Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 19 December 2025

D. Hardman
Provenant, Inc

17 June 2025

Verifiable Voice Protocol
draft-hardman-verifiable-voice-protocol-03

Abstract

Verifiable Voice Protocol (VVP) authenticates and authorizes organizations and individuals making and/or receiving telephone calls. This eliminates trust gaps that malicious parties exploit. Like related technolgies such as SHAKEN, RCD, and BCID, VVP can bind cryptographic evidence to a SIP INVITE, and verify this evidence downstream. VVP can also let evidence flow the other way, proving things about the callee. VVP builds from different technical and governance assumptions than alternatives, and uses stronger, richer evidence. This allows VVP to cross jurisdictional boundaries easily and robustly. It also makes VVP simpler, more decentralized, cheaper to deploy and maintain, more private, more scalable, and higher assurance. Because it is easier to adopt, VVP can plug gaps or build bridges between other approaches, functioning as glue in hybrid ecosystems. For example, it may justify an A attestation in SHAKEN, or an RCD passport for branded calling, when a call originates outside SHAKEN or RCD ecosystems. VVP also works well as a standalone mechanism, independent of other solutions. An extra benefit is that VVP enables two-way evidence sharing with verifiable text and chat (e.g., RCS and vCon), as well as with other industry verticals that need verifiability in non-telco contexts.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://dhh1128.github.io/vvp/draft-hardman-verifiable-voice-protocol.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-hardman-verifiable-voice-protocol/.

Source for this draft and an issue tracker can be found at https://github.com/dhh1128/vvp.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

When we get phone calls, we want to know who’s calling, and why. Often, we want similar information when we _make_ calls as well, to confirm that we’ve truly reached who we intend. Strangers abuse expectations in either direction, far too often.

Regulators have mandated protections, and industry has responded. However, existing solutions have several drawbacks:

* Assurance of callers derives only from the signatures of originating service providers, with no independently verifiable proof of what they assert.

* Proving the identity of the callee is not supported.

* Each jurisdiction has its own governance and its own set of signers. Sharing information across boundaries is fraught with logistical and regulatory problems.

* Deployment and maintenance costs are high.

* Market complexities such as the presence of aggregators, wholesalers, and call centers that proxy a brand are difficult to model safely.

* What might work for enterprises offers few benefits and many drawbacks for individual callers.

VVP solves these problems by applying three crucial innovations.

1.1. Evidence scope

Existing solutions aim to assert variable levels of confidence about a caller’s identity, plus possibly some brand attributes. These assertions rest entirely on a service provider’s judgment and are testable only in the moment a call is initiated; later, they become repudiable.

VVP proves more. It always proves the legal identity of whoever presents evidence, plus any authority that they have delegated to staff and service providers. It typically also proves brand attributes and right to use a phone number. If a call center and/or an AI is involved, it proves the constraints under which that entity operates as a representative. Depending on how it is used, VVP can thus achieve very high levels of assurance about a broad range of facts related to callers, callees, or both.

All VVP proof is traceable back to justifying evidence and can be evaluated in the present or the past. This guarantees accountability for all parties with a permanent, non-repudiable audit trail.

1.2. Evidence format

VVP is rooted in an evidence format called _authentic chained data container_s (_ACDC_s) -- [TOIP-ACDC]. Other forms of evidence (e.g., JWTs/STIR PASSporTs, digital signatures, and optional interoperable inputs from W3C verifiable credentials [W3C-VC] and SD-JWTs [SD-JWT-DRAFT]) also contribute. However, the foundation that VVP places beneath them is unique. For a discussion of the theory behind VVP evidence, see 10. For more about additional evidence types, see 6.2 and 7.

Because of innovations in format, VVP evidence is easier to create and maintain, safer, and more flexible than alternative approaches. It also lasts much longer. This drastically lowers the costs of adoption.

1.3. Vetting refinements

Although VVP interoperates with governance frameworks such as SHAKEN [ATIS-1000074], it allows for a dramatic upgrade of at least one core component: the foundational vetting mechanism. The evidence format used by VVP is also the format used by the Verifiable Legal Entity Identifier (vLEI) standardized in [ISO-17442-3]. vLEIs implement a KYC approach advocated by the G20's Financial Stability Board, and overseen by the G20's Regulatory Oversight Committee. This approach follows LEI rules for KYC ([ISO-17442-1]), and today it's globally required in high-security, high-regulation, cross-border banking.

Millions of institutions have already undergone LEI vetting, and they already use the resulting evidence of their organizational identity in day-to-day behaviors all over the world. By adopting tooling that's compatible with the vLEI ecosystem, VVP gives adopters an intriguing option: _just skip the task of inventing a whole new vetting regime unique to telco, with its corresponding learning curve, costs, and legal and business adoption challenges._

To be clear, VVP does not _require_ that vLEIs be used for vetting. However, by choosing an evidence format that is high-precision and lossless enough to accommodate vLEIs, VVP lets telco ecosystems opt in, either wholly or partially (see 7), to trust bases that are already adopted, and that are not limited to any particular jurisdiction or to the telco industry. It thus offers two-way, easy bridges between identity in phone calls and identity in financial, legal, technical, logistic, regulatory, web, email, and social media contexts.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Overview

Fundamentally, VVP requires identified parties (callers and/or callees) to curate (6) a dossier (6.3.2) of stable evidence that proves things about them. This is done once or occasionally, in advance, as a configuration precondition. Then, for each call, participants decide whether to share this evidence. Callers share evidence by creating an ephemeral STIR-compatible VVP PASSporT (6.2.6) that cites (4) their preconfigured dossier. This passport travels along the delivery route as an Identity header in a SIP

INVITE. Callees share evidence by adding an analogous passport to an attribute line in the SDP [RFC8866] body of their SIP response. This passes a signed citation to their dossier in the other direction. Verifiers anywhere along the route check the citation(s) and corresponding dossier(s), including realtime revocation status, to make decisions (5).

A VVP call may carry assurance in either or both directions. Compliant implementations may choose to support only assurance about the caller, only assurance about the callee, or both.

3.1. Roles

Understanding the workflow in VVP requires a careful definition of roles related to the protocol. The terms that follow have deep implications for the mental model, and their meaning in VVP may not match casual usage.

3.1.1. Allocation Holder

An _allocation holder_ controls how a phone number is used, in the eyes of a regulator. Enterprises and consumers that make and receive calls with phone numbers they legitimately control are the most obvious category of allocation holders, and are called direct _telephone number users_ (_TNUs_). Range holders hold allocations for numbers that have not yet been assigned; they don’t make or receive calls with these numbers, and are therefore not TNUs, but they are still allocation holders.

It is possible for an ecosystem to include other parties as allocation holders (e.g., wholesalers, aggregators). However, many regulators dislike this outcome, and prefer that such parties broker allocations without actually holding the allocations directly.

3.1.2. Callee

For a given phone call, a _callee_ (also referred to as a _terminating party_ or _TP_) receives the call. Typically one callee is targeted, but multiparty SIP flows allow INVITEs to multiple callees, either directly or via a conference server (see [RFC4353] and [RFC4575]). A callee can be an individual consumer or an organization. The direct service provider of the callee is the _terminating service provider_ (_TSP_). In many use cases for VVP, callers attempt to prove things to callees, and callees and their service providers use VVP primarily with a verifier mindset. However, enterprises or call centers that accept inbound calls from individuals may want assurance to flow the other direction; hence, VVP supports optional evidence about callees as well.

3.1.3. Originating Party

An _originating party_ (_OP_) controls the first _session border controller_ (_SBC_) that processes an outbound call, and therefore builds the VVP passport (6.2.6) that cites evidence about the caller.

It may be tempting to equate the OP with "the caller", and in some perspectives this could be true. However, this simple equivalence lacks nuance and doesn't always hold. In a VVP context, it is more accurate to say that the OP creates a SIP INVITE [RFC3261] with explicit, provable authorization from the party accountable for calls on the originating phone number. The OP originates the VVP protocol, but not always the call on the handset.

It may also be tempting to associate the OP with an organizational identity like "Company X". While this is not wrong, and is in fact used in high-level descriptions in this specification, in its most careful definition, the cryptographic identity of an OP should be more narrow. It typically corresponds to a single service operated by an IT department within (or outsourced but operating at the behest of) Company X, rather than to Company X generically. This narrowness limits cybersecurity risk, because a single service operated by Company X needs far fewer privileges than the company as a whole. Failing to narrow identity appropriately creates vulnerabilities in some alternative approaches. The evidence securing VVP MUST therefore prove a valid relationship between the OP's narrow identity and the broader legal entities that stakeholders more naturally assume and understand (see 6.3.4).

The service provider associated with an OP is called the _originating service provider_ (_OSP_). For a given phone call, there may be complexity between the hardware that begins a call and the SBC of the OP -- and there may also be many layers, boundaries, and transitions between OSP and TSP.

3.1.4. Accountable Party

For a given call, the _accountable party_ (_AP_) is the organization or individual (the TNU) that has the right to use the originating phone number, according to the regulator of that number. When a callee asks, "Who's calling?", they have little interest in the technicalities of the OP, and it is almost always the AP that they want to identify. The AP is accountable for the call, and thus "the caller", as far as the regulator and the callee are concerned.

APs can operate their own SBCs and therefore be their own OPs. However, APs can also use a UCaaS provider that makes the AP-OP relationship indirect. Going further, a business can hire a call

center, and delegate to the call center the right to use its phone number. In such a case, the business is the AP, but the call center is the OP that makes calls on its behalf. None of these complexities alter the fact that, from the callee's perspective, the AP is "the caller". The callee chooses to answer or not, based on their desire to interact with the AP. If the callee's trust is abused, the regulator and the callee both want to hold the AP accountable.

In order to verify a caller, VVP requires an AP to prepare a dossier (6.3.2) of evidence that documents a basis for imposing this accountability on them. Only the owner of a given dossier can prove they intend to initiate a VVP call that cites their dossier (see 6.1.6). Therefore, if a verifier confirms that a particular call properly matches its dossier, the verifier is justified in considering the owner of that dossier the AP for the call. Otherwise, someone is committing fraud. Accountability, and the basis for it, are both unambiguous.

3.1.5. Verified Party

A _verified party_ (_VP_) is a party that uses VVP to prove assertions about itself and its delegation decisions. When a VVP provides assurance about callers, the AP is a VP. When VVP provides assurance about callees, the callee is a VP. Some characteristics of proxies, delegates, and service providers may be proved by a dossier, but these parties are not VPs. They don't create dossiers, and dossiers are not focused on them.

3.1.6. Verifier

A _verifier_ is a party that wants to know who's calling or being called, and maybe why -- and that evaluates the answers to these questions by examining formal evidence. Callees, callers, TSPs, OSPs, government regulators, law enforcement doing lawful intercept, auditors, and even APs or OPs can be verifiers. Each may need to see different views of the evidence about a particular phone call, and it may be impossible to comply with various regulations unless these views are kept distinct -- yet each wants similar and compatible assurance.

In addition to checking the validity of cryptographic evidence, the verifier role in VVP MAY also consider how that evidence matches business rules and external conditions. For example, a verifier can begin its analysis by deciding whether Call Center Y has the right, in the abstract, to make or receive calls on behalf of Organization X using a given phone number. However, VVP evidence allows a verifier to go further: it can also consider whether Y is allowed to exercise this right at the particular time of day when a call occurs, or in a particular jurisdiction, given the business purpose asserted in a particular call.

3.2. Lifecycle

VVP depends on three interrelated activities with evidence:

* Curating
* Citing
* Verifying

Chronologically, evidence must be curated before it can be cited or verified. In addition, some vulnerabilities in existing approaches occur because evidence requirements are too loose. Therefore, understanding the nature of backing evidence, and how that evidence is created and maintained, is a crucial consideration for VVP. This specification includes normative statements about evidence.

However, curating does not occur in realtime during phone calls. Citing and verifying are the heart of VVP, and implementers will probably approach VVP from the standpoint of SIP flows [RFC3261], [RFC5626]. Therefore, we defer the question of curation to 6. Where not-yet-explained evidence concepts are used, inline references allow easy cross-reference to formal definitions that come later.

4. Citing

Citing the AP’s dossier A VVP call that makes the caller verifiable begins when the OP (3.1.3) generates a new VVP passport (6.2.6) that complies with STIR [RFC8224] requirements. In its compact-serialized JWT [RFC7519] form, this passport is then passed as an Identity header in a SIP INVITE [RFC3261]. The passport _constitutes_ lightweight, direct, and ephemeral evidence; it _cites_ and therefore depends upon comprehensive, indirect, and long-lived evidence (the AP’s dossier; see 6.3.2). Safely and efficiently citing stronger evidence is one way that VVP differs from alternatives.

4.1. Questions answered by an AP’s passport

The passport directly answers the following questions:

* What is the cryptographic identity of the OP?

* How can a verifier determine the OP’s key state at the time the passport was created?

* How can a verifier identify and fetch more evidence that connects the OP to the asserted AP?

* What brand attributes are asserted to accompany the call?

The first two answers come from the kid header. The third answer is communicated in the required evd claim. The fourth answer is communicated in the optional card and goal claims.

More evidence can then be fetched to indirectly answer the following additional questions:

* What is the legal identity of the AP?

* Does the AP have the right to use the originating phone number?

* Does the AP intend the OP to sign passports on its behalf?

