI Agent
    - Demo hour XBRL
    - Authentic Data
    - Propose Session on did:keri resolver

        - KERI Cardano Backer possible
- IPEX Protocol
    - Issuance and Presentation Exchange Protocol - A disclosure protocol.
        - Follows the principle of least disclosure. - The system should disclose only the minimum amount of information about a given party needed to facilitate a transaction and no more
    - Building in other mechanism beside (in addition to) selective disclosure to ensure control of the data
        - Partial Disclosure
            - Compactness
            - Chain-link Confidentiality
        - Selective Disclosure
            - 1
            - 2
    - Three Party Exploitation Model
        - First party - Discloser of data
        - Second party - Disclosee of data
        - Third party - Observer of data disclosed by First Party to Second Party
        - Second-Party Exploitation
            - implicit permissioned correlation
            - explicit permissioned correlation
            - explicit unpermissioned correlation with other second parties or third parties
        - Third Party Exploitation
            - implicit permissioned correlation
            - explicit unpermissioned correlation via collusion with second parties
        - Contractual anti-correlation commitment
    - Chain-Link Confidentiality
        - Based on paper: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045818
        - contractually links the disclosure of information to obligations to protect that information as the information moves downstream
        - chain contracts contain at leave three kinds of terms
            - obligations and restrictions on use
            - requirements to bind future recipients to same obligations
            - requires to perpetuate the contractual chain
    - Contractual Exchange
        - Disclosure provides non-repudiable Offer which includes terms or restrictions on use
        - Disclosee verifies Offer against composed schema and metadata adherence to desired data
        - Disclosee provides non-repudiable Accept of terms that are contingent on compliant disclosure
        - Discloser provides non-repudiable Disclosure with sufficient compliant detail.
        - Disclosee verifies Disclosure using decomposed schema and adherence of disclosed data
        - Disclose may now engage in permissioned use and carries liability as a deterrent against unpermissioned use
    - Exchange protocol:
        - https://weboftrust.github.io/ietf-ipex/draft-ssmith-ipex.html#name-exchange-protocol

2022-10-25

@ Samuel Smith

@ Kent Bull

@ Phil Feairheller

@ Henk van Cann

@ Neil Thomson

@ Rodolfo Miranda

@ Randy Warshaw

@ Shawn Butterfield

@ Daniel Hardman

Michal Pietrus

Ruth Choueka

@ Kevin Griffin

@ Joseph Lee Hunsaker

@ Mark Scott

Click here for → Zoom meeting Oct 25 2022

Agenda

- **Announcements**
  - **Daniel - Interesting debate in W3C, Let JSON be JSON. Debate over being forced to use JSON-LD and `@context`**
    - **https://github.com/w3c/vc-data-model/issues/947#issuecomment-1290600092**
    - **Almost identical to the same discussion about requiring JSON-LD in DIDDocs.**
    - **Proposal in the thread to evaluate alternatives on their technical merits... an opportunity to put forth ACDCs as an alternative**
      - **Term compatibility. Solution in DIDDoc spec was a registry for specification on how to convert between syntaxes.**
      - **DID Doc Spec solution is a registry of interoperable round trippable conversions between syntaxes (serialization)**
    - **Extensibility is Overrated.**
      - **Extensibility is the ability to ignore fields you don't care about.**
      - **Credential is evidence of entitlement. Driver license example... the license itself can just be the entitlement and the additional forensic information can be chained with ACDC as a follow on credential.**
      - **Developers are highly comfortable with that way of developing their features (looking at docs, inspecting return values and referencing the fields they need)… JSON-LD would instead require that developer to implement a data expansion library that takes an extra 2sec at runtime just to reason about the format/type/meaning of a property**
      - **JSON-LD is a dynamic look-up of a URL resource for VC schema. This is unstable as the URL resource may change without notice. A more stable model is schemas available for retrieval via a SAID for version specific and a Persistent Identifier for a version collection. This points to JSON-Schema to provide references to data schemas (via SAIDs and/or Persistent Identifiers) vs. JSON-LD**
    - **Layer semantic transformation on top of secure ACDCs with immutable, authentic schema.**
      - **OCA as an solution to this: https://humancolossus.foundation/blog/oca-v1-launch**
      - **https://oca.colossi.network/**
    - **When thinking about protocol design it is important to remember that the stack goes in reverse between presenter and verifier. And the verifier gets the data coming off the wire and needs to trust the data and the source of the data before you start processing the application layer aka, semantics.**
      - **As you work your way up the stack, the envelopes from the previous layers can be preserved and referenced in subsequent layers.**
      - **You need to keep the authentic envelopes to prove provenance of the data, this feature brought to you be end-verifiability**
    - **2 Ways ACDC can help W3C**
      - **ACDC provides a model - Immutable schema, append to extend, property graphs through chaining**
      - **ACDCs can be used as a layer below the WC3 data model. Use ACDCs as the authentic envelope around W3C verifiable credential.**
    - **Meeting on November 1st to discuss the Let JSON be JSON issue and come to a resolution**

- **As a community, we should all comment on the GitHub issue in W3C, (https://github.com/w3c/vc-data-model/issues/947)**
- **KERI and ACDC are IETF and if W3C is a big tent then great**
  - **We should make our arguments clear about WHY we favor this approach, not argue to force the W3C to change**
  - **Should be about adoption**

- **IPEX DEP**

2022-10-11

@ Kevin Griffin

@ Kent Bull

Click here for → Zoom meeting Oct 11 2022

Agenda

- **Announcements**
- **vLEI Compact Credentials review**

2022-09-27

Attendees

@ Samuel Smith

@ Kent Bull

@ Henk van Cann

@ Rodolfo Miranda

@ Neil Thomson

@ Joseph Lee Hunsaker

@ Lance Byrd

@ Randy Warshaw

@ Daniel Hardman

@ Mark Scott

@ Arshdeep Singh

Kyle Robinson

@ Trent Larson

@ Steven Milstein

@ P A Subrahmanyam

Click here for → Zoom meeting Sept 27 2022

Agenda

- **Announcements**

    - **W3C TPAC**
    - **Cardano Funded KERI Project**
        - **KERI Bridge for Cardano 3 month effort,**

