vcon
Internet-Draft
Intended status: Standards Track
Expires: 22 January 2026

T. McCarthy-Howe
Strolid, Inc.
S. Lasker
Independent
D. James
Marashlian & Donahue, PLLC

21 July 2025

vCon Lifecycle Management using SCITT
draft-howe-vcon-lifecycle-00

Abstract

This document proposes using the SCITT (Supply Chain, Integrity, Transparency, and Trust) protocol to record, communicate and coordinate the lifecycle of Virtual Conversations (vCons), which are standardized containers for conversational data like call recordings, transcripts, and chat logs. While vCons enable capturing and sharing conversation details for AI analysis and business purposes, they lack mechanisms for proving compliance with privacy regulations and consent management. SCITT addresses this by providing an immutable, append-only transparency ledger that records key lifecycle events— from vCon creation and consent management to call recording, as well as data processing and deletion— enabling entities to demonstrate regulatory compliance and maintain trust across distributed systems. The framework specifically addresses consent management challenges under regulations like GDPR and CCPA, where consent can be revoked at any time, requiring coordinated deletion across all parties that have received the vCon. By combining vCons with SCITT, organizations can build scalable, transparent governance systems that protect personal data rights while enabling responsible use of conversational data for AI and business applications.

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://howethomas.github.io/vcon-dev/draft-howe-vcon-lifecycle.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-howe-vcon-lifecycle/.

Discussion of this document takes place on the Virtualized Conversations Working Group mailing list (mailto:vcon@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/vcon/. Subscribe at https://www.ietf.org/mailman/listinfo/vcon/.

Source for this draft and an issue tracker can be found at https://github.com/vcon-dev/draft-howe-vcon-lifecycle.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Virtual Conversations (vCons) draft-vcon (https://datatracker.ietf.org/wg/vcon/about) are powerful means of capturing and collaborating on the details of human conversations, built to travel. They feed AI systems, enable entities to respond more accurately to customer needs, and manage the health of their business more effectively. The vCon working group focuses on passing conversational data, such as data commonly generated and collected in business and security environments, from chat logs to transcripts to recordings.

Most systems provide a way to store such information, but there are few standards or interoperability within the storage or transmission mechanisms. vCon is a framework for capturing and collaborating on the details of a Virtual Conversation, feeding AI systems, and enabling entities to respond to customer needs more accurately and manage their business's health more effectively.

The two opposing forces influencing such information passing are trying to enforce personal data and communications privacy and providing the ability and interest to use conversations in various ways, e.g., AI analysis.

Although vCons are tools that enable actors to do the right thing, they are not tools that enable actors in a distributed system to prove it. However, when combined with the SCITT protocol draft-scitt (https://datatracker.ietf.org/wg/scitt/about), proof becomes practical. SCITT allows Relying Parties to obtain information

pertinent to the lifecycle of a vCon in a "transparent" way. SCITT achieves this by having producers publish information in a Transparency Service, where Relying Parties can check the information.

These relying parties can then use this information to make decisions based on the current state and context of the vCon to account for changes in consent, updates in the accuracy of the content, or amendments of the information it might contain. SCITT, the Supply Chain, Integrity, Transparency, and Trust protocol, enables clients to register statements about events, physical or virtual, such as when things are created or used. These statements are immutable and are useful to support auditing, governance, and coordination between various distributed systems.

When using vCons to define a conversation, and SCITT to record the events that occur to them, more scalable and transparent systems of governance and provenance can be constructed to support privacy efforts. It is expected that there are many situations where this governance across security boundaries is common and desired by all parties. One real-world example of this is management of consent as it applies to the use of conversations for different purposes, such as machine learning. Using conversations as inputs to machine learning has great benefit to both customers and businesses, yet only responsibly within the defense of personal data rights and compliance with personal data and communications privacy laws, united together by consent. Although consent to a call recording or personal data collection and processing is not always required under the applicable laws, seeking consent is often the best practice, given the Privacy by Design principles, multijurisdictional business operations, and the ever-changing privacy laws. Please see the privacy-primer-vcon (https://datatracker.ietf.org/doc/draft-james-privacy-primer-vcon/) for more information on consent and other data subject protection concepts.

In all of these cases, the ability to define and express the processing of conversations depends on the ability to authoritatively define the lifecycle of a vCon:

* who originated the vCon in the first place to establish provenance

* how it was analyzed and amended, to accurately respond to right-to-know requests

* the authenticity both of the original document for downstream workflow

* and authenticity of the redactions that come from the original, in service of data minimization efforts

* the various expressions of digital rights

* the sharing or deletion in response to the same digital rights

For this document and for purposes of illustration, consent will be used as an example use case. Proper consent management is fundamental to the responsible protection of data and the ability to leverage that data. Consent granted by the data subject of a vCon also needs to be stored and passed, exactly like the other information contained in a vCon. Unlike the rest of the information contained, the gathered consent is expressly not immutable. Consent, when gathered for a purpose, can also be revoked by the data subject at any time and surely after a vCon has been shared for analysis.