* Does the AP have the right to use the brand attributes asserted for the call?

Dossiers can be further expanded to answer even more questions; such dynamic expansion of the scope of proof is compatible with but not specified by VVP.

4.1.1. Sample passport

An example will help. In its JSON-serialized form, a typical VVP passport for an AP (with some long CESR-encoded hashes shortened by ellipsis for readability) might look like this:

```
{
  "header": {
    "alg": "EdDSA",
    "typ": "JWT",
    "ppt": "vvp",
    "kid": "https://agentsrus.net/oobi/EMC.../agent/EAx..."
  },
  "payload": {
    "orig": {"tn": ["+33612345678"]},
    "dest": {"tn": ["+33765432109"]},
    "card": ["NICKNAME:Monde d'Exemples",
      "CHATBOT:https://example.com/chatwithus",
      "LOGO;HASH=EK2...;VALUE=URI:https://example.com/ico64x48.png"],
    "goal": "negotiate.schedule",
    "call-reason": "planifier le prochain rendez-vous",
    "evd": "https://fr.example.com/dossiers/E0F....cesr",
    "origId": "e0ac7b44-1fc3-4794-8edd-34b83c018fe9",
    "iat": 1699840000,
    "exp": 1699840030,
    "jti": "70664125-c88d-49d6-b66f-0510c20fc3a6"
  }
}
```

The semantics of the fields are:

* alg _(required)_ MUST be "EdDSA". Standardizing on one scheme prevents jurisdictions with incompatible or weaker cryptography. The RSA, HMAC, and ES256 algorithms MUST NOT be used. (This choice is motivated by compatibility with the vLEI and its associated ACDC ecosystem, which depends on the Montgomery-to-Edwards transformation.)

* typ _(required)_ Per [RFC8225], MUST be "passport".

* ppt _(required)_ Per [RFC8225], MUST identify the specific PASSporT type -- in this case, "vvp".

* kid _(required)_ MUST be the OOBI of an AID (6.2.3) controlled by the OP (3.1.3). An OOBI is a special URL that facilitates ACDC's viral discoverability goals. It returns IANA content-type application/json+cesr, which provides some important security guarantees. The content for this particular OOBI MUST be a KEL (6.2.8). Typically the AID in question does not identify the OP as a legal entity, but rather software running on or invoked by the SBC operated by the OP. (The AID that identifies the OP as a legal entity may be controlled by a multisig scheme and thus require multiple humans to create a signature. The AID for kid MUST be singlesig and, in the common case where it is not the legal entity AID, MUST have a delegate relationship with the legal entity AID, proved through Delegate Evidence 6.3.4.)

* orig _(required)_ Although VVP does not depend on SHAKEN, the format of this field MUST conform to SHAKEN requirements ([ATIS-1000074]), for interoperability reasons (see 7). It MUST also satisfy one additional constraint, which is that only one phone number is allowed. Depite the fact that a containing SIP INVITE may allow multiple originating phone numbers, only one can be tied to evidence evaluated by verifiers.

* dest _(required)_ For interoperability reasons, MUST conform to SHAKEN requirements.

* card _(optional)_ Contains one or more brand attributes. These are analogous to [RCD-DRAFT] or [CTIA-BCID] data, but differ in that they MUST be justified by evidence in the dossier. Because of this strong foundation that interconnects with formal legal identity, they can be used to derive other brand evidence (e.g., an RCD passport) as needed. Individual attributes MUST conform to the VCard standard [RFC6350].

* goal _(optional)_ A machine-readable, localizable goal code, as described informally by [ARIES-RFC-0519]. If present, the dossier MUST prove that the OP is authorized by the AP to initiate calls with this particular goal.

* call-reason _(optional)_ A human-readable, arbitrary phrase that describes the self-asserted intent of the caller. This claim is largely redundant with goal; most calls will either omit both, or choose one or the other. Since call-reason cannot be analyzed or verified in any way, and since it may communicate in a human language that is not meaningful to the callee, use of this field is discouraged. However it is not formally deprecated. It is included in VVP to facilitate the construction of derivative RCD passports which have the property (see 7).

* evd _(required)_ MUST be the OOBI of a bespoke ACDC (the dossier, 6.3.2) that constitutes a verifiable data graph of all evidence justifying belief in the identity and authorization of the AP, the OP, and any relevant delegations. This URL can be hosted on any convenient web server, and is somewhat analogous to the x5u header in X509 contexts. See below for details.

* origId _(optional)_ Follows SHAKEN semantics.

* iat _(required)_ Follows standard JWT semantics (see [RFC7519]).

* exp _(required)_ Follows standard JWT semantics. As this sets a window for potential replay attacks between the same two phone numbers, a recommended expiration should be 30 seconds, with a minimum of 10 seconds and a maximum of 300 seconds.

* jti _(optional)_ Follows standard JWT semantics.

For information about the signature over a passport, see 6.3.1.

4.2. Citing a callee’s dossier

Optionally, evidence in VVP can also flow from callee to caller. For privacy reasons, individuals who receive phone calls may choose not to use VVP in this way. However, enterprises and call centers may find it useful as a reassurance to their customers about who they’ve reached.

In such cases, the callee must have curated a dossier. The format of the callee dossier is identical in schema to that used by a caller. It may therefore introduce evidence of the callee’s legal identity, right to use a brand, right to use a TN, delegated authority to a call center proxy or an AI, and so forth. (A callee’s dossier might differ in one minor way that doesn’t affect the schema: it could prove the right to use a TN that has a DNO flag.)

A reference to the callee's dossier is conveyed by adding a special a=callee-passport:X attribute line to the SDP [RFC8866] body of the callee's 200 OK response. (Optionally, the lines MAY also be added to a 180 Ringing response, to make the callee verifiable earlier, but it MUST appear on the 200 OK response.) The value of this line is a JWT in compact form, with the ;type=vvp suffix. This is exactly compliant with the format used by callers to convey VVP passports in Identity headers. However, Identity headers are not used for callees because existing SIP tooling does not expect or preserve Identity headers on responses. Furthermore, the identity of a callee is primarily of interest to the caller, who is willing to parse the SDP body; it does not need the same full-route auditability as the identity of a caller.

The callee JWT has a slightly different schema than a caller's VVP passport. It has the same headers, but kid contains the OOBI of the callee, not of the OP. Two new claims are added to the JWT payload: call-id and cseq. These MUST contain the values of the Call-ID and CSeq values on the preceding SIP INVITE. The iat claim MUST also be present and MUST contain a value from the system clock of the callee. The exp field MAY also be present and use a value chosen by the callee; if it is missing, this communicates the callee's intention to impose no new timeout logic on the call. The evd field MUST also be present, and MUST contain the OOBI of the callee's dossier. The card and goal claims are also allowed. Other claims MAY be present, but MUST be ignored by compliant implementations that do not understand them. (Because the callee references the specific SIP dialog via call-id and cseq, there is no point in repeating fields that describe the dialog, like orig, dest, and so forth.)

5. Verifying

5.1. Verifying the caller

5.1.1. Algorithm

When a verifier encounters a VVP passport, they SHOULD verify by using an algorithm similar to the following. Optimizations may combine or reorder operations, but MUST achieve all of the same guarantees, in order to be compliant implementations.

1. Analyze the iat and exp claims to evaluate timing. Confirm that exp is greater than iat and also greater than the reference time for analysis (e.g., _now_), and that iat is close enough to the reference time to satisfy the verifier's tolerance for replays. (A replay attack would have to call from the same orig to the same dest with the same iat, within whatever window the verifier accepts. Thirty seconds is a recommended default value.)

2. Confirm that the orig, dest, and iat claims match contextual observations and other SIP metadata. That is, the passport appears aligned with what is known about the call from external sources.

3. Extract the kid header.

4. Fetch the key state for the OP at the reference time from the OOBI in kid. Caches may be used to optimize this, as long as they meet the freshness requirements of the verifier.

5. Use the public key of the OP to verify that the signature on the passport is valid for that key state. On success, the verifier knows that the OP is at least making an assertion about the identity and authorizations of the AP. (When reference time is now, this is approximately the level of assurance provided by existing alternatives to VVP.)

6. Extract the evd field, which references the dossier (6.3.2) that constitutes backing evidence.

7. Use the SAID (6.2.1) of the dossier as a lookup key to see whether the dossier has already been fully validated. Since dossiers are highly stable, caching dossier validations is recommended.

8. If the dossier requires full validation, perform it. Validation includes checking the signature on each ACDC in the dossier's data graph against the key state of its respective issuer at the time the issuance occurred. Key state is proved by the KEL (6.2.8), and checked against independent witnesses.

   Issuance is recorded explicitly in the KEL's overall event sequence, so this check does not require guesses about how to map issuance timestamps to key state events. Subsequent key rotations do not invalidate this analysis.

   Validation also includes comparing data structure and values against the declared schema, plus a full traversal of all chained CVD (6.2.9), back to the root of trust for each artifact. The verifier MUST accept the root of trust as a valid authority on the vital question answered by each credential that depends upon it. The correct relationships among evidence artifacts MUST also be checked (e.g., proving that the issuer of one piece is the issuee of another piece).

9. Check to see whether the revocation status of the dossier and each item it depends on has been tested recently enough, at the reference time, to satisfy the verifier's freshness requirements. If no, check for revocations anywhere in the data graph of the dossier. Revocations are not the same as key rotations. They can be checked much more quickly than doing a full validation. Revocation checks can also be cached, possibly with a different freshness threshold than the main evidence.

10. Assuming that the dossier is valid and has no breakages due to revocation, confirm that the OP is authorized to sign the passport. If there is no delegation evidence (6.3.4), the AP and the OP MUST be identical, and the OP MUST be the issuee of the vetting credential; otherwise, the OP MUST be the issuee of a delegated signing credential for which the issuer is the AP.

11. Extract the orig field and compare it to the TNAlloc credential (6.3.6) cited in the dossier (6.3.2) to confirm that the AP (3.1.4) -- or, if OP is not equal to AP and OP is using their own number, the OP (3.1.3) -- has the right to originate calls with this number.

12. If the passport includes non-null values for the optional card claim, extract that information and check that the brand attributes claimed for the call are justified by a brand credential (6.3.7) in the dossier.

13. Check any business logic. For example, if the passport includes a non-null value for the optional goal claim, confirm that the verifier is willing to accept a call with that goal. Or, if the delegated signer credential says that the OP can only call on behalf of the AP during certain hours, or in certain geos, check those attributes of the call.

5.2. Verifying the callee

The callee is verified with an algorithm that MAY be optimized but MUST achieve the same security guarantees as this:

1. Confirm that the call-id and cseq claims match the values of Call-ID and CSeq from the preceding SIP INVITE.

2. Confirm that the iat claim matches contextual observations and other SIP metadata. That is, the timing described by the callee appears aligned with what is known about the call from external sources.

3. If the exp claim is present, analyze the iat and exp claims to evaluate timeout.

4. Extract the kid header.

5. Fetch the key state for the callee at the reference time from the OOBI in kid. Caches may be used to optimize this, as long as they meet the freshness requirements of the verifier.

6. Use the public key of the callee to verify that the signature on the passport is valid for that key state.

7. Extract the evd field, which references the dossier (6.3.2) that constitutes backing evidence.

8. Use the SAID (6.2.1) of the dossier as a lookup key to see whether the dossier has already been fully validated. Since dossiers are highly stable, caching dossier validations is recommended.

9. Confirm that the dossier was signed (issued) by the same AID that appears in the kid header.

10. If the dossier requires full validation, perform it.

11. Check to see whether the revocation status of the dossier and each item it depends on has been tested recently enough, at the reference time, to satisfy the verifier’s freshness requirements.

12. Compare the callee’s TN to the TNAlloc credential (6.3.6) cited in the dossier (6.3.2) to confirm that the callee has the right to accept calls at this number.

13. If the passport includes non-null values for the optional card claim, extract that information and check that the brand attributes claimed for the call are justified by a brand credential (6.3.7) in the dossier.

14. Check any business logic. For example, if the passport includes a non-null value for the optional goal claim, and the preceding INVITE included a VVP passport that also declared a goal, confirm that the callee’s and caller’s goals overlap (one must be a subset of the other). Or, if the delegated signer credential says that a call center or an AI can accept calls during certain hours, or in certain geos, check those attributes of the call.

5.3. Planning for efficiency

A complete verficiation of either caller or callee passport, from scratch, is quite rigorous. With no caches, it may take several seconds, much like a thorough validation of a certificate chain. However, much VVP evidence is stable for long periods of time and lends itself to caching, subject to the proviso that revocation freshness must be managed wisely. Since the same dossier is used to add assurance to many calls -- perhaps thousands or millions of calls, for busy call centers -- and many dossiers will reference the same issuers and issuees and their associated key states and KELs (6.2.8), caching will produce huge benefits.

Furthermore, because SAIDs and their associated data (including links to other nodes in a data graph) have a tamper-evident relationship, any party can perform validation and compile their results, then share the data with verifiers that want to do less work. Validators like this are not oracles, because consumers of such data need not trust shared results blindly. They can always directly recompute some or all of it from a passport, to catch deception. However, they can do this lazily or occasionally, per their preferred balance of risk/effort.