- **IPEX Presentation Continued**

Minutes

- ACDC spec changes from 9-15-22 include:
    - Addition of DI2I unary operator: delegated issuer to issuer; expands class of allowed Issuer AIDs in ACDC nodes an edge resides in to include delegated AIDs which also implies that the ACDC node pointed to by the edge must be a targeted ACDC.
    - Tiered and Basic selective disclosure mechanism comments
    - A few explanatory comments and elaborations on existing material
    - Added a TODO for Append to Extend extensibility (discussed in today's meeting)
    - Clarified that the Registry Identifier is derived from the Issuer Identifier, an Autonomic Identifier (AID)
    - Many spelling, spacing, and grammar improvements
- Append To Extend discussion
    - ACDCs and SAIDS eliminated the need for a centrally controlled namespace registry for credential schemas.
- GLEIF vLEI Authorized Attestation Example explanation

Glossary explanation added 2022-09-27

collision, persistent data structure, graph fragment, registry, schema registry, domain, domain name

2022-09-13

Attendees

@ Samuel Smith

@ Kevin Griffin

@ Phil Feairheller

@ Rodolfo Miranda

@ Neil Thomson

@ Joseph Lee Hunsaker

@ P A Subrahmanyam

@ Mark Scott

@ Steven Milstein

@ Daniel Hardman

@ Vikas Malhotra

@ Lance Byrd

@ Randy Warshaw

Click here for → Zoom meeting Sept 13 2022

Agenda

- **Announcements:**
    - Sam presenting at W3C Sept 15 4:30 PT Introduction to ACDC
    - Daniel - Peer DID Spec question from DIF. Submitted a PR that adds to the top of DID Peer Method spec a

reference redirecting people to KERI
    - https://daniel-hardman.medium.com/response-to-kaliyas-being-real-post-13fddb9410f0
  - LinkedIn discussion regarding credentials with Kaliya -
    - https://github.com/decentralized-identity/peer-did-method-spec/pull/43/files
    - https://www.linkedin.com/feed/update/urn:li:activity:6975044750290657280/
- IPEX Specification
  - **https://github.com/WebOfTrust/ietf-ipex**

IPEX Presentation - Sam Smith

- Difference between issuance and disclosure. With issuance, the issuer is signing the data and "putting their name behind" the data.
  - ACDCs are called "data **containers**" because they are not always entitlements or authorizations. ACDCs are more general than credentials
    - This includes data attestations.
  - Issuance Exchange is defined as special case where the Discloser is the Issuer or the Origin ACDC
  - W3C definitions are not precise enough including the use of Subject in every credential
- Only one "origin vertex" in a disclosure chain. Calling this "Append-to-Extend".
  - No need to modify schema with custom fields. Just extend to a new bespoke ACDC. Eliminates vendor registries for namespaces.
- How do you provide proof of issuance
  - Issuance is proven by signing the SAID of the most compact version of the ACDC
- Compact Version of credentials - When a given field includes the SAID of the block instead of the full block.
- Issuer gets to decide the level of disclosure of the ACDC they are issuing by controlling the composability of the schema.
- ACDCs are analogous to Merkle Trees
  - Verification by verifying the signature on the root hash (SAID of most compact ACDC) and verifying the hashes down the DAG made up of the SAIDs of all the components
  - Allows all the variants to be disclosed and the proof still works.
- Why Proof-of-Disclosure?
  - It is essential to "contractually protected disclosure".
  - Engaged in a "bid-ask" exchange by signing what you are going to disclose, signing an agreement to contractual obligations then signing the final disclosure.

2022-08-30

Attendees

@ **Samuel Smith**

@ **Lance Byrd** **(RootsID) <lance.byrd@rootsid.com>**

@ **Kent Bull**

@ **Phil Feairheller**

@ **Kevin Griffin**

@ **Kevin Dean**

@ **Rodolfo Miranda**

@ **Daniel Hardman**

@ **Henk van Cann**

Click here for → Zoom meeting Aug 30 2022

Agenda

- **Announcements**
    - **ToIP Architecture Specification Draft**
        - **https://github.com/trustoverip/TechArch/issues/10**
- KERI -DIDComm
- NIST PostQuantum Finalists
    - Falcon
- The other Multi-Sigs
    - Software Threshold Multi-Sig
    - Threshold Signatures (Collective Signatures)
    - Endorsements (Notary)
        - Use Case Petition
        - Suggestion:
            - New signature attachment type CESR for group of attached endorser signatures
            - New REceipt message type for Endorsers of ACDCs or any other SAD not witnesses of Key event messages
                - Receipt on a SAID by an Endorser
- **IPEX Discussion**
    - **https://github.com/WebOfTrust/ietf-ipex**

2022-08-16

Attendees

@ **Samuel Smith**

@ **Lance Byrd**

@ **Joseph Lee Hunsaker**

@ **Henk van Cann**
@ **Phil Feairheller**
@ **Kent Bull**
@ **Kevin Griffin**
@ **Neil Thomson**
@ **Rodolfo Miranda**
@ **P Subrahmanyam**

Click here for → Zoom meeting Aug 16 2022

Agenda

- **Announcements**
    - **Cardano and KERI Bridge 4.92/5 rating on proposal**
    - **Glossary KERI ToIP (Daniel Hardman Tooling) Henk van Cann Doing work: Updated.**
    - **https://github.com/w3c/vc-data-model/issues/76#issuecomment-1211422037**
    - **https://github.com/w3c/vc-data-model/issues/895**
    - **Linux Foundation Open Wallet Foundation**
        - **Not proprietary Google, Apple, etc Mobile Wallet**
        - **Linux OS, MS OS, Mac/iOS? Android?**
        - **Jim St. Clair is organizing Meeting Reach out to him to ask for an invite to meeting.**
- **Items**
    - **w3c Authorized Issuer Lists**
        - **Thread on CCG list Manu Sporny create a list of authorized issuers Vested Authoritarian Sources**
        - **Why Not Trust Registries ToIP**
        - **ACDCs WebOfTrust RootOfTrust**
            - **Trust Anchors as the basis for the Web of Trust as a reputation system**
            - **vLEI GLEIF Governance**
            - **Canadian Standards Assoc (CSA)**

            - **Goverance Organization vetting , Trust Anchor**
            - **provenance**
        - **Consumer Reports**
- **New Auth Credential for vLEIs**
    - **GLEIF Root delegates GLEIF Ext AID. GLEIF Ext AID issues to QVI, QVI issues to LE, LE issues to QVI Auth to issue OOR, QVI Issues OOR to Person**
    - **Enforcement ex post facto via audit vs. upfront verifiability (audit free enforcement)**
    - **Replace manual authorization with ACDC role auth credential**
    - **Less Work**
        - **requirement in schema**
        - **minimizes impact Ghost Credentials (LE can revoke the auth credential which breaks the chain independent of action by the QVI to revoke)**
        - **Reduces trust transaction costs**
    - **AID contained and Role name**
- **IPEX Specification**
- **End State for Internet Security**
    - **Zero-Trust Architecture where every data item of import is signed in motion and at rest. Where signature is against an AID (autonomic ID)**
    - **Web of TRust on top**