Multiple regulations, including the US-born California Consumer Protection Act (CCPA) CCPA (https://oag.ca.gov/privacy/ccpa) and the EU-born General Data Protection Regulation (GDPR) GDPR (https://gdpr.eu/), outline requirements for entities to use and dispose of PII information responsibly upon request. Consent, although illustrative, is not the only example of mutability in the lifecycle of a vCon. Verification of parties, improvements in the analysis, and additions of contextual attachments result in updates to a vCon after data is shared, begging for a mechanism to track and govern such changes.

To honor the working group’s charter to pass conversational data safely between consenting parties, this draft provides an overview of the requirements, a workflow and an example consent structure for using SCITT to manage the vCon lifecycle at scale, providing end-to-end, interoperable services and tooling. The workflow enables entities in the workflow to collaborate on a vCon while assuring all entities in the workflow adhere to relevant PII regulations using a SCITT Ledger. Actual implementations of these workflows are left to implementers and applications; this draft provides an authoritative list of the entries that should appear on the SCITT transparency ledger to enable them.

1.1. Acts of Trust and Transparency

Throughout this workflow, no single entity can prove that other entities performed the required actions. However, by auditing the SCITT Ledgers of all involved parties, entities can prove they acted on the acknowledged consent and intent of the Data Subject, holding other entities accountable for performing required operations. In short, this audit can help to prove that "the good guys did the right

thing", to measure the compliance of those outside this architecture who may have chosen different methods of compliance assurance.

1.2. Standards-Based Interoperability

A wide range of industries and business scenarios benefit from virtual conversations, making them valuable across countless organizations.The breadth of industries and scenarios that benefit from virtual conversations spans numerous companies. The power of this technology lies in enabling cross-conversation collaboration. By implementing a standards-based approach, both collaborative and competitive companies can easily integrate with solutions for transcription, consent management, and CRM integration.

Packaging conversations and associated metadata in the vCon format provides a standardized means to communicate what has been sent. Due to the personally identifiable information and digital fingerprinting in vCons, it’s critical to understand and adhere to regulatory requirements for PII management. Defining and implementing a standard provides stability in information management throughout the lifecycle.

Recording which vCon elements were sent to various parties holds each accountable for what was sent, what was received, and when these exchanges occurred.

1.3. What Differentiates SCITT from a Database

The information written to SCITT could be compared to information in a standard database. What makes SCITT different:

* *Immutable and Append-Only nature*: Once written, data cannot be modified or deleted

* *Cryptographic security*: Through pre-signed statements, making SCITT a notary that cannot alter contents

* *Independent verifiability*: Parties can verify data without trusting the service provider

* *Separation*: Between the immutable, append-only ledger and the evidentiary metadata store (which can be deleted/redacted for PII governance)

* *Standardized communication*: And enforcement of regulations and compliance

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 (https://www.rfc-editor.org/info/rfc8174) when, and only when, they appear in all capitals, as shown here.

The following terms, derived from CCPA (https://oag.ca.gov/privacy/ccpa), GDPR (https://gdpr.eu/) and privacy-primer-vcon (https://datatracker.ietf.org/doc/draft-james-privacy-primer-vcon/), are used throughout the document:

Conserver: A vCon workflow engine that ingests vCons, routing them for processing and enhancements. A conserver doesn’t store a vCon, rather it processes the vCon for transcription, sentiment, integrity protection on egress, verification on ingress, retrieving it from, and saving it to a vCon Registry.

Data Subject: The individual(s) whose personal information is processed (also referred to as the "consumer" in many personal data privacy laws).

Data Originator: The Entity that records and initiates the vCon, identifying the parties, including the media of the conversation. For a phone call, this may include the phone numbers and the audio recording. For internet-based calls, such as Microsoft Teams, Zoom, Google meet, this may include emails and audio/video recording. The Data Originator is a facilitator with access to the content of the call. This document addresses the instance where the Data Originator is a data processor under the applicable data privacy laws, collecting and processing data on behalf of a Data Controller. However, Data Originators may also act as Data Controllers when collecting and processing data for their own purposes. This document does not address such an instance, and implementers will need to adjust the technical process accordingly. In general, Data Originators may be required to collect consent by applicable law when acting as Data Controllers and by the relevant data processing agreements with Data Controllers when acting as Data Processors. . One or all of the Data Subjects must initiate consent, giving the Data Originator the right to record the conversation, which may be the Data Controller’s responsibility to identify.