In toto, these characteristics mean that no centralized registry is required in any given ecosystem. Data can be fetched directly from its source, across jurisdictional boundaries. Because it is fetched from its source, it comes with consent. Privacy can be tuned (see 9). Simple opportunistic, uncoordinated reuse (e.g., in or across the datacenters of TSPs) will arise spontaneously and will dramatically improve the scale and efficiency of the system.

5.4. Historical analysis

Normally, the verification algorithm determines whether the passport verifies _now_. (This is the only evaluation that’s valid for most JWTs, because they depend on ephemeral key state fetched just in time from x5u). However, a VVP passport can do more. Its kid header references a KEL for the signer’s AID, and its evd header references a dossier issued by either the AID of the AP or the AID of the callee. From thence it connects to a KEL (see 6.2.8). These data structures provide key state transitions that are timestamped -- both by the controllers of the AIDs, and by their independent witnesses. Although the timestamps are not guaranteed to be perfectly synchronized, they can be compared to establish fuzzy transition times and to detect duplicity.

Using this historical information, it becomes possible to ask whether a VVP passport verified at an arbitrary moment in the past. In such framings, the reference time from the verification algorithm is _then_, not _now_. In the normal case where _then_ falls outside a fuzzy range, answers about key state are clear to all observers. In the rare cases where _then_ falls inside a fuzzy range, a state transition was underway but not yet universally known, and a verifier can compute the key state (and thence, the outcome of the verification algorithm) according to their preferred interpretation.

6. Curating

The evidence that’s available in today’s telco ecosystems resembles some of the evidence described here, in concept. However, existing evidence has gaps, and its format is fragile. It requires direct trust in the proximate issuer, and it typically needs to be organized for discovery; both characteristics lead to large, centralized registries at a regional or national level. These registries become a trusted third party, which defeats some of the purpose of creating decentralized and independently verifiable evidence in the first place. Sharing such evidence across jurisdiction boundaries requires regulatory compatibility and bilateral agreements. Sharing at scale is impractical at best, if not illegal.

How evidence is issued, propagated, quality-controlled, and referenced is therefore an important concern for this specification.

6.1. Activities

The following curation activities guarantee the evidence upon which a VVP ecosystem depends.

6.1.1. Witnessing and watching

In an ACDC-based ecosystem, issuers issue and revoke their own evidence without any calls to a centralized registry or authority. However, KERI’s decentralized witness feature MUST be active. This provides an official, uniform, and high-security methodology for curating the relationship between keys and identifiers, and between identifiers and non-repudiable actions like issuing and revoking credentials. In addition, watchers MAY be used by given verifiers, to provide efficient caching, pub-sub notifications of state changes, and duplicity detection. For more about these topics, see 11.

6.1.2. Vetting identity

Entities that SHOULD be vetted in a VVP ecosystem include APs 3.1.4, but also OPs 3.1.3 and callees 3.1.2, depending on which identities need to be verified. The job of vetting legal entities and issuing vetting credentials (6.3.5) is performed by a _legal entity vetter_. VVP MUST have evidence of vetted identity. It places few requirements on such vetters, other than the ones already listed for vetting credentials themselves. Vetting credentials MAY expire, but this is not particularly desirable and might actually be an antipattern. ACDCs and AIDs facilitate much longer lifecycles than certificates; proactive key rotation is recommended but creates no reason to rotate evidence. However, a legal entity vetter MUST agree to revoke vetting credentials in a timely manner if the legal status of an entity changes, or if data in a vetting credential becomes invalid.

6.1.3. Vetting brand

At the option of the verified entities, VVP MAY prove brand attributes. When this feature is active, the job of analyzing the brand assets of a legal entity and issuing brand credentials (6.3.7) is performed by a _brand vetter_. A brand vetter MAY be a legal entity vetter, and MAY issue both types of credentials after a composite analysis. However, the credentials themselves MUST NOT use a combined schema, the credentials SHOULD have independent lifecycles. This allows the assurances associated with each credential type to remain independent.

A brand vetter MUST verify the canonical properties of a brand, but it MUST do more than this: it MUST issue the brand credential to the AID 6.2.3 of an issuee that is also the issuee of a vetting credential that already exists, and it MUST verify that the legal entity in the vetting credential has a right to use the brand in question. This link MUST NOT be based on mere weak evidence such as an observation that the legal entity’s name and the brand name have some or all words in common, or the fact that a single person requested both credentials. Further, the brand vetter MUST agree to revoke brand credentials in a timely manner if the associated vetting credential is revoked, if the legal entity’s right to use the brand changes, or if characteristics of the brand evolve.

6.1.4. Allocating TNs

At the option of the AP and OP, VVP SHOULD prove the right to use the originating phone number. At the option of the callee, VVP MAY prove the right to use the terminating phone number. When this feature is active, regulators MUST issue TNAlloc credentials (6.3.6) to range holders, and range holders MUST issue them to downstream AHs in an unbroken chain that reaches telephone number users (TNUs; see 3.1.1). TNUs MAY in turn issue them to a delegate such as a call center. If aggregators or other intemediaries hold an RTU in the eyes of a regulator, then intermediate TNAlloc credentials MUST be created to track that RTU as part of the chain. On the other hand, if TNUs acquire phone numbers through aggregators, but regulators do not consider aggregators to hold allocations, then aggregators MUST work with range holders to assure that the appropriate TNAlloc credentials are issued to the TNUs.

6.1.5. Authorizing brand proxy

When VVP is used to prove brand, VPs (3.1.5) MAY issue brand proxy credentials (6.3.8) to delegates, giving them the right to use the VP’s brand. Without this credential, the delegate has the right to use the phone number, not the brand.

Decisions about whether to issue vetting and brand credentials might be driven by large databases of metadata about organizations and brands, but how such systems work is out of scope. The credentials themselves contain all necessary information, and once credentials are issued, they constitute an independent source of truth as far as VVP is concerned. No party has to return to the operators of such databases to validate anything.

6.1.6. Delegating signing authority

A VP (3.1.5) MUST prove, by issuing a delegated signer credential (6.3.9), that the signer of its VVP passports does so with its explicit authorization. Normally the signer is automation under the control of the delegate, but the issuee of the credential MAY vary at the VP’s discretion.

Since this credential merely documents the issuer’s intent to be accountable for the actions of the signer, the VP MAY choose whatever process it likes to issue it.

6.1.7. Revoking

Revoking an ACDC is as simple as the issuer signing a revocation event and distributing it to witnesses (see 11). Parties that perform a full validation of a given ACDC (see 5) will automatically detect the revocation event in realtime, because they will contact one or more of these witnesses. Parties that are caching their validations MAY poll witnesses very efficiently to discover revocation events. Some witnesses may choose to offer the option of registering a callback, allowing interested parties to learn about revocations even more efficiently.

6.2. Building blocks

The term "credential" has a fuzzy meaning in casual conversation. However, understanding how evidence is built from credentials in VVP requires considerably more precision. We will start from lower-level concepts.

6.2.1. SAID

A _self-addressing identifier_ (_SAID_) is the hash of a canonicalized JSON object, encoded in self-describing CESR format [TOIP-CESR]. The raw bytes from the digest function are left-padded to the nearest 24-bit boundary and transformed to base64url [RFC4648]. The left-pad char from the converted left-pad byte is replaced with a code char that tells which digest function was used.

An example of a SAID is E81Wmjyz5nXMCYrQqWyRLAYeKNQvYLYqMLYv_qm-qP7a, and a regex that matches all valid SAIDs is: [EFGHI][-_\w]{43}|0[DEFG][-_\w]{86}. The E prefix in the example indicates that it is a Blake3-256 hash.

SAIDs are evidence that hashed data has not changed. They can also function like a reference, hyperlink, or placeholder for the data that was hashed to produce them (though they are more similar to URNs than to URLs [RFC3986], since they contain no location information).

6.2.2. Signature

A digital signature over arbitrary data D constitutes evidence that the signer processed D with a signing function that took D and the signer’s private key as inputs: signature = sign(D, privkey). The evidence can be verified by checking that the signature is bound to D and the public key of the signer: valid = verify(signature, D, pubkey). Assuming that the signer has not lost unique control of the private key, and that cryptography is appropriately strong, we are justified in the belief that the signer must have taken deliberate

action that required seeing an unmodified D in its entirety.

The assumption that a signer has control over their private keys may often be true (or at least believed, by the signer) at the time a signature is created. However, after key compromise, an attacker can create and sign evidence that purports to come from the current or an earlier time period, unless signatures are anchored to a data source that detects anachronisms. Lack of attention to this detail undermines the security of many credential schemes, including in telco. VVP explicitly addresses this concern by anchoring signatures on non-ephemeral evidence to KELs (6.2.8).

6.2.3. AID

An _autonomic identifier_ (_AID_) is a short string that can be resolved to one or more cryptographic keys at a specific version of the identifier's key state. Using cryptographic keys, a party can prove it is the controller of an AID by creating digital signatures. AIDs are like W3C DIDs [W3C-DID], and can be transformed into DIDs. The information required to resolve an AID to its cryptographic keys is communicated through a special form of URI called an _out-of-band invitation_ (_OOBI_). An OOBI points to an HTTP resource that returns IANA content-type application/json+cesr; it is somewhat analogous to a combination of the kid and x5u constructs in many JWTs. AIDs and OOBIs are defined in the KERI spec [TOIP-KERI].

An example of an AID is EMCYrQqWyRLAYqMLYv_qm-qP7eKN81Wmjyz5nXQvYLYa. AIDs are created by calculating the hash of the identifier's initial state; since this state is typically a canonicalized JSON object, AIDs usually match the same regex as SAIDs (which are hashes of JSON). A noteworthy exception is that non-transferrable AIDs begin with B instead of E or another letter. Such AIDs hash only their public key, not a document. They are analogous to did:key values, and play a limited role in VVP. They are incapable of rotating keys or anchoring events to a KEL. They therefore lack OOBIs and can receive but not issue ACDCs. However, their virtue is that they can be created and used without a sophisticated wallet. This may make them a convenient way to identify the automation that signs passports and receives a delegated signer credential (see 6.1.6).

An example of an OOBI for an AID is https://agentsrus.net/oobi/EMCYrQqWyRLAYqMLYv_qm-qP7eKN81Wmjyz5nXQvYLYa/agent/EAxBDJkpA0rEjUG8vJrMdZKw8YL63r_7zYUMDrZMf1Wx. Note the same EMCY... in the AID and its OOBI. Many constructs in KERI may have OOBIs, but when OOBIs are associated with AIDs, such OOBIs always contain their associated AID as the first URL segment that matches the AID regex. They point either to an agent or a witness that provides verifiable state information for the AID.

AIDs possess several security properties (e.g., self-certification, support for prerotation and multisig, support for witnesses, and cooperative delegation) that are not guaranteed by DIDs in general. Such properties are vital to some of VVP's goals for high assurance.

6.2.4. Signatures over SAIDs

Since neither a SAID value nor the data it hashes can be changed without breaking the correspondence between them, and since the cryptographic hash function used ensures strong collision resistance, signing over a SAID is equivalent, in how it commits the signer to content and provides tamper evidence, to signing over the data that the SAID hashes. Since SAIDs can function as placeholders for JSON objects, a SAID can represent such an object in a larger data structure. And since SAIDs can function as a reference without making a claim about location, it is possible to combine these properties to achieve some indirections in evidence that are crucial in privacy and regulatory compliance.

VVP uses SAIDs and digital signatures as primitive forms of evidence.

6.2.5. X509 certificates

VVP does not depend on X509 certificates [RFC5280] for any of its evidence. However, if deployed in a hybrid mode, it MAY be used beside alternative mechanisms that are certificate-based. In such cases, self-signed certificates that never expire might suffice to tick certificate boxes, while drastically simplifying the burden of maintaining accurate, unexpired, unrevoked views of authorizations and reflecting that knowledge in certificates. This is because deep authorization analysis flows through VVP's more rich and flexible evidence chain. See 7.

6.2.6. Passport

VVP uses STIR PASSporTs that are fully compliant with [RFC8225] in all respects, except that it MAY omit the x5u header that links it to an X509 certificate (see 7.2).

The passport is a form of evidence suitable for evaluation during the brief interval when a call is being initiated, and it is carefully backed by evidence with a longer lifespan (6.3.2). Conceptually, VVP's version is similar to a SHAKEN passport [RFC8588]. It MAY also reference brand-related evidence, allowing it to play an additional role similar to the RCD passport [RCD-PASSPORT].

Neither VVP's backing evidence nor its passport depends on a certificate authority ecosystem. The passport MUST be secured by an EdDSA digital signature [RFC8032], [FIPS186-4], rather than the signature variants preferred by the other passport types. Instead of including granular fields in the claims of its JWT, the VVP passport cites a rich data graph of evidence by referencing the SAID of that data graph. This indirection and its implications are discussed below.