2022-08-02

Attendees

@ **Samuel Smith**

@ **Lance Byrd**

@ **Henk van Cann**
@ **Phil Feairheller**
@ **Kent Bull**
@ **Kevin Griffin**
@ **Neil Thomson**
@ **Rodolfo Miranda**

Click here for → Zoom meeting Aug 2 2022

Agenda

- **Announcements**
    - **Transcribing IIW Demo CLI Demo of ACDC**
    - **SATP WG IETF**
- **Items?**
    - **GLEIF ACDC vLEI Credentials**
        - **moving toward production Q4 2022**
        - **Privacy Preserving Credentials for ECR credentials**
        - New Auth credential (is it per credential or blanket)
    - Issue ACDC expanding W3C DATA Model to allow ACDC compliant

        https://github.com/w3c/vc-data-model/issues/895

    - JWP JSON Web Proofs
        - Proposal IETF
            - single use signatures and hashes for selective disclosure and unlinkability using simplest most adoptable mechanism
            - which is same concept used by ACDC as minimally sufficient means for selective disclosure and presentation unlinkabili
    - Demo transcription
        - https://github.com/trustoverip/acdc/wiki

2022-07-19

Attendees

@ **Samuel Smith**

@ **Henk van Cann**

@ **Lance Byrd**

@ **Kent Bull**

Click here for → **Zoom meeting July 19 2022**

Agenda

Proof of Authority example

https://github.com/trustoverip/acdc/wiki/proof-of-authority#example-apc--book-rights-sold

- **ACDC XBRL Demo (Phil and Kevin)**

2022-07-05

Attendees

@ **Samuel Smith**

@ **Henk van Cann**

Click here for → **Zoom meeting July 5 2022**

Agenda

- **ACDC Spec**

  Continued Tiered selective disclosure

2022-06-21

Attendees

@ **Samuel Smith**

@ **Henk van Cann**

@ **Vikas Malhotra**

@ **P A Subrahmanyam**

Click here for → **Zoom recording June 21 2022**

Click here for → **Zoom recording June 21 2022** **(same? or is one of them the recording of June 7th?**

Agenda

- **ACDC Spec**
  - Review 3 party Exploitation Model
  - **Tiered Selective Disclosure**
    - **Which exploitation type to protect from and how**
    - **Minimally Sufficient Means**
      - **Adoptability**

2022-06-07

Attendees
@ **Samuel Smith**

@ **Kevin Griffin**

@ **Kevin Dean**

@ **Lance Byrd**

Neil Thomson

@ **Kent Bull**

@ **Steven Milstein**
Michal Pietrus

No Zoom recording available yet

Agenda

- **SAID Specification Issues (Kevin Dean)**
    - **https://github.com/WebOfTrust/ietf-said/issues/21**
- **ACDC Spec**
    - **Functional Privacy and Provisional Authenticity**
        - **https://www.windley.com/archives/2022/03/provisional_authenticity_and_functional_privacy.shtml**
    - **Rule Section**
    - **Bespoke Issued Disclosure**
    - **Selective Disclosure**
        - **Started**

2022-05-24

Attendees
@ **Samuel Smith**
@ **Kevin Griffin**
@ **Phil Feairheller**

@ **Kent Bull**

Click here for → **Zoom recording May 24 2022**

Agenda

- The ACDC edge section
- The ACDC rule section
- The Selective disclosure mechanisms

2022-05-10

Attendees

@ **Samuel Smith**

@ Phil Feairheller

@ **Kevin Griffin**

@ **Henk van Cann**

@ **Steven Milstein**

@ **Lance Byrd**

@ **Kevin Dean**

@ **Robert Mitwicki**

@ **Kent Bull**

Carly Huitema

Click here for -> Zoom recording May 10 20022

Agenda

- **IIW Presentations**
  - ACDC for Muggles https://docs.google.com/presentation/d/1mO1EZa9BcjAjWEzw7DWi124uMfyNyDeM3HuajsGNoTo/edit#slide=id.ga411be7e84_0_
  - ACDC for Wizards https://github.com/SmithSamuelM/Papers/blob/master/presentations/ACDC_Overview.web.pdf
  - CESR Proof Signatures: https://docs.google.com/presentation/d/1Kkzi0Ay97VLdlFFnYuxcQ2csPo6h6rCDxDkAJS7Q97c/edit?usp=sharing
  - ACDC for Automated Reasoning Reputation Systems https://github.com/SmithSamuelM/Papers/blob/master/presentations/AR_ACDC_Rep.web.pdf
  -

- ACDC for Dummies: https://blockchainbird.org/a/acdc/ so far only focus on SAIDs.
- Overlay Capture Architecture (OCA),e.g. layered verifiable credentials: oca.colossi.network

2022-04-26

No meeting this week because of IIW. See you at IIW.

2022-04-12

Attendees

@ **Samuel Smith**

@ Kent Bull

@ Phil Feairheller

@ **Henk van Cann**

@ **Kevin Griffin**

@ **Steven Milstein**

@ **Robert Mitwicki**

@ **Drummond Reed**

Click here for → Zoom meeting April 12 2022

Agenda

- **IIW Presentations**
  - **KEEP Demo vLEI ACDC (Early Draft)**

    - **ACDC Latest Draft Graduated Disclosure and Contractually Protected Disclosure**
    - **Continuation of What can you do with KERI - Issuing VLEI Credentials or ACDCS**
    - **CESR Proof Signatures event forwarding and ACDC**
    - **UX/UI Presentation on KEEP**
    - **Interoperability with VC Spec V2 attend or present**
- **Review Latest Draft ACDC Spec**

  https://github.com/trustoverip/tswg-acdc-specification

2022-03-29

Attendees

@ **Samuel Smith**

@ **Henk van Cann**

@ **Phil Feairheller**

@ **Robert Mitwicki**

@ **Neil Thomson**

@ **Lance Byrd**

@ **Kevin Griffin**

@ **Steven Milstein**

Click here for → Zoom meeting March 29 2022

Agenda

- **Review Latest Draft ACDC Spec**

  https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/ACDC_Spec.md

- **Issue on GitHub**

2022-03-15

Attendees

@ **Samuel Smith**

@ **Phil Feairheller**

@ **Lance Byrd**

Click here for → Zoom meeting March 15 2022

Agenda

- **GDPR Issues with ACDCs**
    - Article 17 of the GDPR which summarizing states:
        - Right of Erasure applies IF:
            - The personal data is no longer necessary for the purpose an organization originally collected or processed it.
        - Right of Erasure does not apply IF:
            - The data is being used to comply with a legal ruling or obligation.