Data Controller: An Entity or individual with decision-making authority over data processing who determines the purposes and methods of data processing, bears primary responsibility under privacy laws and is the main target of most privacy and data protection regulations. Under most data privacy laws, Data

Controllers are required to enter into data processing agreements with their Data Processors, detailing the rules for data collection and processing in accordance with applicable laws.

Data Processor: An individual or an Entity, which processes personal data on behalf of the Data Controller. It is often a third-party service provider who processes data on behalf of the data controller. Under HIPAA data processors are referred to as "business associates." Data processors may be hired for specialized tasks or to improve efficiency; can subcontract to other processors, creating a chain of responsibility; must operate within the scope defined by the data controller; and are expected to maintain trust and adhere to the controller’s guidelines. A Conserver often calls out to Data Processors for Transcription, Sentiment Analysis, Fraud Detection, email/text messaging.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data. Among other things, this includes collection, storage, use, disclosure, and deletion.

Personal Data: any information relating to an identified or identifiable Data Subject, including a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the Data Subject.

Entity: A generic reference to companies, groups or individuals that may share, alter, or use a vCon. An Entity may be a Data Originator, Data Controller, Data Processor or some other role that has not yet been defined that participates in the possession and/or processing of a vCon.

Party: A party, or participant of a vCon, as identified in the vCon draft.

SCITT Transparency Service: An append-only ledger for integrity protecting vCons, ensuring the state of a vCon is known at a point in time for conformance to governance and regulatory requirements.

vCon Registry: A storage service, capable of storing vCons, including rich metadata and larger attachments including audio and video recordings.

3. vCon Lifecycle

3.1. Example Use Case: Consent Management

The example use case, consent management, has the following requirements, all considered necessary to fulfill the proper sharing of personal information responsibly:

* As an individual, I wish to express my data subject rights to express my consent for various purposes, and to withdraw the same.

* As a member of an organization, I want to operationally assure that the processing of personal data is within the consent I gained from the data subject, and to safely record those activities to provide to both data subjects and governance bodies.

* As a regulator, I wish to have a measurement system to support compliance, bias and regulatory enforcement of policy.

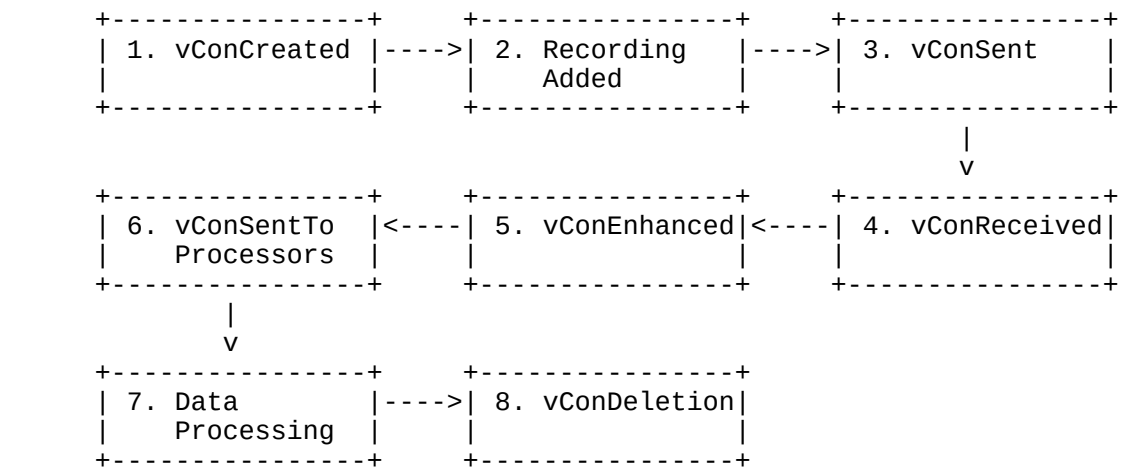
* As a technologist, I wish to maintain the integrity of conversational pipelines, maintaining the trust both stakeholders and data subjects have in the trust and transparency of the process.

3.2. vCon Lifecycle Scope

3.2.1. Creation, Distribution and Deletion

The vCon lifecycle comprises a series of phases from creation through distribution to deletion. Tracking these phases enables fundamental privacy rights, such as the right to know how your data was processed, and secures AI supply chains by establishing provenance and guaranteeing integrity.

The phases of a vCon’s life include:



1. *vConCreated*: The call completes, and a vCon is created with call metadata stored in the vCon Registry.

2. *RecordingAdded*: The actual recording is saved and added to the attachments section of the vCon.