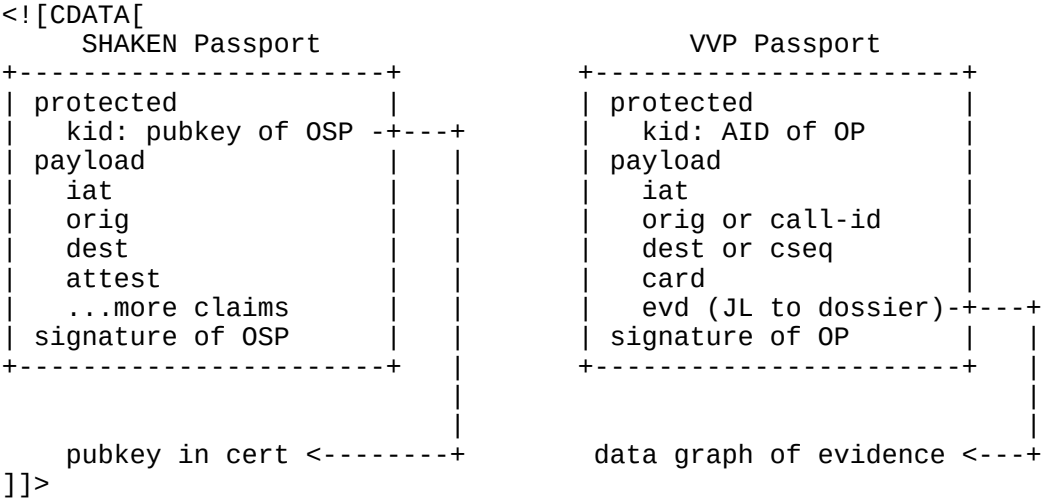

Figure 1: SHAKEN Passport compared to VVP Passport

6.2.7. ACDCs

Besides digital signatures and SAIDs, and the ephemeral passport, VVP uses long-lasting evidence in the ACDC format [TOIP-ACDC]. This is normalized, serialized data with an associated digital signature. Unlike X509 certificates, ACDCs are bound directly to the AIDs of their issuers and issuees, not to public keys of these parties. This has a radical effect on the lifecycle of evidence, because keys can be rotated without invalidating ACDCs (see 10).

6.2.8. KELs

Unlike X509 certificates, JWTs [RFC7519], and W3C Verifiable Credentials [W3C-VC], signatures over ACDC data are not _contained inside_ the ACDC; rather, they are _referenced by_ the ACDC and _anchored in_ a verifiable data structure called a _key event log_ or _KEL_ [TOIP-KERI].

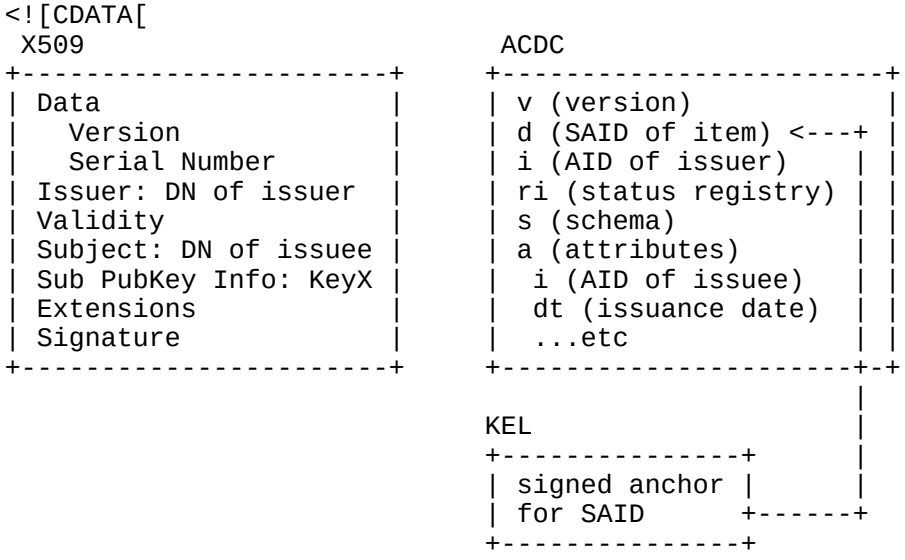

Figure 2: X509 compared to ACDC

A KEL has some trust characteristics that resemble a blockchain. However, it is specific to one AID only (the AID of the issuer of the ACDC) and thus is not centralized. The KELs for two different AIDs need not (and typically do not) share any common storage or governance, and do not require coordination or administration. KELs thus suffer none of the performance and governance problems of blockchains, and incur none of blockchain's difficulties with regulatory requirements like data locality or right to be forgotten.

ACDCs can be freely converted between text and binary representations, and either type of representation can also be compacted or expanded to support nuanced disclosure goals (see 9.1). An ACDC is also uniquely identified by its SAID, which means that a SAID can take the place of a full ACDC in certain data structures and processes. None of these transformations invalidate the associated digital signatures, which means that any variant of a given ACDC is equivalently verifiable.

The revocation of a given ACDC can be detected via the witnesses declared in its issuer's KEL. Discovering, detecting, and reacting to such events can be very efficient. Any number of aggregated views can be built on demand, for any subset of an ecosystem's evidence, by any party. This requires no special authority or access, and does not create a central registry as a source of truth, since such views are tamper-evident and therefore can be served by untrusted parties.

Further, different views of the evidence can contain or elide different fields of the evidence data, to address privacy, regulatory, and legal requirements.

6.2.9. CVD

Cryptographically verifiable data (_CVD_) is data that's associated with a digital signature and a claim about who signed it. When CVD is an assertion, we make the additional assumption that the signer intends whatever the data asserts, since they took an affirmative action to create non-repudiable evidence that they processed it. CVD can be embodied in many formats, but in the context of VVP, all instances of CVD are ACDCs. When CVD references other CVD, the computer science term for the resulting data structure is a _data graph_.

6.2.10. Credential

A _credential_ is a special kind of CVD that asserts entitlements for its legitimate bearer -- _and only its bearer_. CVD that says Organization X exists with a particular ID number in government registers, and with a particular legal name, is not necessarily a credential. In order to be a credential, it would have to be associated with an assertion that its legitimate bearer -- _and only its bearer_ -- is entitled to use the identity of Organization X. If signed data merely enumerates properties without conferring privileges on a specific party, it is just CVD. Many security gaps in existing solutions arise from conflating CVD and credentials.

ACDCs can embody any kind of CVD, not just credentials.

6.2.11. Bearer token

VVP never uses bearer tokens, but we define them here to provide a contrast. A _bearer token_ is a credential that satisfies binding requirements by a trivial test of possession -- like a movie ticket, the first party that presents the artifact to a verifier gets the privilege. Since Bearer Credentials can be stolen or copied, this is risky. JWTs, session cookies, and other artifacts in familiar identity technologies are often bearer tokens, even if they carry digital signatures. Although they can be protected to some degree by expiration dates and secure channels, these protections are imperfect. For example, unbeknownst to the parties on either end, TLS channels can be terminated and recreated at multiple places between call origination and delivery.

6.2.12. Targeted credential

A _targeted credential_ is a CVD that identifies an issuee as the bearer, and that requires the issuee to prove their identity cryptographically (e.g., to produce a proper digital signature) in order to claim the associated privilege. All credentials in VVP are targeted credentials.

6.2.13. JL

A _justifying link_ (_JL_) is a reference, inside of one CVD, to another CVD that justifies what the first CVD is asserting. JLs can be SAIDs that identify other ACDCs. JLs are edges in an ACDC data graph.

6.3. Specific artifacts

6.3.1. PSS

Each voice call begins with a SIP INVITE. If VVP is being used to make a caller verifiable, each SIP INVITE contains an Identity header that MUST have a signature from the call's OP (3.1.3). If VVP is being used to make a callee verifiable, each 200 OK response contains an a=callee-passport attribute line in its body, where the passport has a signature from the callee. In either case, the _passpport-specific signature_ (_PSS_) MUST be an Ed25519 signature serialized as CESR; it is NOT a JWS. The 64 raw bytes of the signature are left-padded to 66 bytes, then base64url-encoded. The AA at the front of the result is cut and replaced with 0B, giving an 88-character string. A regex that matches the result is: 0B[-_\w]{86}, and a sample value (with the middle elided) is: 0BNzaC1lZD...yRLAYeKNQvYx.

The signature MUST be the result of running the EdDSA algorithm over input data in the manner required by [RFC7519]: signature = sign(base64url(header) + "." + base64url(payload). Also per the JWT spec, when the signature is added to the compact form of the JWT, it MUST be appended to the other two portions of the JWT, with a . delimiter preceding it. Per STIR conventions, it MUST then be followed by ";ppt=vvp" so tools that scan the string can decide how to process the passport without doing a full parse of the JWT.

The headers in a VVP passport MUST include alg, typ, ppt, and kid, as described in 4.1.1. They MAY include other values, notably x5u (see 7.2). The claims MUST always include iat and evd. Caller passports MUST also include orig, dest, and exp; callee passports MUST also include call-id and cseq, and MAY include exp. Passports MAY include card, goal, call_reason, jti, origId, and other values (also described in 4.1.1). The signature MUST use all headers and all claims as input to the data stream that will be signed.

6.3.2. Dossier

The evd field in the passport contains the OOBI (6.2.3) of an ACDC data graph called the _dossier_. The dossier is a compilation of all the permanent, backing evidence that justifies trust in the identity and authorization of the AP and OP (when referenced by the caller) or of the callee (when referenced the other direction). It is created and must be signed by the party that uses it. It is CVD (6.2.9) asserted to the world, not a credential (6.2.10) issued to a specific party.

6.3.3. Verified Party Evidence

The dossier MUST include at least what is called _verified party evidence_ (_VPE_).

VPE consists of several credentials, explored in detail below. It MUST include a vetting credential for the verified party (the AP or the callee). It SHOULD include a TNAlloc credential that proves RTU. Normally the RTU MUST be assigned to the verified party; however, if a proxy is active and uses their own phone number, the RTU MUST be assigned to the proxy instead. If the verified party intends to contextualize the call with a brand, it MUST include a brand credential for the verified party. (In cases where callers are private individuals, "brand" maps to descriptive information about the individual, as imagined in mechanisms like VCard [RFC6350] or JCard [RFC7095].) If no brand credential is present, verifiers MUST NOT impute a brand to the call on the basis of any VVP guarantees. VPE MAY also include evidence that will aid in settlement.

6.3.4. Delegation Evidence

When a private individual makes a call with VVP, they might be both the AP and the OP; when they receive a call, they are the callee. An AID belonging to such an individual is likely to be the issuee (recipient) of all the VPE, and no backing evidence beyond the VPE may be necessary. However, in business contexts, it will almost always be true that the OP role is played by a delegate, and callees may be proxied as well. In such conditions, evidence must also

include proof that this indirection is valid. We call this _delegation evidence_ (_DE_).

DE is nearly always required when the verified party is an organization, because the cryptographic identifier for the organization as a legal entity is typically not the same as the cryptographic identifier for the organization's automated software that prepares SIP INVITEs or SIP responses. DE can thus distinguish between Acme Corporation in general, and software operated by Acme's IT department for the express purpose of signing voice traffic. The former has a vetting credential and legal accountability, and can act as the company to publish press releases, prepare invoices, spend money, and make attestations to regulators; the latter should only be able to sign voice calls on Acme's behalf. Failing to make this distinction creates serious cybersecurity risks.

Delegation evidence may also be used to prove that an AI-powered agent is empowered to interact on phone calls on behalf of a verified party.

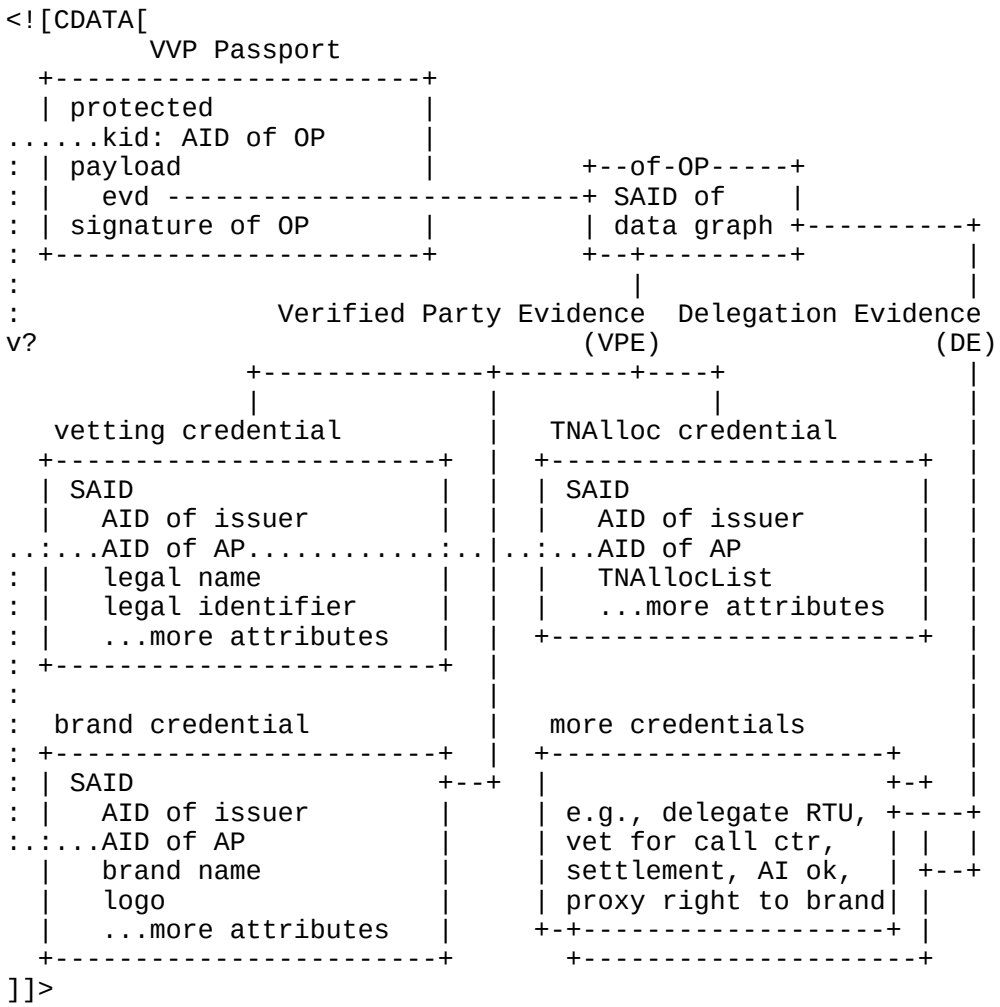

Figure 3: Sample evidence graph; OP kid could bind to VPE or DE

Where DE exists, the VPE will identify and authorize the verified party, but the OOBI in the kid claim of the passport will identify the OP or the callee's delegate, and these two parties will be different. Therefore, the DE in the dossier MUST include a delegated signer credential that authorizes the delegate (e.g., an OP) to act on the verified party's behalf and that stipulates the constraints that govern this delegation. In addition to the vetting credential for the verified party, which is required, it SHOULD also include a vetting credential for the delegate, that proves the delegate's identity. If the VPE includes a brand credential, then the DE MUST also include a brand proxy credential, proving that the delegate not only can use the verified party's allocated phone number, but has permission to project the verified party's brand while doing so.