- Performance-of-Contract = Compliance with a Legal Obligation:
    - One of the reasons that an organization collects PII is as part of a transaction (contract) such as a sale. In order to meet legal obligations for book-keeping, clearing, proof of ownership, receipt of sale etc associated with such a transaction the organization may keep a copy of said transaction details. Any transaction between two parties may be viewed as a form of contract especially if either or both parties incur obligations or exchange value as part of the transaction.
        - A commonly cited example are e-receipts. A company may request and keep an email address as PII in order to send an e-receipt but may not use the email address for marketing purposes unless specifically authorized.
        - Likewise if a sale or a product or service comes with a warranty then keeping PII associated with the warranty may be classified as “performance-of-contract” which is another way of describing compliance with a legal obligation.
    - Performance-of-contract is not dependent on continued consent during the lifecycle of the contract. In other words the contract itself is consent to keep the PII and lasts for the length of the lifecycle of the contract. i.e. the PII is needed in order to provide the product or service purchased or requested for the time you are obligated to perform the service or warranty the product. Performance of includes credit card chargeback and refunds.

      “The interesting thing about performance of a contract as a basis for processing data, is that it’s not dependent on continued consent if the use of the data is required for the product or service’s lifecycle (such as subscriptions, warranties or credit card chargebacks).
    - You still can’t use this data for any other purpose. But it’s much easier to prove you’re providing a good or service than proving that you have consent or dealing with consent withdrawals.”
-

  Right-of-Erasure Paradox:
-
    - A request to erase includes PII. But keeping the right of erasure request means keeping the PII. But without the PII in the right of erasure request there is no way to ensure that erasure persists. A new copy of the erased data may be added without knowing that it was erased.
    - The legal obligation to comply with a right of erasure request should be reason enough to keep the right of erasure request including the necessary PII to ensure performance of contract and not erase it. Only the PII not directly related to the right of erasure transaction may be kept. The performance of contract in this case is the erasure of PII. The service you have requested (erasure of PII) can't be provided unless I have enough PII to ensure that I have correctly erased the PII you have requested. If the request for erasure is indefinite (i.e. erased for all time) the the lifecycle of the contract erasure request is also indefinite. This could mean therefore that a cryptographic digest of the PII being erased could be maintained indefinitely as a performance of contract to ensure that the exact PII is never un-erased because the check against the digest for any new data stored would match the digest. Without the digest there is no way to ensure performance of contract.

- **Draft Specification HackMD Review**
    - **https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/ACDC_Spec.md**
- **Revised labels and sections due to selective disclosure mechanisms and better clarity on schema as type.**
    - **Composed schema**
    - **@Robert Mitwicki comment: We must include in the specification a prohibition of using schema references in ACDC JSON Schema (links to external websites).**
- **Chain link confidentiality exchange**
    - **Offer with verifiable metadata with terms. Partial disclosure**
        - **verify with Composed Schema**
    - **Accept terms**
    - **Full Disclosure**
        - **verify with decomposed schema**
- **Exploitation Model as the basis for selective disclosure**
    - **first party (discloser)**
    - **second party (disclosee)**
        - implicit permissiond correlation
        - **explicit permissioned correlation**
        - **malicious (explicit unpermissioned correlation)**
    - **third party (observer)**

        - implicit permissioned correlation
        - **explicit unpermissioned correlation via collusion**
- **Note: Meeting went for 2 hours and was fully recorded. If you were only able to attend the first hour make sure to watch the second hour. We covered the spec in detail in the second hour.**

2022-03-01

Attendees

@ **Samuel Smith**

@ **Kevin Griffin**

@ **Phil Feairheller**

@ Steven Milstein

@ Robert Mitwicki

@ Drummond Reed

Click here for → Zoom meeting March 1 2022

Agenda

- **New IETF spec repo**
    - **https://github.com/trustoverip/tswg-acdc-specification**
    - **IETF License and Apache2 license**
- **3/01**
- **Spec Writing**
    - **Target IETF Internet Draft by IIW Late April 24,-26**
        - **Kevin Dean OCA Overlay**
            - **Haystacks Overlay**
        - **Informative Section vLEI examples first production use of ACDC @phil Feairheller**
        - **TBD**
- **KERI IPR**
- **Attestation vs Authorization ACDCs (add as informative example)**
    - **Pharmaceutical Use Case Authorization and Attestation ePI Suggest use as seminal example for ACDC**
    - **Counterfeiting protections Provenance chain Supply Chain**
    - **Wallet construction for attestion can be much simpler than wallet construction**
        - **Portable attestations cached**
- **Compact and Confidential Credentials**
- **Conditional Schema for SAID, SAD validation**

2022-02-14

Attendees

@ **Samuel Smith**

@ **Kevin Griffin**

@ **Phil Feairheller**

@ Kevin Dean

@ arthur greef

@ Henk van Cann

Rodolfo Miranda

@ Steven Milstein

Click here for → Zoom meeting Feb 14 2022

Agenda

- **New IETF spec repo**
  - **https://github.com/trustoverip/tswg-acdc-specification**
  - **IETF License and Apache2 license**
- **Proposed new bi-weekly meeting time**
  - **Tuesday 3 p.m UTC, 8 a.m. MT, 10 a.m. ET, 4 PM CET,**
    - **Change calendar invite to new time.**
- **Spec Writing**
  - **Target IETF Internet Draft by IIW Late April 24,-26**
    - **Kevin Dean OCA Overlay**
      - **Haystacks Overlay**
    - **Informative Section vLEI examples first production use of ACDC @phil Feairheller**
    - **TBD**
- **RI field moved and GLEIF schema and vLEI changes**
- **Ricardian Contracts in Issuance and Presentation Exchange**
- **Compact and Confidential Credentials**
- **Conditional Schema for SAID and Data validation**