3. *vConSent*: The Data Originator sends the vCon to the Data Controller with integrity protection using SCITT.

4. *vConReceived*: The Data Controller receives the vCon and records this in the SCITT Transparency Service.

5. *vConEnhanced*: The Data Controller adds transcription and license information and identifies themselves.

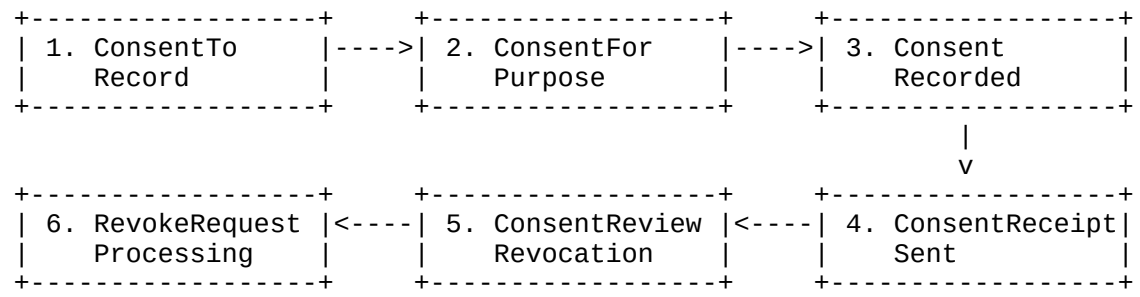
6. *vConSentToProcessors*: The Data Controller sends the vCon to relevant Data Processors.

7. *Data Processing*: Value-added services are performed on the vCon data.

8. *vConDeletion*: The vCon is deleted when no longer needed, when consent is revoked, or when it expires.

3.2.2. Digital Rights Management

Interwoven with the vCon lifecycle is consent management. A modern consent model is envisioned: consent is gathered by the Data Controller (or the Data Originator acting as a data processor on behalf of the Data Controller) for particular purposes (such as training or sharing) and can be withdrawn by the Data Subject on demand. This withdrawal may result in revoking the vCon or modifying it to remove non-consenting portions.



Lifecycle events in Digital Rights Management include:

1. *ConsentToRecord*: Consent is requested from the Data Subject to record the conversation.

2. *ConsentForPurpose*: Confirmation of consent for specific purposes (e.g., "sales followup") is obtained.

3. *ConsentRecorded*: The Data Controller records where consent was confirmed in the transcript or recording.

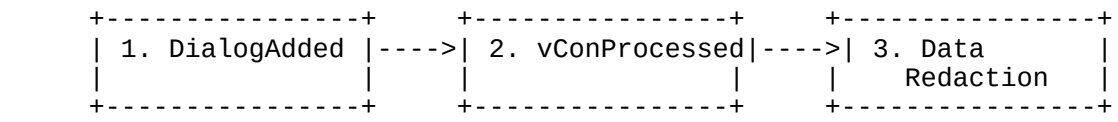
4. *ConsentReceipt Sent*: Notification is sent to Data Subject(s) with a link to review consent details.

5. *ConsentReview/Revocation*: Data Subject can review or choose to revoke consent at any time.

6. *RevokeRequestProcessing*: If consent is revoked, the request is processed and communicated to all parties.

3.2.3. Amendment of Existing vCons

Under normal circumstances, vCons may be amended. For example, at creation time, parties to a vCon may be verified through methods such as OAuth. However, if account credentials are later found to be compromised, the verification status may need revision. Party verification issues often trigger "Rights to Correct" requests and are fundamental to responsible data rights management. Other enhancements and modifications may occur for security reasons, future processing needs, or in response to regulatory changes.



Events that may be recorded on the distributed ledger include:

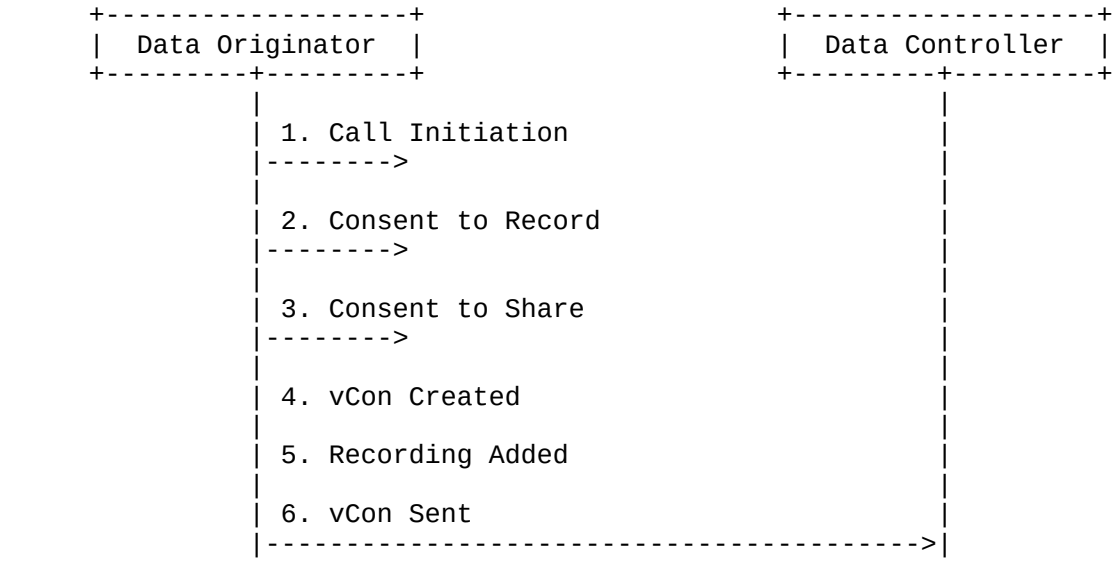
1. *DialogAdded*: A dialog is saved and added to the vCon.

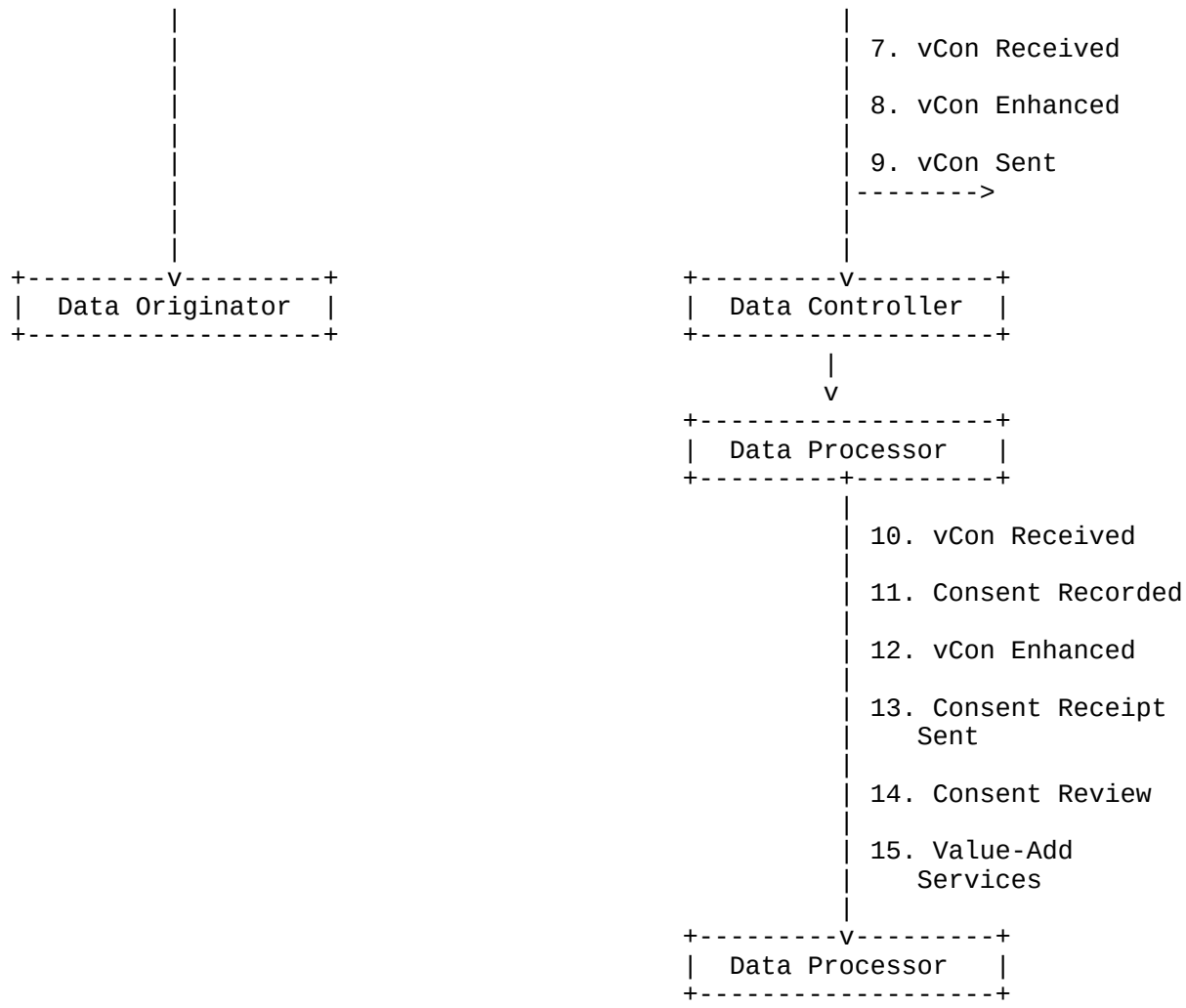
2. *vConProcessed*: The Data Controller processes the vCon.