In VVP calls that verify the caller, the passport-specific signature MUST come from the OP, not the OSP or any other party. The OP can generate this signature in its on-prem or cloud PBX, using keys that it controls. It is crucial that the distinction between OP and AP be transparent, with the relationship proved by strong evidence that the AP can create or revoke easily, in a self-service manner.

6.3.5. Vetting credential

A vetting credential is a targeted credential that enumerates the formal and legal attributes of a unique legal entity. It MUST include a legal identifier that makes the entity unique in its home jurisdiction (e.g., an LEI), and it MUST include an AID for the legal entity as a participant in voice traffic. This AID is globally unique.

The vetting credential is so called because it MUST be issued according to a documented vetting process that offers formal assurance that it is only issued with accurate information, and only to the entity it describes. A vetting credential confers the privilege of acting with the associated legal identity if and only if the bearer can prove their identity as issuee via a digital signature from the issuee's AID.

A vetting credential MUST include a JL to a credential that qualifies the issuer as a party trusted to do vetting. This linked credential that qualifies the issuer of the vetting credential MAY contain a JL that qualifies its own issuer, and such JLs MAY be repeated through as many layers as desired. In VVP, the reference type of a vetting credential is an LE vLEI; see [ISO-17442-3] and 12.2. This implies both a schema and a governance framework. Other vetting credential types are possible, but they MUST be true credentials that meet the normative requirements here. They MUST NOT be bearer tokens. An alternate schema for a vetting credential with lower levels of assurance is published at [ORG-VET-SCHEMA].

To achieve various design goals, a vetting credential MUST be an ACDC, but this ACDC MAY be a transformation of a credential in another format (e.g., W3C VC, SD-JWT, X509 certificate). See 7.

6.3.6. TNAlloc credential

A TNAlloc credential is a targeted credential that confers on its issuee the right to control how one or more phone numbers are used. Regulators issue TNAlloc credentials to range holders, who in turn issue new TNAlloc credentials to TNUs. TNUs often play the verified party roles in VVP. If an AP delegates RTU to a proxy (e.g., an employee or call center), the AP MUST also issue a TNAlloc credential to the proxy, to confer the RTU. With each successive reallocation, the set of numbers in the new TNAlloc credential may get smaller.

Except for TNAlloc credentials issued by regulators, all TNAlloc credentials MUST contain a JL to a parent TNAlloc credential, having an equal or bigger set of numbers that includes those in the current credential. This JL in a child credential documents the fact that the child’s issuer possessed an equal or broader RTU, from which the subset RTU in child credential derives.

To achieve various design goals, a TNAlloc credential MUST be an ACDC, but this ACDC MAY be a transformation of a credential in another format (e.g., a TNAuthList from [RFC8226]). See 7.3.

An example TNAlloc credential and its schema are described in 12.3.

6.3.7. Brand credential

A brand credential is a targeted credential that enumerates brand properties such as a brand name, logo, chatbot URL, social media handle, and domain name. It MUST be issued to an VP (3.1.5) as a legal entity, but it does not enumerate the formal and legal attributes of the VP; rather, it enumerates properties that would be meaningful to a callee who’s deciding whether to accept a phone call.

It confers on its issuee the right to use the described brand by virtue of research conducted by the issuer (e.g., a trademark search).

This credential MUST be issued according to a documented process that offers formal assurance that it is only issued with accurate information, and only to a legal entity that has the right to use the described brand. A single VP MAY have multiple brand credentials (e.g., a fictional corporation, Amce Space Travel Deutschland, GmbH, might hold brand credentials for both Sky Ride and for Orb鱈tame Latinoam辿rica). Rights to use the same brand MAY be conferred on multiple VPs (Acme Space Travel Deutschland, Gmbh and Acme Holdings Canada, Ltd may both possess brand credentials for Sky Ride). A brand credential MUST contain a JL to a vetting credential, that shows that the right to use the brand was evaluated only after using a vetting credential to prove the identity of the issuee.

An example brand credential and its schema are described in 12.4.

6.3.8. Brand proxy credential

A brand proxy credential confers on an OP or call center the right to project the brand of a VP when making or receiving phone calls, subject to a carefully selected set of constraints. This is different from the simple RTU conferred by TNAlloc. Without a brand proxy credential, a call center could make calls or receive on behalf of an VP, using the VP's allocated phone number, but would be forced to do so under its own name or brand, because it lacks evidence that the VP intended anything different. If an VP intends for phone calls to be made by a proxy, and wants the proxy to project the VP's brand, the AP MUST issue this credential.

An example brand proxy credential and its schema are shown in 12.5.

6.3.9. Delegated signer credential

A delegated signer credential proves that automation running under the control of the OP (for verified callers) or the callee's delegate (for verified callees) has been authorized by the VP to originate VVP traffic (and thus, sign VVP passports) on its behalf.

An example delegated signer credential and its schema are shown in 12.6.

6.3.10. Additional credential types

New credential types can be added to a dossier, to answer any number of novel questions for verifiers, without changing the core characteristics of VVP.

For example, a credential could be attached to a dossier to prove that the caller is a human being instead of an AI (see [F2F-SCHEMA] and [PERSONHOOD-CRED]), or a credential could be attached to a dossier to prove that the VP empowered an AI agent to make or receive calls on its behalf (analogous to how chatbots represent companies in RCS contexts). An additional credential could assist with questions about settlement (how the terminating service provider will be paid to connect the call). It might document the relationship between an AP and one or more financial clearinghouses.

7. Interoperability

VVP can achieve its goals without any dependence on RCD, SHAKEN, or similar mechanisms. However, it also provides easy bridges so value can flow to and from other ecosystems with similar goals.

7.1. Chat and conversations

A dossier cited in a VVP passport may also be cited by an RCS verification authority (VA), may include evidence that is also submitted to a VA, or may consist of evidence created by a VA. This unlocks synergies between vetting for RCS ([GSMA-RCS]) and vetting for voice. It may also allow properly vetted RCS chatbots to make verifiable voice calls, including calls that carry brand information (see [RCD-DRAFT] and [CTIA-BCID]), distinguishing them with 100% confidence from AI-driven voice scams.

When conversations are captured in rich containers such as vCon ([VCON-DRAFT]), a VVP passport may be included (e.g., in the stir field of a vCon), proving the identity of a calling party. As long as signatures over the data structure assert truthfully that the passport was verified at the time of attachment, no replay attack is possible, and all of VVP’s guarantees transfer. A VVP dossier by itself can also provide permanent evidence of assertions as attachments to a conversation.

7.2. Certificates

Certificates can add value to VVP, and VVP can add value to certificate-based ecosystems or stacks. In the rest of this section, note the difference between normative language (imposing requirements on VVP implementations) and non-normative language (suggesting how other solutions could react).

7.2.1. Cascaded mode

Verifiers who prefer to operate in certificate ecosystems such as SHAKEN and RCD can be satisfied by having an intermediary verify according to VVP rules (see 5), and then signing a new passport in a certificate-dependent format (e.g., for SHAKEN and/or RCD). In such cases, the new passport contains an x5u header pointing to the certificate of the new signer.

This form of trust handoff is called _cascaded mode_. In cascaded mode, if the certificate fetched from the x5u URL satisfies enough trust requirements of the verifier, the goals of the new context are achieved. For example, if this intermediary is the OSP, the standard assumptions of SHAKEN are fully met, but the OSP's attestation can always be A, since VVP conclusively proves the identity of the AP and OP.

7.2.2. Foundation mode

In another pattern called _foundation mode_, a VVP passport MAY itself contain an x5u header. If it does, the x5u header MUST NOT be used to achieve any VVP verification guarantees; the key state of the signer's AID (fetched via kid) MUST still justify any acceptance of the signature. However, the associated X509 certificate SHOULD be issued to the public key of the party that signs the passport. If and only if it does so, the full weight of VVP evidence about the signer's status as a trusted voice traffic signer for the VP could be transferred to the certificate, even if the certificate is self-issued or otherwise chains back to something other than a known, high-reputation certificate authority.

Valid VVP passports that obey this requirement can thus be used to enable VVP-unaware but certificate-based checks without certificate authorities (or without prior knowledge of them). Such certificate-based checks should be done in real-time, since the binding between a key and the owner of a cert cannot be known to be valid except at the current moment.

7.3. Other credential formats

The stable evidence that drives VVP -- vetting credential (6.3.5), TNAlloc credential (6.3.6), brand credential (6.3.7), brand proxy credential (6.3.8), and delegated signer credential (6.3.9) -- MUST all be ACDCs. This is because only when the data in these credentials is modeled as an ACDC is it associated with permanent identities that possess appropriate security guarantees.

However, VVP can easily be driven by other approaches to evidence, treating the ACDCs as a somewhat secondary format transformation. In such a case, a _bridging party_ plays a pivotal role. This party MUST verify foreign evidence (e.g., W3C verifiable credentials [W3C-VC]), and then issue ACDCs that derive from it (e.g., using [CITATION-SCHEMA]). It MAY radically transform the data in the process (e.g., combining or splitting credentials, changing schemas or data values).

This transformation from foreign evidence to ACDCs is very flexible, and allows for tremendous interoperability. On the citing side, any ecosystem that deals in cryptographic evidence can provide input to VVP, no matter what evidence mechanisms they prefer.

(On the verifying side, the information carried via ACDCs in VVP could be transformed again, with a second bridging party, to enable even more interoperability. However, the goals of such a secondary transformation are undefined by VVP, so the constraints and rules of the transformation are out of scope here.)

All VVP stakeholders need to understand that accepting foreign evidence does much more than alter format. Bridging is not a simple conversion or reissuance. It replaces identifiers (e.g., DIDs as specified in [W3C-DID] with AIDs as specified in [TOIP-KERI]). The new identifiers have different lifecycles and different trust bases than the original. Bridging also changes the _meaning_ of the credential. Foreign evidence directly asserts claims backed by the reputation of its original issuer. A new ACDC embodies a claim by the bridging party, that they personally verified foreign evidence according to foreign evidence rules, at a given moment. It cites the foreign evidence as a source, and may copy claims into the ACDC, but the bridging party is only asserting that they verified the original issuer’s commitment to the claims, not that the bridging party commits to those claims.

Verifiers MAY choose to accept such derivative ACDCs, but the indirection SHOULD color their confidence. They MUST NOT assume that identifiers in the foreign evidence and in the ACDC have the same referents or controllers. They MUST NOT hold the bridging party

accountable for the claims -- only for the claim that they verified the original issuer’s commitment to the claims. Unless additional governance offers guarantees beyond those explicitly provided by VVP, they MUST accept that there is no defined relationship between revocation of the foreign evidence and revocation of the ACDC.

8. Security Considerations

Complying with a specification may forestall certain easy-to-anticipate attacks. However, _it does not mean that vulnerabilities don’t exist, or that they won’t be exploited_. The overall assurance of VVP requires reasonable vigilance. Given that a major objective of VVP is to ensure security, implementers are strongly counseled to understand the underlying principles, the assumptions, and the ways that choices by their own or other implementations could introduce risk.

Like most cryptographic mechanisms, VVP depends on the foundational assumption that human stakeholders will manage cryptographic keys carefully. VVP enforces this assumption more thoroughly than many existing solutions:

* Parties that issue credentials MUST be identified with AIDs (6.2.3) that use witnesses (11). This guarantees a non-repudiable, publicly accessible audit log of how their key state evolves, and it makes key rotation easy. It also offers compromise and duplicity detection. Via prerotation, it enables recovery from key compromise. AIDs can be upgraded to use quantum-proof signing algorithms without changing the identifier.

* Parties that issue credentials MUST do so using ACDCs (6.2.7) signed by their AID rather than a raw key. This makes evidence revocable. It also makes it stable across key rotation, and prevents retrograde attacks by allowing verifiers to map an issuance or revocation event to an unambiguous key state in the KEL (6.2.8).