2022-01-31

Attendees

@ **Samuel Smith**

@ **Kevin Griffin**

@ **Phil Feairheller**

@ **Kevin Dean**

@ **arthur greef**

@ **Henk van Cann**

@ **Robert Mitwicki**

Click here for → Zoom Meeting January 31 2022

Agenda

- **Update on Repo setup IETF for draft spec (@ Drummond Reed)**
  - **IETF directed project or task force within ToIP uses IETF format template for spec**
  - **What about W3C. Approach is to have interoperability profile of IETF/TOIP ACDC and VC v2 Big Tent**
  - **Brent Zundel who is the Chair of w3c VC spec 2 intent is to big tent**
- **Make assignments for section to write**
- **Arthur Cardano Goals**
  - **IOG Cardano Circular Economy Ecosysm (Input Output Global) Own the Prism SDK write software for Cardano**
  - **Prism SDK uses Merkle Tree for Identity store on Cardano**
- **Ricardian Contracts in Issuance and Presentation Exchange**
- **Compact and Confidential Credentials**
- **Conditional Schema for SAID and Data validation**

2022-01-17

Attendees

@ Samuel Smith

@ Kevin Dean

@ Henk van Cann

@ Phil Feairheller

@ Drummond Reed

Click here for → Zoom meeting January 17 2022

Agenda

- **Finalize draft spec for ACDC**
    - **ToIP to use IETF Templates @ Drummond Reed to do**
    - **New repo to replace existing repo to be templatized for ietF fomat draft @ Kevin Griffin**
- **Exchange protocols**
    - **should we combine the issuance and exchange protocols into one spec**
        - Background (WACI PEX)
        - ACDC
            - KERI Compatible Exchagne Message
            - Transposable Signatures with Signature Pathing
        - Suggestion @Drummond that the specs should be recognized as common related spec so Start as one spec
        - Resolved: Combine the two into one spec Issuance and Presentation Exchange Protocol
            - MUST support other transports besides HTTP such as UDP base TCP etc.
            - MUSt support both Solicited and Unsolicited Initiation
                - waiver and consent make issuance and presentation similar with contract terms in the exchange
        - **Issuance Exchange**
        - **Presentation Exchange**
        - **Both Solicited and Unsolicited Initiation of either protocol**
    - **DIDComm3 co-protocols impact on these protocols?**

2022-01-03

Attendees

@ Samuel Smith

@ Kevin Dean

Zoom recording not yet available.

Agenda

- **Dicuss ACDC and GS1**

2021-12-20

Attendees

@ **Samuel Smith**

@ **Henk van Cann**

@ **Kevin Dean**

@ **Vikas Malhotra**

@ **Phil Feairheller**

@ **Drummond Reed**

@ **Kevin Griffin**

Click here for →

Agenda

- **ACDC Spec Roadmap**
- **How to replace the role authority of a issuer in an ecosystem with ACDC once they have left the ecosytem (Kevin Dean)**
- **Pre-Rotation vs HDK**
- **ACDC CESR SAD Pathing**

2021-12-06

Attendees

@ **Samuel Smith**

@ **Phil Feairheller**

@ **Kevin Griffin**

@ **Henk van Cann**

Steven Milstein

@ **Darrell O'Donnell**

@ **Kevin Dean**

@ **Scott**

Agenda

- Continue GS1 notional application of chained credentials as ACDCs (Kevin Dean)
- IETF CESR Internet Draft
- IETF CESR Proof Format for ACDC with SAD Pathing
- Holiday Schedule (No changes regular schedule)

2021-11-22

Attendees

@ Samuel Smith

@ Kevin Dean

@ Kevin Griffin

@ Drummond Reed

@ Brent Zundel

@ Steven Milstein

@ Phil Feairheller

Agenda

- Review W3C Charter for V2.0 ACDC inclusion (Brent Zundel)
- Review GS1 notional application of chained credentials as ACDCs (Kevin Dean)
- Holiday Schedule

2021-11-08

Attendees

- @ Kevin Dean - GS1
- @ Samuel Smith
- @ Kevin Griffin
- Henk van Cann
- @ Steven Milstein
- @ Phil Feairheller
- @ Drummond Reed
- @ Robert Mitwicki
- @ Brent Zundel

Announcements

- @ **Drummond Reed** thought it worth bringing the Own Your Own DID (did:oyd) method spec to the TF's attention—it appears to be a simple form of a KERI Event Log.

ACDC Spec List

- Status of Version 2 Charter of W3C VC spec (Brent Zundel)
    - Scope of charter use cases. Good News.
        - In scope includes a complete revision replacement of current spec. ACDC is in scope for the charter so no reason not to be in scope.
        - Need people to participate in V 2.0 WG.
        - Immediate action item is for us to review charter to clear enough to include ACDC work.
    - Bad news. Because status of DID spec approval timeline is uncertain. This makes the next version of VC spec timeline uncertain.
    - https://github.com/w3c/vc-wg-charter
- Congrats—the table on our home page has a number of new spec entries.
- Review of the ACDC spec.

2021-10-25

Administration

- Review IIW
    - session attendance good

Review ACDC

Other

2021-10-11

Administration

- We discussed filling in the rest of the Deliverables table on the ACDC home page.

ACDC Sessions

- Proposed sessions
  - GLEIF vLEI Business T S1
  - GLEIF vLEI: Demo T S2 Distributed Multi-Sig Chained Credentials using KERI and ACDC — @ Phil Feairheller and @ Kevin Griffin
  - MicroLedger Four Provenance Logs Authentic Data EcoSystem T S3 @ Robert Mitwicki
  - What is ACDC? T S4— @ Samuel Smith
    - KERI and ACDC Technical Session
    - Covers all the contributing specs @ Samuel Smith
- Related Sessions
  - Introduction to KERI W @ Drummond Reed
  - Practical Introduction to KERI: How Can I Actually Use it Today?W @ Phil Feairheller @ Kevin Griffin (Command Line Tools with KeriPy)
  - Systems Design PAC Theorem Privacy Authenticity Confidentiality Tradespace W Th @ Samuel Smith
  - Secure Attribution with KERI: How it Fixes the Broken Internet W Th — @ Samuel Smith
  - Zero Trust Data Management BADA RUN vs CRUD: discovery and authorization mechanisms W or Th @ Samuel Smith

2021-09-27

Administration

- We need to complete the final Lead Author assignments in the Deliverables table on the ACDC home page (<5 mins)— @ Samuel Smith
- We quickly cleaned up the table so that all specs have lead authors.

Terminology

- ACDC Terms Wiki— @ Drummond Reed
- @ Steven Milstein reminded us that @ Daniel Hardman already set up an ACDC terms wiki at https://github.com/trustoverip/acdc-tf-terms/wiki
- @ Drummond Reed suggested that it be simplified to "acdc-terms/wiki".
- DECISION: We should revise this terms wiki to use the name "acdc-terms".
- ACTION: @ Drummond Reed to contact @ Daniel Hardman to rename the repo.