3. *Data Redaction*: Data Processors delete the data or redact the Data Subject.

4. Detailed Use Case

4.1. vCon Create, Consent and Share





4.1.1. Data Originator

1. *Initiating Call*: An initiating caller contacts a Data Subject to provide a service.

2. *Consent to Record*: The initiating caller requests consent to record the call for training purposes.

3. *Consent to Share*: The call completes, confirming consent for the recording to be used for "sales followup", noting that the Data Subject can review and revoke consent later. Depending on the types of personal data communicated on the call and the purpose of its processing, the consent request language may need to include additional information.

4. *vCon Created*: The call completes, the vCon is created, and call metadata is recordedin the vCon Registry.

5. *Recording Added*: The recording is saved to the vCon Registry, adding it to the vCon’s attachments section.

6. *vCon Sent*: The Data Originator completes their responsibilities and sends the vCon to the Data Controller.

4.1.2. Data Controller

1. *vCon Received*: The vCon is received from the Data Originator, and a vcon_received operation is recorded in the SCITT Transparency Service.

2. *vCon Enhanced with License and Data Controller*: The Data Controller adds transcription, specifies the intended license, and identifies themselves as the Data Controller on the vCon.

3. *vCon Sent*: The Data Controller sends the vCon to the Data Processor(s).

4.1.3. Data Processor(s)

1. *vCon Received*: The Data Processor validates the vCon’s SCITT receipt from the Data Controller.

2. *Consent Recorded*: The Data Processor records consent confirmation in the SCITT Transparency Service.

3. *vCon Enhanced*: Sentiment analysis and other enhancements are processed through the Data Processor’s Conserver workflows.

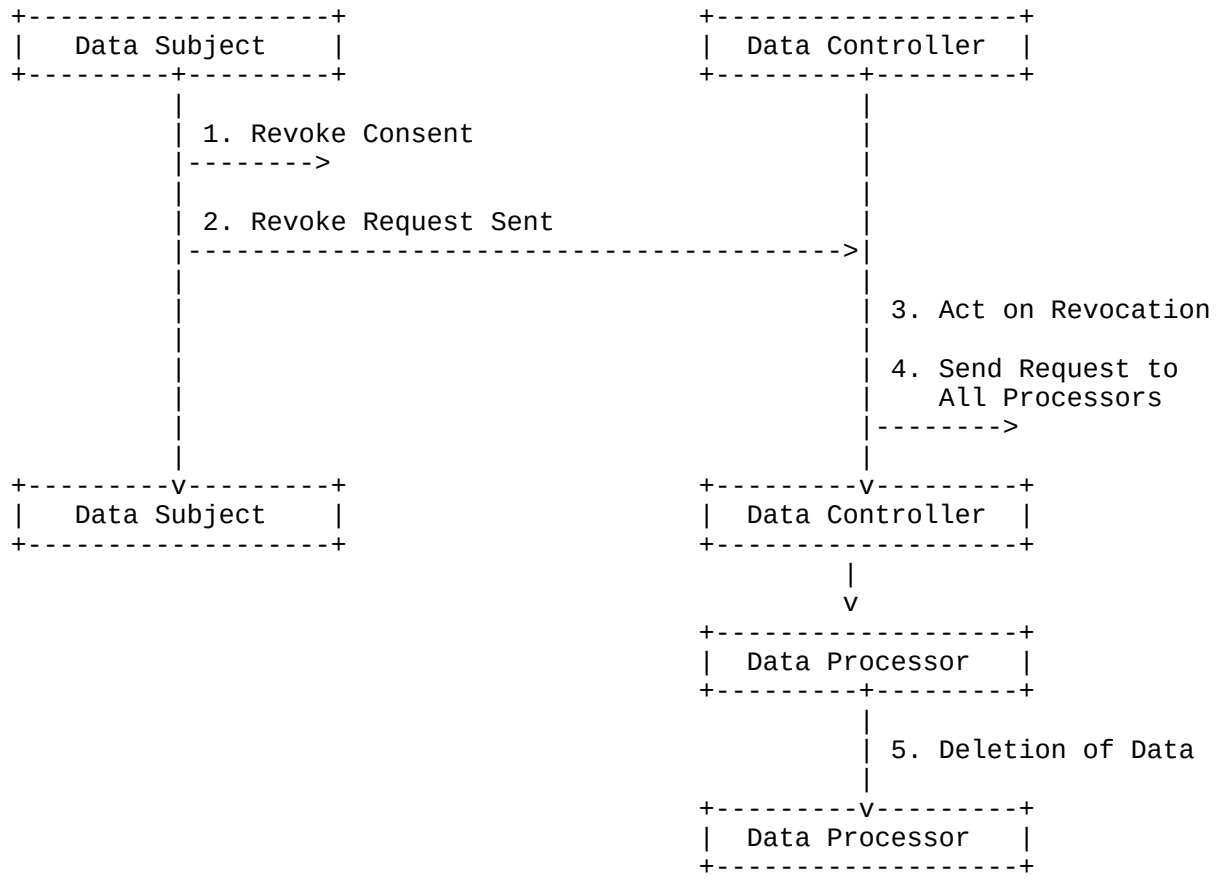
4. *Consent Receipt Sent*: The Data Processor sends notification to the Data Subject(s) with a link to review consent details.