* Parties that issue credentials SHOULD employ threshold-based multi-signature schemes. This enhances security by distributing signing authority across multiple key holders, reducing the risk of single-point compromise. Threshold-based signatures ensure that no single key compromise undermines the system寰洰 integrity while enabling controlled key recovery and rotation without disrupting credential validity.

Nonetheless, it is still possible to make choices that weaken the security posture of the ecosystem, including at least the following:

* Sharing keys or controlling access to them carelessly

* Issuing credentials with a flimsy basis for trust

* Delegating authority to untrustworthy parties

* Delegating authority without adequate constraints

* Failing to fully verify evidence

Generally understood best practices in cybersecurity will avoid many of these problems. In addition, the following policies that are specific to VVP are strongly recommended:

1. Passports SHOULD have an aggressive timeout (e.g., 30 seconds). Signatures on passports are not anchored in a KEL, and must therefore be evaluated for age with respect to the time they were received. Overly old passports could be a replay attack (a purported second call with the same orig and dest numbers, using the same backing evidence, soon after the first.)

2. Witnesses (which MUST be used) SHOULD be used in such a way that high availability is guaranteed, and in such a way that duplicity by the controller of an AID is detected. See 11. (Verifiers will be able to see the witness policy of each AID controller, and SHOULD decide for themselves whether the party is reliable, depending on what they observe.)

3. Revocations SHOULD be timely, and the timeliness guarantees of issuers SHOULD be published.

4. Watchers SHOULD propagate events to local caches with a low latency, and MUST provide information that allows verifiers to decide whether that latency meets their freshness requirements.

9. Privacy

Institutions and individuals that make or receive phone calls as verified parties may have privacy goals. Although their goals might differ in some ways, both will wish to disclose some attributes to the counter party, and both may wish to suppress some of that same information from intermediaries. Both will want control over how this disclosure works.

9.1. Graduated Disclosure

ACDCs support a technique called _graduated disclosure_ that enables this.

The hashing algorithm for ACDCs resembles the hashing algorithm for a merkle tree. An ACDC is a hierarchical data structure that can be modeled with nested JSON. Any given layer of the structure may consist of a mixture of simple scalar values and child objects. The input to the hashing function for a layer of content equals the content of scalar fields and the _hashes_ of child objects.

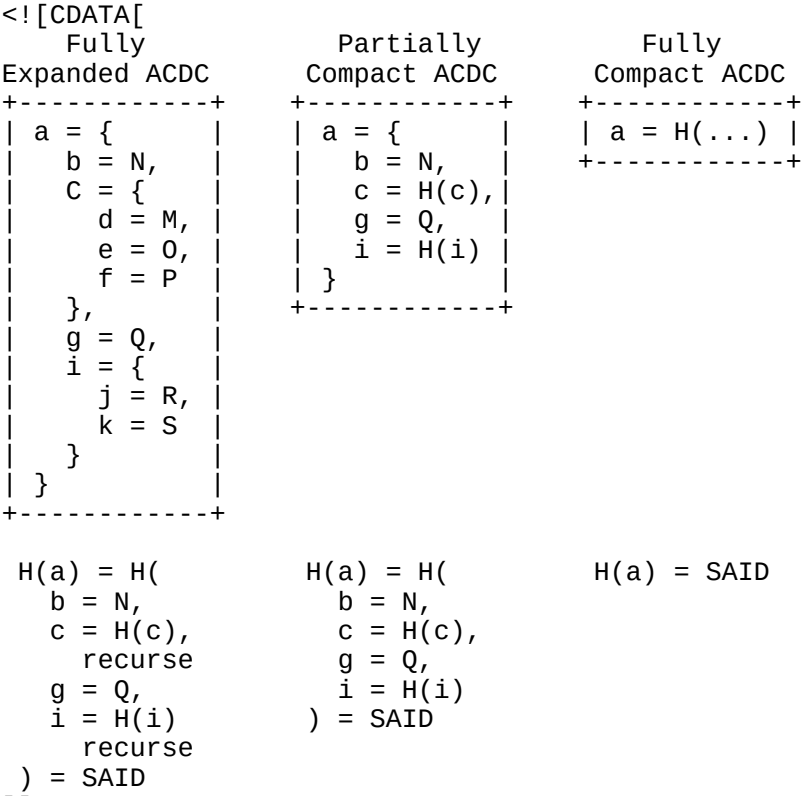

Figure 4: ACDC hashes like a Merkle tree

This means is that any given child JSON object in an ACDC can be replaced with its hash, _without altering the hash of the parent data_. Thus, there can be expanded ACDCs (where all data inside child objects is visible) or compacted ACDCs (where some or all of the child objects are opaquely represented by their equivalent hashes). A signature over an expanded ACDC is also a signature over any of the compacted versions of the same ACDC, and a revocation event over any of the versions is guaranteed to mean the same thing.

In combination with the evd claim in a passport, graduated disclosure can be used to achieve privacy goals, because different verifiers can see different variations on an ACDC, each of which is guaranteed to pass the same verification tests and has the same revocation status.

For example, suppose that company X wants to make a call to an individual in jurisdiction Y, and further suppose that auditor Z requires proof that X is operating lawfully, without knowing the name of X as a legal entity. In other words, the auditor needs to _qualify_ X but not necessarily _identify_ X. Company X can serve the KEL for its dossier from a web server that knows to return the expanded form of the vetting credential in the dossier to the individual or the individual's TSP in Y, but a compacted form of the vetting credential (revealing just the vetter's identity and their signature, but not the legal identity of the issuee, X) to auditor Z. Later, if law enforcement sees the work of the auditor and demands to know the legal identity of X, discovery of the expanded form can be compelled. When the expanded form is disclosed, it will demonstrably be associated with the compact form that Z recorded, since the qualifying and identifying forms of the ACDC have the same hash.

Company X doesn't have to engage in sophisticated sniffing of traffic by geography to achieve goals like this. It can simply say that anonymous and unsigned HTTP requests for the dossier return the compact form; anyone who wants the expanded form must make an HTTP request that includes in its body a signature over terms and conditions that enforce privacy and make the recipient legally accountable not to reshare.

Importantly, transformations from expanded to compact versions of an ACDC can be performed by anyone, not just the issuer or holder. This means that a verifier can achieve trust on the basis of expanded data, and then cache or share a compacted version of the data, meaning that any subsequent or downstream verifications can have equal assurance but higher privacy. The same policy can be applied to data any time it crosses a regulatory, jurisdictional boundary where terms and conditions for disclosure have weaker enforcement. It can also be used when business relationships should be redacted outside of a privileged context.

Schemas for credentials should be designed to allow graduated disclosure in increments that match likely privacy goals of stakeholders. ACDC schema design typically includes a salty nonce in each increment, avoiding rainbow attacks on the hashed data. VVP encourages but does not require this.

9.2. Correlation

Privacy theorists will note that, even with contractually protected graduated disclosure and maximally compact ACDCs, verifiers can still correlate by using some fields in ephemeral passports or long-lived ACDCs, and that this may undermine some privacy goals.

There are three correlators in each passport:

1. Any brand information in card (may strongly identify a VP)

2. the kid header (identifies the signer of the passport -- the OP for verified callers, or perhaps a call center or TSP automation for verified callees)

3. the evd claim (uniquely identifies a dossier used by a VP)

We discount the first correlator, because if it is present, the VP is explicitly associating its correlated reputation with a call. It has asserted this brand publicly, to every stakeholder in the SIP pipeline. In such cases, any question of the VP’s privacy is off the table, and no privacy protections on the other two correlators will be effective. However, if the first correlator is missing, the other two correlators become more interesting.

9.2.1. kid

In VVP, the passport signer role that’s identified by kid is played by automation. Automation is unlikely to have any direct privacy goal. Automation is assumed to be operated by a company, and that company is likely to be either a service provider, or a large corporation capable of significant IT investments. Either way, the signer is in the business of servicing phone calls, and is likely to be content for its traffic to be correlated publicly. Therefore, the fact that kid correlates the signer is not particularly interesting.

However, could the signer be used as an indirect correlator for the VP?

The signer’s SBC can service calls for many thousands or millions of clients, providing a some herd privacy. This is not a perfect protection, but it is a beginning. We add to this the crucial observation that _the signer doesn’t need to have a stable reputation to support VVP goals_. Trust in the signer comes from the existence of a delegated signer credential (see 6.3.9), not from a certificate or any other long-term identity. Therefore, the AID that provides cryptographic identity for a signer MAY be rotated often (as often as VPs are willing to delegate to a new one). Further, even without

rotation, a signing organization MAY provide multiple instances of its automation, each using a different AID. Also, a VP MAY delegate signing authority to multiple signing organizations, each of which is using various strategies to mitigate correlation. Taken together, these measures offers reasonable protection -- protection that a VP can tune -- against correlating a VP via kid.

9.2.2. evd

The other correlator, evd, tracks a VP more directly, because a dossier is uniquely identified by its SAID, and can only be used by a single VP. Furthermore, if someone resolves evd to an actual dossier (something that might be avoidable with judicious use of graduated disclosure), the dossier will at a minimum have an issuer field that ties it to the VP as a perfect correlator.

One answer here is to introduce a _VP blinding service_. This service creates _derived dossiers_ on a schedule or by policy. Each derivation includes the hash of the original dossier, in a field that is hidden but available (along with a salty nonce) via graduated disclosure. The derived dossier is signed by the blinding service rather than the original VP. It embodies an assertion, by the blinding service, that it has verified the original dossier according to published rules, and that it will revoke the derivative if the original is revoked. VP blinding services would have to be trusted by verifiers, much like root CAs in SHAKEN. However, unlike CAs, their actions could be trivially audited for correctness, since every derivation would have to be backed by a dossier that has the associated hash. Such a mechanism is probably unnecessary for b2c calling, but may be justified when VVP is used by individual VPs if they wish to merely qualify without identifying themselves to some intermediaries or callees.

10. Appendix A: Evidence theory

Most existing approaches to secure telephony uses X509 certificates [RFC5280] for foundational identity. Certificates have great virtues. Notably, they are well understood, and their tooling is ubiquitous and mature. However, they also have some serious drawbacks. They are protected by a single key whose compromise is difficult to detect. Recovery is cumbersome and slow. As a result, _certificates are far more temporary than the identities they attest_.

This has numerous downstream consequences. When foundational evidence of identity has to be replaced constantly, the resulting ecosystem is fragile, complex, and expensive for all stakeholders. Vulnerabilities abound. Authorizations can only be analyzed in a

narrow _now window_, never at arbitrary moments in time. This creates enormous pressure to build a centralized registry, where evidence can be curated once, and where the cost of reacting to revocations is amortized. The entire fabric of evidence has to be rebuilt from scratch if quantum security becomes a requirement.

In contrast, the issuers and holders of ACDCs -- and thus, the stakeholders in VVP passports -- are identified by autonomic identifiers, not raw keys. This introduces numerous security benefits. Keys, key types, and signing algorithms can all change (even for post-quantum upgrades) without invalidating evidence. Signing and rotation operations are sequenced deterministically, making historical audits possible. Key compromises are detected as soon as an attacker attempts consequential actions. Recovery from compromise is trivial. Multisig signing policies allow diffuse, nuanced control.

The result is that _identities in ACDCs are as stable as identities in real organizations_. This makes delegations and chaining mechanisms far more robust than their analogs in certificates, and this in turn makes the whole ecosystem safer, more powerful, and easier to maintain. Revocations are cheap and fast. No central registries are needed, which eliminates privacy concerns and regulatory hurdles. Adoption can be opportunistic; it doesn’t require a central mandate or carefully orchestrated consensus throughout a jurisdiction before it can deliver value.

ACDCs make it practical to model nuanced, dynamic delegations such as the one between Organization X and Call Center Y. This eliminates the gap that alternative approaches leave between accountable party and the provider of call evidence. Given X’s formal approval, Y can sign a call on behalf of X, using a number allocated to X, and using X’s brand, without impersonating X. They can also prove to any OSP or any other party, in any jurisdiction, that they have the right to do so. Furthermore, the evidence that Y cites can be built and maintained by X and Y, doesn’t get stale or require periodic reissuance, and doesn’t need to be published in a central registry.

Even better, when such evidence is filtered through suballocations or crosses jurisdictional boundaries, it can be reused, or linked and transformed, without altering its robustness or efficiency. Unlike W3C verifiable credentials and SD-JWTs, which require direct trust in the proximate issuer, ACDCs and the JWTs that reference them verify data back to a root through arbitrarily long and complex chains of issuers, with only the root needing to be known and trusted by the verifier.

The synergies of these properties mean that ACDCs can be permanent, flexible, robust, and low-maintenance. In VVP, no third party has to guess who's accountable for an outbound call or who's answering an inbound call; that party is transparently and provably accountable, period. (Yet notwithstanding this transparency, ACDCs support a form of pseudonymity and graduated disclosure that satisfies vital privacy and data processing constraints. See 9.)

11. Appendix B: Witnesses and Watchers

A full description of witnesses and watchers is available in [TOIP-KERI]. Here, we merely summarize.