Compact Label Normalization

- Future KERI change to use SAIDs Revised labels for ACDC that are normalized @ Samuel Smith
- See screenshot #1 below.

Microledger

- **@ Robert Mitwicki**
- He gave an explanation of microledgers based on a spec being developed at the Human Colossus Foundation— see screenshots #2 and #3 below.
- It generalizes the idea of a KEL (key event log).
- @ Samuel Smith agreed that the generalization of event logs is a good idea. His only concern is that when it is generalized, it becomes much easier to make security mistakes. That's why the KERI and ACDC specs are much tighter.
- @ Robert Mitwicki is planning to give a session at IIW on microledgers.

Screenshots (for notes above)

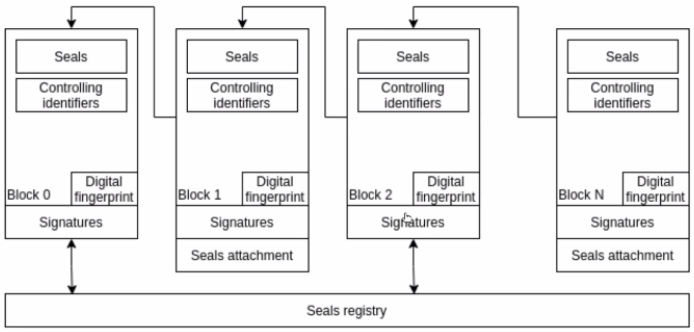
#1

```
{
  "v": "ACDC10JSON00011c_",
  "d": "EBdXt3gIXOf2BBWNHdSXCJnFJL5OuQPyM5K0neuniccM",
  "i": "did:keri:EmkPreYpZfFk66jpf3uFv7vklXKhzBrAqjsKAn2EDIPM",
  "s": "E46jrVPTzlSkUPqGGeIZ8a8FWS7a6s4reAXRZOkogZ2A",
  "a": {
    "d": "EgveY4-9XgOcLxUderzwLIr9Bf7V_NHwY1lkFrn9y2PY",
    "i": "did:keri:EQzFVaMasUf4cZZBKA0pUbRc9T8yUXRFLyM1JDASYqAA",
    "dt": "2021-06-09T17:35:54.169967+00:00",
    "ri": "did:keri:EymRy7xMwsxUelUauaXtMxTfPAMPAI6FkekwlOjkggt",
    "LEI": "254900OPPU84GM83MG36",
    "t": [
      "VerifiableCredential",
      "LegalEntityvLEICredential"
    ]
  },
  "p": [
    {
     "qualifiedvLEIIssuervLEICredential": {
      "d": "EIl3MORH3dCdoFOLe71iheqcywJcnjtJtQIYPvAu6DZA",
      "i": "Et2DOOu4ivLsjpv89vgv6auPntSLx4CvOhGUxMhxPS24"
     }
    }
]
}
```

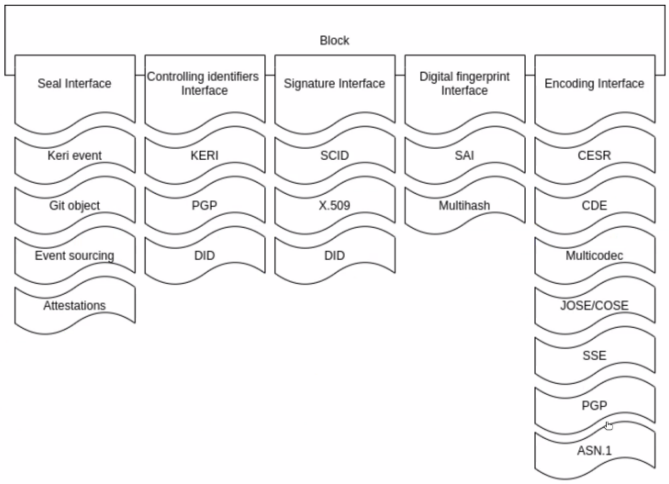

#2

Concept

Microledger consists of fundamental building blocks called blocks. Each next block is bound to the previous block by including its cryptographic digest content.



#33



GLEIF VLEI update @ **Phil Feairheller**

ACDC Sessions

- Proposed sessions
  - GLEIF vLEI: Distributed Multi-Sig Chained Credentials using KERI and ACDC — @ Phil Feairheller and @ Kevin Griffin
  - What is ACDC? — @ Samuel Smith
    - KERI and ACDC Technical Session
    - Covers all the contributing specs
  - Why ACDC? (And Why Not _____?) — @ Robert Mitwicki
    - This would include A Feature Comparison Table
  - Secure Attribution with KERI: How it Fixes the Broken Internet — @ Samuel Smith
  - Practical Introduction to KERI: How Can I Actually Use it Today?
- Related Sessions
  - GLEIF vLEI
  - Zero Trust Data Management BADA RUN vs CRUD: discovery and authorization mechanisms @ Samuel Smith
  - MicroLedger @ Robert Mitwicki

<next>

2021-09-13

Brief update on wiki page reorg— @ **Drummond Reed**

- Meeting page has been broken out into a standalone page (this one)
- A table of deliverables has been added to the ACDC home page
  - We should be sure this table is complete and kept current

IIW Strategy: Daniel Hardman

- Daniel: How many sessions would we like at IIW?
- Sam: one session per day
- Daniel: in previous IIWs, Sam had done 2-3 sessions per day
- Sam: plan on one per day, and then possibly have a second one
- Robert: have one technical session, and one non-technical session focused on use cases and business cases
  - Data flows, data supply chain, product supply chain

        - For example, GS1 has very specific requirements that the KERI family of specs can meet
    - Daniel: can we develop a spreadsheet showing a classic product comparison table (similar to what the DIF DIDComm WG has created for DIDComm & HTTP(S))
        - Robert liked the idea of the table being something that stresses the business
        - ACTION: @ Robert Mitwicki will prepare a draft of a feature comparison table before our next meeting.
        - ACTION: @ Drummond Reed to talk to @ Brent Zundel about a session about VC V2 at IIW
    - Proposed sessions
        - GLEIF: Distributed Multi-Sig Chained Credentials using KERI and ACDC — @ Phil Feairheller and @ Kevin Griffin
        - What is ACDC? — @ Samuel Smith
            - KERI and ACDC Technical Session
            - Covers all the contributing specs
        - Why ACDC? (And Why Not _____?) — @ Robert Mitwicki
            - This would include A Feature Comparison Table
        - Secure Attribution with KERI: How it Fixes the Broken Internet — @ Samuel Smith
        - Practical Introduction to KERI: How Can I Actually Use it Today? -