5. *Consent Review*: The Data Subject(s) can review vCon information at any time and revoke consent if desired.

6. *Data Processor Value-Add*: The Data Processor performs value-added services for the Data Subject(s).

4.2. Revocation and the Right to Be Forgotten

At any point, a Data Subject can request revocation or the right to be forgotten, requiring all vCon possessors to act accordingly. vCons must be tracked for where they were sent and who to contact when a Data Subject makes such requests. The SCITT Transparency Service maintains metadata about ingested vCons, ensuring integrity and inclusion protection.



4.2.1. Data Subject

1. *Revoke Consent*: The Data Subject revokes consent by some manner: i.e. clicks a link included in all communications between the Data Processor and the Data Subject(s), through an external system or in conversation with the data controller.

2. *Revoke Request Sent*: If the vcon_consent_revoked operation was handled by the Data Processor, they MUST contact the Data Controller to communicate the Data Subject’s intent.

4.2.2. Data Controller Revocation

1. *Act on Consent Revocation Request*: The Data Controller receives the vCon Consent Revocation Request and records it on their SCITT Transparency Service.

2. *Send Revocation Request to Data Controllers*: If the vCon was sent to other Data Processors, they must communicate the revocation request to any Data Processor that hasn’t yet acknowledged it.

4.2.3. Data Processor Revocation

1. *Deletion of Data*: Any Data Processor that hasn’t yet acted on the request must acknowledge it.

5. vCon Lifecycle Events

The following events outline important "moments that matter" in a vCon’s lifecycle. These events are not intended to be stored within the vCon itself, but rather as operations stored on SCITT to provide context for the vCon’s intent at specific points in time:

* *vcon_created*: The initial vCon document as first recorded. The vCon may start with a basic structure defining minimal metadata, as recordings or attachments may be added asynchronously upon encoding completion.

* *vcon_enhanced*: The vCon has been amended or appended. While vCons are considered immutable, information may be amended or appended—previous values exist in the vCon Registry but may be superseded. Amendments may include transcription corrections or consent changes.

* *vcon_sent*: The vCon was sent to an external party. This operation seals the vCon’s integrity, recording what was sent, to whom, and when in the SCITT Transparency Service. A SCITT receipt from the receiving service confirms possession.

* *vcon_received*: The vCon was received from an external entity. This documents possession at a specific time, sealing content integrity and returning a SCITT receipt to the sender.

* *vcon_consent_accepted*: One or more parties have consented to the vCon being recorded and shared for its intended purpose. Consent may not be established during initial vCon creation, as the Data Controller, not the Data Originator (infrastructure provider), is responsible for managing Data Subject consent.

* *vcon_consent_revoked*: One or more parties have revoked consent for one or more purposes. Depending on region, license, and regulatory requirements, one revocation may or may not require all Data Processors to act.

* *vcon_party_redacted*: A party to the vCon has been redacted. This differs from consent revocation, as the vCon may remain viable if a party's information can be redacted while maintaining integrity and usefulness.

* *vcon_deleted*: The vCon has been deleted due to an implicit act such as revocation or no longer being needed. When a Data Controller deletes a vCon, they must inform all recipients to either delete it or assume Data Controller responsibilities.

* *vcon_expired*: The vCon has expired due to license terms or compliance requirements. This triggers deletion and notification to all shared entities.

* *vcon_rcvr_purged*: When a vCon is sent from a Data Controller, the receiving Entity may maintain it indefinitely, for a set period, or delete it upon operation completion. If the Entity no longer needs to maintain the vCon, they can delete it and notify the sender.