A KERI _witness_ is a lightweight server that acts as a notary. It exposes a standard interface. It receives signed events from the controller of an identifier that it services. If these events are properly sequenced and aligned with the identifier's signing policy and key state, they are recorded and become queryable, typically by the public. KERI allows the controller of an autonomic identifier to choose zero or more witnesses. The witnesses can change over the lifecycle of the identifier. However, the relationship between an identifier and its witnesses cannot be changed arbitrarily; the controller of the identifier makes a cryptographic commitment to its witnesses, and can only change that commitment by satisfying the signing policy of the identifier. In VVP, identifiers used by issuers MUST have at least one witness, because this guarantees viral discoverability, and SHOULD have at least 3 witnesses, because this guarantees both high availability and the detection of duplicity by the controller of the identifier.

Witnesses provide, for VVP, many of the security guarantees that alternate designs seek from blockchains. However, witnesses are far more lightweight than blockchains. They can be run by anyone, without coordination or approval, and can be located in any jurisdiction that the owner of the identifier prefers, satisfying regulatory requirements about data locality. Although a single witness may service mulptiple identifiers, the records related to any single identifier are independent, and no consensus algorithm is required to order them relative to others. Thus, every identifier's data evolves in parallel, without bottlenecks, and any identifier can be deleted without affecting the integrity of other identifiers' records, satisfying regulatory requirements about erasure. Witnesses only store (and thus, can only expose to the public) what a given data controller has instructed them to store and publish. Thus, witnesses do not create difficulties with consent or privacy.

In VVP, when a party shares an identifier or a piece of evidence, they do so via a special URL called an OOBI (out of band invitation). The OOBI serves a tamper-evident KEL (6.2.8) that reveals the full, provable history of the key state and other witnesses for the identifier, and even includes a forward reference to new witnesses, if they have changed. It also allows the discovery of issuance and revocation events, and their sequence relative to one another and to key state changes.

An additional and optional feature in KERI is enabled by adding _watchers_. Watchers are lightweight services that synthesize witness data. They may MAY monitor multiple witnesses and enable hyper-efficient caching. They SHOULD also compare what multiple witnesses for a given identifier are saying, which prevents controllers of an identifier from forking reality in a duplicitous way, and which can detect malicious attempts to use stolen keys.

Witnesses are chosen according to the preference of each party that controls an identifier, and a mature ecosystem could have dozens, hundreds, or thousands. Watchers, on the other hand, address the needs of verifiers, because they distill some or all of the complexity in an ecosystem down to a single endpoint that verifiers can query. Any verifier can operate a watcher at any time, without any coordination or approval. Viral discoverability can automatically populate the watcher’s cache, and keep it up-to-date as witness data evolves.

Verifiers can share watchers if they prefer. Anything that watchers assert must be independently verified by consulting witnesses, so watchers need not have a complete picture of the world, and they are a convenience rather than an oracle that must be trusted. The data that watchers synthesize is deliberately published by witnesses for public consumption, at the request of each data stream’s associated data controllers, and does not represent surveillance (9). If a watcher can no longer find witness data to back one of its assertions, it MUST delete the data to satisfy its contract. This means that acts of erasure on witnesses propagate to watchers, again satisfying regulatory erasure requirements.

12. Appendix C: Sample Credentials

12.1. Common fields

Some structure is common to all ACDCs. For details, consult [TOIP-ACDC]. Here, we provide a short summary.

* v _(required)_ Contains a version statement.

* d _(required)_ Contains the SAID (6.2.1) of the ACDC. (Nested d fields contain SAIDs of nested JSON objects, as discussed in 9.1.

* i _(required)_ In the outermost structure, contains the AID (6.2.3) of an issuer. Inside a, contains the AID of the issuee.

* ri _(optional)_ Identifies a registry that tracks revocations that might include one for this credential.

* s _(required)_ Contains the SAID of a schema to which the associated ACDC conforms.

* a _(required)_ Contains additional attributes for this specific ACDC, as allowed by its schema.

* dt _(optional)_ Contains the date when the issuer claims to have issued the ACDC. This data will correspond closely with a timestamp saved in the issuer's KEL, at the point where the signature on the ACDC was signed and anchored there. The ordering of the signature in the KEL, relative to other key state events, is what is definitive here; the timestamp itself should be viewed more as a hint.

* e _(optional)_ Contains edges that connect this ACDC to other data upon which it depends.

* r _(optional)_ Contains one or more rules that govern the use of the ACDC. Holding the credential requires a cryptographically nonrepudiable admit action with a wallet, and therefore proves that the holder agreed to these terms and conditions.

All ACDCs are validated against a schema that conforms to [JSON-SCHEMA]. Below we show some sample credentials and their corresponding schemas. VVP does not require these specific schemas, but rather is compatible with any that have roughly the same information content.

12.2. Vetting credential

The schema of a vetting credential (6.3.5) can be very simple; it needs to identify the issuer and issuee by AID, and it needs to identify the vetted legal entity in at least one way that is unambiguous. Here is a sample LE vLEI that meets these requirements. The issuer's AID appears in the first i field, the issuee in the second i field, and the connection to a vetted legal entity in the LEI field. (The validity of this credential depends on its issuer having a valid, unrevoked QVI credential; the specifc credential it links to is conveyed in e. The full text of rules has been elided to

keep the example short.)


```
{
  "v":"ACDC10JSON0005c8_",
  "d":"Ebyg1epjv7D4-6mvl44Nlde1hTyL8413LZbY-mz60yI9",
  "i":"Ed88Jn6CnWpNbSYz6vp9DOSpJH2_Di5MSwWTf1l34JJm",
  "ri":"Ekfi58Jiv-NVqr6GOrxgxzhrE5RsDaH4QNwv9rCyZCwZ",
  "s":"ENPXp1vQzRF6JwIuS-mp2U8Uf1MoADoP_GqQ62VsDZWY",
  "a":{
    "d":"EdjPlxlRyujxarfXHCwFAqSV-yr0XrTE3m3XdFaS6U3K",
    "i":"Eeu5zT9ChsawBt2UXdU3kPIf9_lFqT5S9Q3yLZvKVfN6",
    "dt":"2024-09-19T13:48:21.779000+00:00",
    "LEI":"9845006A4378DFB4ED29"
  },
  "e":{
    "d":"EeyVJC9yZKpbIC-LcDhmlS8YhrjD4VIUBZUOibohGXit",
    "qvi":{
      "n":"EmatUqz_u9BizxwOc3JishC4MyXfiWzQadDpgCBA6X9n",
      "s":"EBfdlu8R27Fbx-ehrqwImnK-8Cm79sqbAQ4MmvEAYqao"
    }
  },
  "r":{
    "d":"EgZ97EjPSINR-O-KHDN_uw4fdrTxeuRXrqT5ZHHQJujQ",
    "usageDisclaimer":{
      "l":"Usage of a valid...fulfilled."
    },
    "issuanceDisclaimer":{
      "l":"All information...Governance Framework."
    }
  }
}
```


The schema that governs this credential, ENPX...DZWY, is shown in the s field. LE vLEI credential schemas are managed by GLEIF and published at [LE-VLEI-SCHEMA].

An alternate schema for vetting credentials -- one that incurs less effort to quality and to perform vetting, but that offers correspondingly lower levels of assurance, is published at [ORG-VET-SCHEMA].

As fundamentally public artifacts that are issued only to organizations, most vetting credentials will not be designed for graduated disclosure (9.1). Vetting credentials for individuals would require a different schema -- perhaps one that documents their full legal name but allows disclosure strategies such as first name + last initial, or first initial plus last name.

12.3. TNAlloc credential

A TNAlloc credential needs to identify its issuer and issuee. If and only if it isn't issued by a national regulator that acts as a root of trust on allocation questions, it also needs to cite an upstream allocation that justifies the issuer's right to pass along a subset of the numbers it controls.

Here is a sample TNAlloc credential that meets these requirements.


```
{
  "v": "ACDC10JSON0003cd_",
  "d": "EEeg55Yr01gDyCScFUaE2QgzC7IOjQRpX2sTckFZp1RP",
  "u": "0AC8kpfo-uHQvxkuGZdlSjGy",
  "i": "EANghOmfYKURt3rufd9JNzQDw_7sQFxnDlIew4C3YCnM",
  "ri": "EDoSO5PEPLsstDr_XXa8aHAf0YKfPlJQcxZvkpMSzQDB",
  "s": "EFvnoHDY7I-kaBBeKlbDbkjG4BaI0nKLGadxBdjMGgSQ",
  "a": {
      "d": "ECFFejktQA0ThTqLtAUTmW46unVGf28I_arbBFnIwnWB",
      "u": "0ADSLntzn8x8eNU6PhUF26hk",
      "i": "EERawEn-XgvmDR_-2ESVUVC6pW-rkqBkxMTsL36HosAz",
      "dt": "2024-12-20T20:40:57.888000+00:00",
      "numbers": {
          "rangeStart": "+33801361002",
          "rangeEnd": "+33801361009"
      },
      "channel": "voice",
      "doNotOriginate": false
  },
  "e": {
      "d": "EI9qlgiDbMeJ7JTZTJfVanUFAoa0TMz281loi63nCSAH",
      "tnalloc": {
          "n": "EG16t8CpJROovnGpgEW1_pLxH5nSBs1xQCbRexINYJgz",
          "s": "EFvnoHDY7I-kaBBeKlbDbkjG4BaI0nKLGadxBdjMGgSQ",
          "o": "I2I"
      }
  },
  "r": {
      "d": "EJFhpp0uU7D7PKooYM5QIO1hhPKTjHE18sR4Dn0GFscR",
      "perBrand": "Issuees agree not to share..."
  }
}
```


The schema used by this particular credential, EFvn...GgSQ, is published at [TN-ALLOC-SCHEMA].

12.4. Brand credential

TODO ~~~json ~~~

12.5. Brand proxy credential

A brand proxy credential (6.3.8) is very similar to a delegated signer credential, in that it proves carefully constrained delegated authority. The difference lies in what authority is delegated (proxy a brand vs. sign passports).

A Generalized Cooperative Delegation (GCD) credential embodies delegated but constrained authority in exactly this way. A GCD credential suitable for use as a brand proxy in VVP might look like this:


```
{
    "v": "ACDC10JSON00096c_",
    "d": "EWQpU3nrKyJBgUJGw5461CbWcug9BZj7WXUkKbNOlnFx",
    "u": "0ADE6oAxBl4E7uKeGUb7BEYi",
    "i": "EC4SuEyzrRwu3FWFrK0Ubd9xejlo5bUwAtGcbBGUk2nL",
    "ri": "EM2YZ78SKE8eO4W1lQOJeer5xKZqLmJV7SPr3Ji5DMBZ",
    "s": "EL7irIKYJL9Io0hhKSGWI4OznhwC7qgJG5Qf4aEs6j0o",
    "a": {
        "d": "EPQhEk5tfXvxyKe5Hk4DG63dSgoP-F2VZrxuIeIKrT9B",
        "u": "0AC9kH8q99PTCQNteGyI-F4g",
        "i": "EIkxoE8eYnPLCydPcyc_lhQgwOdBHwzkSe36e2gqEH-5",
        "dt": "2024-12-27T13:11:29.062000+00:00",
        "c_goal": ["ops.telco.*.proxybrand"],
        "c_proto": ["VVP:OP,callee"]
    },
    "r": {
        "d": "EFthNcTE20MLMaCOoXlSmNtdooGEbZF8uGmO5G85eMSF",
        "noRoleSemanticsWithoutGfw": "All parties agree...",
        "issuerNotResponsibleOutsideConstraints": "Although verifiers...",
        "noConstraintSansPrefix": "Issuers agree...",
        "useStdIfPossible": "Issuers agree...",
        "onlyDelegateHeldAuthority": "Issuers agree..."
    }
}
```


Note the c_goal field that limits goals that can be justified with this credential, and the c_proto field that says the delegate can only exercise this authority in the context of the "VVP" protocol with the "OP" or "callee" role. The wildcard in c_goal and the addition of the "callee" role in c_proto are complementary changes that allow this credential to justify proxying the brand on both outbound and inbound calls. (Branding on inbound calls is out of

scope for VVP, but is included here just to show that the same credentials can be used for both VVP and non-VVP solutions. To convert this credential to a purely outbound authorization, replace the wildcard with send, and limit the roles in VVP to OP.)

The schema for GCD credentials, and an explanation how to add additional constraints, is documented at [GCD-SCHEMA].

12.6. Delegated signer credential

A delegated signer credential (6.3.9) must prove that the issuer is giving authority to the issuee. This authority should be carefully constrained so that it applies only to outbound voice calls, not to signing invoices or legal contracts. It can also be constrained so it only applies on a particular schedule, or when the call originates or terminates in a particular geo or jurisdiction.