ACDC Specification Strategy: Daniel Hardman

- SAID spec—Sam Smith
- IXP spec—Phil Feairheller
- PXP spec—Phil Feairheller
- PTel spec—Phil Feairheller
- CESR spec—Sam Smith
- CESR proof spec—Phil Feairheller
- AID spec—Sam Smith
- ACDC spec—Sam Smith
- SIS spec—Robert Mitwiki
- ACTION: @ Drummond Reed to update the ACDC home page deliverable table with these leads

General Discussion:

- Suggestion is that KERI is too large to be a single spec, so break it into smaller specs.
- For example, CESR can be broken out into a separate composable serialization spec.
- And you separate out identifier specs.
- Once you take the identifier formats and composable streaming format out, then KERI becomes a definition of events.
- We also talked about the future of the W3C Verifiable Credentials spec— @ Brent Zundel is working on the charter for the V2 Working Group
    - What is being discussed is the possibility of the new WG taking a "Big Tent" approach
    - In that case, ACDC would be one of the "branches" or "options" or "families" of a W3C VC V2 compliant
    - The big question is whether others that would be in that big tent would be tolerant (or even welcoming) of having the ACDC family under the tent
- Sam brought up the question of how KERI and ACDC deal with dynamic data
    - DIDs and DID documents try to be dynamic and VCs try to be dynamic, but neither does it with strong security
    - KERI and ACDC have a way of handling dynamic data with a zero-trust security model
    - Robert talked about how KELs can essentially act as microledgers ("single node blockchains") to trace the changes in state to any kind of data set
    - Sam agreed to you need both authentity, monotinicity, and protection from replay event logs
        - DID docs use the CRUD model
        - This requires using the RUN model (Read, Update, Nullify)
- ACTION: @ Drummond Reed to ask Elisa to change the ACDC meeting to auto-record

2021-08-30

Details of how GLEIF is using ACDC and associated specs. Placeholder spec repositories at https://github.com/WebOfTrust

Specs WoT

KeyStorage keeping.py module Manager and Keeper classes encrypted secrets

vLEI Credentials rely on the following specifications:

1. JSON Required https://datatracker.ietf.org/doc/html/rfc7159
2. JSON Schema Version 2020-12 https://json-schema.org/draft/2020-12/json-schema-core.html
3. Composable Event Streaming Representation (CESR) Specification https://github.com/WebOfTrust/cesr
4. Attributable Identifiers (Autonomic Identifiers, AIDs,SCIDs) for Issuers and Holders using the did:keri Method (secure attribution) https://github.com/WebOfTrust/aid
5. KERI Decentralized Identifiers (AIDs) did:keri Specification https://github.com/WebOfTrust/did-keri
6. Self Addressing Identifiers (SAIDs) https://github.com/WebOfTrust/said
7. Schema Immutability Specification (SIS) https://github.com/WebOfTrust/sis
8. Composable Event Streaming Representation (CESR) Proof Format https://github.com/WebOfTrust/cesr-acdc-proof
9. ToIP Authentic Chained Data Container (ACDC) Specification https://github.com/trustoverip/TSS0033-technology-stack-acdc
    a. (Informative) JSON required as defined in https://www.w3.org/TR/vc-data-model/#json
        i. Exception @context MUST NOT be included.
10. Issuance Exchange Protocol Specification for ACDC and KERI (Key Event Receipt Infrastructure)
11. Presentation Exchange Protocol Specification for ACDC and KERI
    a. WACI PEx https://github.com/decentralized-identity/waci-presentation-exchang
12. Public Transaction Event Log (PTEL) Specification

Core Components of KERI Robert Mitwicki

Key Provanance Log -> KEL
Self-Certifying Identifier -> SCI, keri prefix
Self-Addressing Identifier → SAI
General purpose registry -> TEL
Secure communication proctocol CESR/DIDComm?
Self Describing cryptograhic material encoding - CESR/Multicodec/CDE/JOSE/COSE
Key Storage

Relationship between ACDC and W3C VC 2.0 (Daniel Hardman)

Not RDF Triples

Compact IoT credentials

Futures:

Collaborate W3C VC Big Tent

Go our own way with ToIP/IETF ACDC

Suck the Air Strategy ToIP/IETF ACDC

2021-08-16

OCA as a SAID based Schema Immutability specification

More details on ToIP glossary wiki facility

HCF working with ESSIF on Rules section of ACDC https://github.com/decentralised-dataexchange/automated-data-agreements

2021-08-02

Issues with security privacy suggested pull request (Daniel Hardman)

Terminology (Daniel Hardman)

- How to formally manage terminology in Specs: (Other group) create terms wiki
- GitHub.com/trustoverip/acdc-tf-terms/wiki/ Create new page
- Glossary may be auto-generated from the wiki using the TT tool. (python)

Order of creation of SAIDs (Daniel Hardman)

Degree of Saidification (Sam Smith)

Continue discussion on Schema and SAIDs

IGrant Data Agreement with ACDC (Robert Mitwicki)

GLEIF ACDC vs VC models

LPG model

Calendar of ToIP Meetings

2021-07-19

Continue discussion on Schema and SAIDs

LPG model

2021-06-28

Alignment with VC data model

Multiple Endorsers

Continue discussion on Schema and SAIDs

2021-06-21

Phil talk about JSON Schema and SAID

Change meeting time ?

Proof signature

Alignment with VC data model

Multiple Endorsers

2021-06-07

discussed and refined example in index.md of draft spec. Decided that certain blocks in VC MUST use SAI (self addressing identifiers) so that can reason about the data using the identifier.

This allows compactness and secure universal verifiability. Either the block is explicitly included or instead of the block a SAID.