6. Security Considerations

The security of the vCon lifecycle depends heavily on the integrity and availability of the SCITT Transparency Service. Entities MUST ensure that their SCITT implementations are properly secured and that access controls are in place to prevent unauthorized modifications.

The handling of personally identifiable information (PII) throughout the vCon lifecycle requires careful consideration of privacy regulations and data protection requirements. Entities MUST implement appropriate technical and organizational measures to protect PII and ensure compliance with applicable regulations.

7. Privacy Considerations

This document describes a framework for managing vCons that contain personally identifiable information. Implementers MUST ensure compliance with applicable privacy regulations, including but not limited to GDPR GDPR (https://gdpr.eu/) and CCPA CCPA (https://oag.ca.gov/privacy/ccpa).

The framework provides mechanisms for consent management and data subject rights, but implementers are responsible for ensuring that their implementations properly respect and enforce these rights.

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. Normative References

9.2. Informative References

10. Informative References

[CBOR] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[CDDL] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/rfc/rfc8610>.

[CDR] ITU, "Recommendation Q.825: Specification of TMN applications at the Q3 interface: Call detail recording", n.d., <https://www.itu.int/rec/T-REC-Q.825>.

[GEOPRIV] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, DOI 10.17487/RFC4119, December 2005, <https://www.rfc-editor.org/rfc/rfc4119>.

[GZIP] Deutsch, P., "GZIP file format specification version 4.3", RFC 1952, DOI 10.17487/RFC1952, May 1996, <https://www.rfc-editor.org/rfc/rfc1952>.

[HTTPS] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/rfc/rfc9110>.

[IANA-COSE-ALG] "COSE Algorithms", n.d., <<https://www.iana.org/assignments/cose/cose.xhtml>>.

[ISOBMFF] "Information technology -- Coding of audio-visual objects -- Part 12: ISO base media file format", ISO/IEC 14496-12:2022, January 2022, <https://www.iso.org/standard/83102.html>.

[JMAP] Jenkins, N. and C. Newman, "The JSON Meta Application Protocol (JMAP)", RFC 8620, DOI 10.17487/RFC8620, July 2019, <https://www.rfc-editor.org/rfc/rfc8620>.

[JSON] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/rfc/rfc8259>.

[JWE] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, <https://www.rfc-editor.org/rfc/rfc7516>.

[JWK] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/rfc/rfc7517>.

[JWS] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/rfc/rfc7515>.

[JWT] 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>.

[MAILTO] Duerst, M., Masinter, L., and J. Zawinski, "The ’mailto’ URI Scheme", RFC 6068, DOI 10.17487/RFC6068, October 2010, <https://www.rfc-editor.org/rfc/rfc6068>.

[MEDIATYPE] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/rfc/rfc6838>.

[MIME] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/rfc/rfc2045>.

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

[PIDF-LO] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", RFC 5491, DOI 10.17487/RFC5491, March 2009, <https://www.rfc-editor.org/rfc/rfc5491>.

[SHA-512] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/rfc/rfc6234>.

[SIP-XFER] Sparks, R., Johnston, A., Ed., and D. Petrie, "Session Initiation Protocol (SIP) Call Control - Transfer", BCP 149, RFC 5589, DOI 10.17487/RFC5589, June 2009, <https://www.rfc-editor.org/rfc/rfc5589>.

[SMTP] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/rfc/rfc5321>.

[STIR-PASS] 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>.

[TEL] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, DOI 10.17487/RFC3966, December 2004, <https://www.rfc-editor.org/rfc/rfc3966>.

[UUID] Peabody, B. and K. R. Davis, "New UUID Formats", Work in Progress, Internet-Draft, draft-peabody-dispatch-new-uuid-format-04, 23 June 2022, <https://datatracker.ietf.org/doc/html/draft-peabody-dispatch-new-uuid-format-04>.

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

[vCon-white-paper] Howe, T., Petrie, D., Lieberman, M., and A. Quayle, "vCon: an Open Standard for Conversation Data", n.d., <https://github.com/vcon-dev/vcon/blob/main/docs/vCons_%20an%20Open%20Standard%20for%20Conversation%20Data.pdf>.

Appendix A. Acknowledgments

* Thank you to Allistair Woodman for connecting the first dots between VCon and SCITT

* Thank you to Jeff Pulver and Cody Launius for their collaboration and support

Authors' Addresses

Thomas McCarthy-Howe
Strolid, Inc.
Email: thomas.howe@strolid.com

S. Lasker
Independent
Email: stevenlasker@hotmail.com

Diana James
Marashlian & Donahue, PLLC
Email: daj@commlawgroup.com