A Generalized Cooperative Delegation (GCD) credential embodies delegated but constrained authority in exactly this way. A GCD credential suitable for use as a delegated signer credential in VVP might look like this:


```
{
    "v": "ACDC10JSON00096c_",
    "d": "EDQpU3nrKyJBgUJGw5461CbWcug9BZj7WXUkKbNOlnFR",
    "u": "0ADE6oAxBl4E7uKeGUb7BEYi",
    "i": "EC4SuEyzrRwu3FWFrK0Ubd9xejlo5bUwAtGcbBGUk2nL",
    "ri": "EM2YZ78SKE8eO4W1lQOJeer5xKZqLmJV7SPr3Ji5DMBZ",
    "s": "EL7irIKYJL9Io0hhKSGWI4OznhwC7qgJG5Qf4aEs6j0o",
    "a": {
        "d": "EPQhEk5tfXvxyKe5Hk4DG63dSgoP-F2VZrxuIeIKrT9B",
        "u": "0AC9kH8q99PTCQNteGyI-F4g",
        "i": "EIkxoE8eYnPLCydPcyc_lhQgwOdBHwzkSe36e2gqEH-5",
        "dt": "2024-12-27T13:11:29.062000+00:00",
        "c_goal": ["ops.telco.send.sign"],
        "c_proto": ["VVP:OP"]
    },
    "r": {
        "d": "EFthNcTE20MLMaCOoXlSmNtdooGEbZF8uGmO5G85eMSF",
        "noRoleSemanticsWithoutGfw": "All parties agree...",
        "issuerNotResponsibleOutsideConstraints": "Although verifiers...",
        "noConstraintSansPrefix": "Issuers agree...",
        "useStdIfPossible": "Issuers agree...",
        "onlyDelegateHeldAuthority": "Issuers agree..."
    }
}
```

Note the c_goal field that limits goals that can be justified with this credential, and the c_proto field that says the delegate can only exercise this authority in the context of the "VVP" protocol with the "OP" role.

The schema for GCD credentials, and an explanation how to add additional constraints, is documented at [GCD-SCHEMA].

12.7. Dossier

A dossier (6.3.2) contains little direct data of its own. It consists almost entirely of edges -- that is, links to other credentials. Here’s what one might look like:

```
{
  "v": "ACDC10JSON00036f_",
  "d": "EKvpcshjgjzdCWwR4q9VnlsUwPgfWzmy9ojMpTSzNcEr",
  "i": "EIkxoE8eYnPLCydPcyc_lhQgwOdBHwzkSe36e2gqEH-5",
  "ri": "EMU5wN33VsrJKlGCwk2ts_IJi67IXE6vrYV3v9Xdxw3p",
  "s": "EFv3_L64_xNhOGQkaAHQTI-lzQYDvlaHcuZbuOTuDBXj",
  "a": {
    "d": "EJnMhz8MJxmI0epkq7D1zzP5pGTbSb2YxkSdczNfcHQM",
    "dt": "2024-12-27T13:11:41.865000+00:00"
  },
  "e": {
    "d": "EPVc2ktYnZQOwNs34lO1YXFOkT51lzaILFEMXNfZbGrh",
    "vetting": {
      "n": "EIpaOx1NJc0N_Oj5xzWhFQp6EpB847yTex62xQ7uuSQL",
      "s": "ENPXp1vQzRF6JwIuS-mp2U8Uf1MoADoP_GqQ62VsDZWY",
      "o": "NI2I"
    },
    "alloc": {
      "n": "EEeg55Yr01gDyCScFUaE2QgzC7IOjQRpX2sTckFZp1RP",
      "s": "EFvnoHDY7I-kaBBeKlbDbkjG4BaI0nKLGadxBdjMGgSQ",
      "o": "I2I"
    },
    "brand": {
      "n": "EKSZT4yTtsZ2AqriNKBvS7GjmsU3X1t-S3c69pHceIXW",
      "s": "EaWmoHDYbkjG4BaI0nK7I-kaBBeKlbDLGadxBdSQjMGg",
      "o": "I2I"
    },
    "bproxy": {
      "n": "EWQpU3nrKyJBgUJGw5461CbWcug9BZj7WXUkKbNOlnFx",
      "s": "EL7irIKYJL9Io0hhKSGWI4OznhwC7qgJG5Qf4aEs6j0o",
      "o": "I2I"
    },
    "delsig": {
      "n": "EMKcp1-AvpW0PZdThjK3JCbMsXAmrqB9ONa1vZyTppQE",
      "s": "EL7irIKYJL9Io0hhKSGWI4OznhwC7qgJG5Qf4aEs6j0o",
      "o": "NI2I"
    }
  }
}
```


Notice how each named edge references one of the previous sample credentials in its n field, and that other credential’s associated schema in the s field.

The schema for this credential is documented at [DOSSIER-SCHEMA].

13. IANA Considerations

This document defines a new SDP [RFC8866] session-level attribute:

Attribute name: callee-passport Long-form description: Contains a STIR-compatible passport that references a dossier of evidence about the callee’s identity, brand, and related attributes. Used in 200 OK and/or 180 Ringing responses. Type of attribute: session-level Subject to charset: No Reference: This document

This specification also depends on OOBIs (see 6.2.3) being served as web resources with IANA content type application/json+cesr.

14. References

14.1. Normative References

[ATIS-1000074]
Alliance for Telecommunications Industry Solutions, "Signature-Based Handling of Asserted Information Using toKENs (SHAKEN)", February 2019, <https://atis.org/resources/signature-based-handling-of-asserted-information-using-tokens-shaken-atis-1000074-e/>.

[FIPS186-4]
National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)", July 2013, <https://doi.org/10.6028/NIST.FIPS.186-4>.

[ISO-17442-1]
International Organization for Standardization, "Financial services 窶Legal entity identifier (LEI) Part 1: Assignment", 2020, <https://www.iso.org/standard/78829.html>.

[ISO-17442-3]
International Organization for Standardization, "inancial services Legal entity identifier (LEI) Part 3: Verifiable LEIs (vLEIs)", 2024, <https://www.iso.org/standard/85628.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <https://www.rfc-editor.org/rfc/rfc3261>.

[RFC4353] Rosenberg, J., "A Framework for Conferencing with the Session Initiation Protocol (SIP)", RFC 4353, DOI 10.17487/RFC4353, February 2006, <https://www.rfc-editor.org/rfc/rfc4353>.

[RFC4575] Rosenberg, J., Schulzrinne, H., and O. Levin, Ed., "A Session Initiation Protocol (SIP) Event Package for Conference State", RFC 4575, DOI 10.17487/RFC4575, August 2006, <https://www.rfc-editor.org/rfc/rfc4575>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/rfc/rfc4648>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC5626] Jennings, C., Ed., Mahy, R., Ed., and F. Audet, Ed., "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)", RFC 5626, DOI 10.17487/RFC5626, October 2009, <https://www.rfc-editor.org/rfc/rfc5626>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/rfc/rfc8032>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018, <https://www.rfc-editor.org/rfc/rfc8224>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/rfc/rfc8225>.

[RFC8866] Begen, A., Kyzivat, P., Perkins, C., and M. Handley, "SDP: Session Description Protocol", RFC 8866, DOI 10.17487/RFC8866, January 2021, <https://www.rfc-editor.org/rfc/rfc8866>.

[TOIP-ACDC] Smith, S., Feairheller, P., Griffin, K., Ed., and Trust Over IP Foundation, "Authentic Chained Data Containers (ACDC)", November 2023, <https://trustoverip.github.io/tswg-acdc-specification/>.

[TOIP-CESR] Smith, S., Griffin, K., Ed., and Trust Over IP Foundation, "Composable Event Streaming Representation (CESR)", November 2023, <https://trustoverip.github.io/tswg-cesr-specification/>.

[TOIP-KERI] Smith, S., Griffin, K., Ed., and Trust Over IP Foundation, "Key Event Receipt Infrastructure (KERI)", January 2024, <https://trustoverip.github.io/tswg-keri-specification/>.

14.2. Informative References

[ARIES-RFC-0519] Hardman, D., "Aries RFC 0519: Goal Codes", April 2021, <https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0519-goal-codes/README.md>.

[CITATION-SCHEMA] Hardman, D., "Citation Schema", April 2025, <https://github.com/provenant-dev/public-schema/blob/main/citation/index.md>.

[CTIA-BCID] CTIA, "Branded Calling ID Best Practices", November 2022, <https://api.ctia.org/wp-content/uploads/2022/11/Branded-Calling-Best-Practices.pdf>.

[DOSSIER-SCHEMA] Singh, A., "Verifiable Voice Dossier", January 2025, <https://github.com/provenant-dev/public-schema/blob/main/vvp-dossier/vvp-dossier.schema.json>.

[F2F-SCHEMA]
Hardman, D., "Face-to-Face Credentials", December 2023, <https://github.com/provenant-dev/public-schema/blob/main/face-to-face/index.md>.

[GCD-SCHEMA]
Hardman, D., "Generalized Cooperative Delegation (GCD) Credentials", December 2023, <https://github.com/provenant-dev/public-schema/blob/main/gcd/index.md>.

[GSMA-RCS] GSMA, "Rich Communication Suite - Advanced Communications Services and Client Specification, version 11.0", October 2019, <https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2019/10/RCC.07-v11.0.pdf>.

[JSON-SCHEMA]
JSON Schema Community, "JSON Schema Specification 2020-12", June 2022, <https://json-schema.org/specification>.

[LE-VLEI-SCHEMA]
GLEIF, "Legal Entity vLEI Credential", November 2023, <https://github.com/GLEIF-IT/vLEI-schema/blob/main/legal-entity-vLEI-credential.json>.

[ORG-VET-SCHEMA]
Hardman, D., "Org Vet Credentials", June 2025, <https://github.com/provenant-dev/public-schema/blob/main/org-vet/index.md>.

[PERSONHOOD-CRED]
Adler, S., Hitzig, Z., Jain, S., Brewer, C., Chang, W., DiResta, R., Lazzarin, E., McGregor, S., Seltzer, W., Siddarth, D., Soliman, N., South, T., Spelliscy, C., Sporny, M., Srivastava, V., Bailey, J., Christian, B., Critch, A., Falcon, R., Flanagan, H., Duffy, K. H., Ho, E., Leibowicz, C. R., Nadhamuni, S., Rozenshtein, A. Z., Schnurr, D., Shapiro, E., Strahm, L., Trask, A., Weinberg, Z., Whitney, C., and T. Zick, "Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online", August 2024, <https://arxiv.org/pdf/2408.07892>.

[RCD-DRAFT]
Wendt, C. and J. Peterson, "SIP Call-Info Parameters for Rich Call Data", Work in Progress, Internet-Draft, draft-ietf-sipcore-callinfo-rcd-19, 21 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sipcore-callinfo-rcd-19>.

[RCD-PASSPORT]
Wendt, C. and J. Peterson, "PASSporT Extension for Rich Call Data", Work in Progress, Internet-Draft, draft-ietf-stir-passport-rcd-26, 5 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-stir-passport-rcd-26>.

[RFC3262] Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, DOI 10.17487/RFC3262, June 2002, <https://www.rfc-editor.org/rfc/rfc3262>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[RFC6350] Perreault, S., "vCard Format Specification", RFC 6350, DOI 10.17487/RFC6350, August 2011, <https://www.rfc-editor.org/rfc/rfc6350>.

[RFC7095] Kewisch, P., "jCard: The JSON Format for vCard", RFC 7095, DOI 10.17487/RFC7095, January 2014, <https://www.rfc-editor.org/rfc/rfc7095>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/rfc/rfc7519>.

[RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", RFC 8226, DOI 10.17487/RFC8226, February 2018, <https://www.rfc-editor.org/rfc/rfc8226>.

[RFC8588] Wendt, C. and M. Barnes, "Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)", RFC 8588, DOI 10.17487/RFC8588, May 2019, <https://www.rfc-editor.org/rfc/rfc8588>.

[SD-JWT-DRAFT]
Fett, D., Yasuda, K., and B. Campbell, "Selective Disclosure for JWTs (SD-JWT)", Work in Progress, Internet-Draft, draft-ietf-oauth-selective-disclosure-jwt-22, 29 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-oauth-selective-disclosure-jwt-22>.

[TN-ALLOC-SCHEMA]
Provenant, "TN Allocation Credential", December 2024, <https://github.com/provenant-dev/public-schema/blob/main/tn-alloc/tn-alloc.schema.json>.

[VCON-DRAFT]
Petrie, D. and T. McCarthy-Howe, "The JSON format for vCon - Conversation Data Container", Work in Progress, Internet-Draft, draft-ietf-vcon-vcon-container-03, 19 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-vcon-vcon-container-03>.

[W3C-DID] Guy, A., Ed., Reed, D., Ed., Sporny, M., Ed., and M. Sabadello, Ed., "Decentralized Identifiers (DIDs) v1.0", W3C REC REC-did-core-20220719, W3C REC-did-core-20220719, 19 July 2022, <https://www.w3.org/TR/2022/REC-did-core-20220719/>.

[W3C-VC] Zundel, B., Ed., Burnett, D., Ed., Longley, D., Ed., Noble, G., Ed., Hartog, K. D., Ed., and M. Sporny, Ed., "Verifiable Credentials Data Model v1.1", W3C REC REC-vc-data-model-20220303, W3C REC-vc-data-model-20220303, 3 March 2022, <https://www.w3.org/TR/2022/REC-vc-data-model-20220303/>.

Acknowledgments

Much of the cybersecurity infrastructure used by VVP depends on KERI, which was invented by Sam Smith, and first implemented by Sam plus Phil Fairheller, Kevin Griffin, and other technical staff at GLEIF. Thanks to logistical support from Trust Over IP and the Linux Foundation, and to a diverse community of technical experts in those communities and in the Web of Trust group.

Techniques that apply KERI to telco use cases were developed by Daniel Hardman, Randy Warshaw, and Ruth Choueka, with additional contributions from Dmitrii Tychinin, Yaroslav Lazarev, Arshdeep Singh, and many other staff members at Provenant, Inc. Thanks as well to Ed Eykholt for multiple editorial improvements.

Author’s Address

Daniel Hardman
Provenant, Inc
Email: daniel.hardman@gmail.com