The schema is nested with SAI blocks for the corresponding blocks in the VC

schema of data payload

schema of rules

2021-05-17

Write spec outline

Abstract Model

Two concrete implementations. One VC Linked-Data with schema.org with security caveats, the Other JSON and immutable JSON-Schema

Example Spec Outline

https://w3c-ccg.github.io/vc-json-schemas/

Abstract

Introduction

Terminology

Specification
- Overview
  - Security
  - Guarantees
  - Storage
  - Versioning
- Definition

Versioning Guidelines
- Revision
- Model

Extensibility

Examples
- Verifiable Credentials

Drawbacks

Alternatives

Security & Privacy Considerations

Interoperability
- Security
- Semantics

Index
- Terms defined by this specification

References
- Informative References

https://github.com/trustoverip/WP0035-decentralized-resource-identifiers

High-Level Summary

Abstract

Motivation

Scope

Problem Statement

Solution

References

2021-05-10

Semantic inference and reasoning under uncertainty

https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/VC_Enhancement_Strategy.md

Work Item for next week write spec outline

2021-03-26

OCA (Overlays Capture Architecture) @ Robert Mitwicki (input and semantic WG at ToIP) standard

Deck: https://docs.google.com/presentation/d/17DS11jHQm3jGAUXCNwP5qFUBJrw7tcKiSGMgH2k0giA/edit?usp=sharing

OCA Article: https://humancolossus.foundation/blog/cjzegoi58xgpfzwxyrqlroy48dihwz
OCA editor: https://editor.oca.argo.colossi.network/
OCA spec draft: https://github.com/the-human-colossus-foundation/oca-spec

JSON-LD Security EndState Sam

Proposal Identifiers Sam

MetaDiscussion Daniel

RoadMap

Hypothesis

Continue Discussion

Notes about ADC and its structure: https://hackmd.io/RX8ZAycxQhSpGZgBfRzqbg

2021-03-01

Data Item Model

Authentic Data Item = Attestation

Data Controller ID: DID namespace controller

Attestation ID: (in order to reason with data)(IETF RATS Alignment) ID of the Attributable Item Attestion.

Derived DID from DID namespace

Derived from Data Item Content (such as https://iscc.codes)(correlate attestations)

Verifiable Registry of Data Item

Data Attributes:{NonAuthentic Attributes}

Data Controller Signature on Data Item: (nonredudiable, integral)

Data Mesh Meetup

2021-03-01

MKDocs GitHub

https://github.com/trustoverip/TSS0033-technology-stack-acdc

https://tools.ietf.org/html/draft-ietf-tls-subcerts-10

Delegation chain separate from identity chain

hiding part of the chain

privacy in both direction walking back up to the root and privacy walking down from the root

2021-02-15

Followup on getting repo setup in MkDocs

Use Cases Selected:

Supply Chain (Mitwicki)

GLEIF (Smith and Reed)

Delegation (Hardman)

Data Source Provenance (Hardman and Smith)

IoT (Hardjono)

Next task

Create proposals for chaining semantics with syntax. (assume Verifiable Credential Based)

Express each use case in each chaining proposal.

Iterate on proposals.

Open Question:

Syntax should at least support Trees and DAGs (Directed Acyclic Graphs) not merely linear chain

Should syntax also support cyclical graphs.

2021-02-01

Finalize choice of MkDocs vs SpecUp: Decided on MKDocs:

Action Item: Sam work with TOIP to setup GitHub repo with MkDocs

EiDas Links: (See 2021-02-01) Robert Mitwicki. Discussion of SSI etc in EiDAS

Relation to Legal Framework for Digital Signatures

https://en.wikipedia.org/wiki/Electronic_signatures_and_law

https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-sign-us-guide-e-signatures-wp-ue.pdf

UETA https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034

ESIGN Act https://www.fdic.gov/regulations/compliance/manual/10/X-3.1.pdf

EiDAS

Advanced Electronic Signature Qualified Electronic Signature Notaries with Certificate = Handwrittern Signature

Review Use Cases:

Semantic Containers: Pauls Knowles Semantic Container. Nested Forms. Consent.

Distinguish between different types of containers as part of specification for ACDC

2021-01-18

Action Item Robert Mitwicki add information on EIDAS regulation allows for linking.

- eIDAS: https://en.wikipedia.org/wiki/EIDAS
- eIDAS SSI bridge: is a pilot focusing on providing a cross-border identity solution compliant with the *eIDAS* trust framework:
  https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about
- Related links:
  https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI
  https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf
  https://en.wikipedia.org/wiki/Advanced_electronic_signature
  https://ssimeetup.org/introducing-ssi-eidas-legal-report-ignacio-alamillo-webinar-55/
  https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification
  https://oneflow.com/blog/what-makes-electronic-signature-legal/
  https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0.pdf
  https://www.cencenelec.eu/news/brief_news/Pages/TN-2019-049.aspx

Discussed CCG Meeting on ZCap vs VC Authorization

Discussed Use Cases

MkDocs vs Spec Up (Tables?)

Action Item Sam review and present at next meeting

2021-01-04

Use Case Summaries

GLEIF vLEI https://hackmd.io/dlnfd8xOSqmD90v4Y6mzFQ (Sam Smith ProSapien)

Supply Chain https://hackmd.io/vYztT346RC-m34aVmFB7vg (Robert Mitwiki Human Colossus)

Global ID for life https://hackmd.io/vYztT346RC-m34aVmFB7vg (IdNum - Robert)

Digital Immunization Passport https://hackmd.io/vYztT346RC-m34aVmFB7vg (Robert)

Authorizations for Encrypted Backups use_case.md (Charles Cunningham Eugeniu Rusu Jolocom)

Guardianship Chain of Credentials (Evernym Daniel and Drummond)

Delegating Access to Rented Car (Evernym)

Provenancing Inherited Attributes (Daniel Hardman Evernym ProSapien)

Delegation of Certification Authority PKI Certificate Like Chaining (Ned Smith Intel)

Object Capabilities Like Authorizations (See authorizations for encrypted backups)

Critical Supply Chain Provenancing (Carsten Stoecker Spherity)

Open Accredited Market Participation Energy Market (Jolocom)

Provenance Virtuous Supply Chains Conscious Consumers Demand Pull

Data Supply Chain Provenance

Data Supply Chain Consent Provenance Consented Data Privacy (Samuel Smith ProSapien)

Content Distrubution Networks (copyright, acknowledgement, usage, attribution) (Thomas Hardjano MIT)

IoT Onboarding Devices (Ned Smith Intel, Thomas Hardjano MIT)

Attestation Chaining

Anonymized Data Chains - https://hackmd.io/vYztT346RC-m34aVmFB7vg

Representing business processes/entity lifecycles with SSI - Representing Lifecycles of Entities using States + SSI.pdf

Attribution Chaining Semantic Super Semantic

Secure Attribution of statement to controller of a decentralized identifier

A securely attributed chaining statement links two securely attributed statements together

A chaining statement is a special case statement whose semantics are to securely linked by attribution.

This chaining may be applied recursively.

The chained statements that are not chaining statements may convey sub-semantics such as authorization, delegation, attestation, provenance, etc.

Attribution Verification Types: Nonrepudiable Signatures. ZKPs. Anonymized Data.

Certificate Result Certification

Certifying the result of a decision

Verifiable Algorithm

CoSWID Tags IETF

No labels