vCon
Internet-Draft
Intended status: Standards Track
Expires: 1 December 2026

T. McCarthy-Howe
VCONIC

30 May 2026

vCon Lawful Basis
draft-howe-vcon-lawful-basis-02

Abstract

This document defines a lawful basis extension for Virtualized Conversations (vCon) that provides standardized mechanisms for recording, verifying, and managing the lawful basis for processing data within conversation containers. The lawful basis extension addresses privacy compliance challenges through structured attachment metadata, including the specific lawful basis being asserted, temporal validity periods where applicable, and cryptographic proof mechanisms.

The extension is designed as a Compatible vCon extension that introduces lawful basis management capabilities without altering existing vCon semantics. It defines a "lawful_basis" attachment (identified by the attachment "purpose" value "lawful_basis") with structured records for each of the six lawful bases defined in regulations like GDPR, including consent, contract, legal obligation, vital interests, public task, and legitimate interests.

Key features include automated lawful basis detection during conversation processing, auditable records with cryptographic proofs, granular purpose-based permissions for all lawful bases, documented justifications for other lawful bases, and integration with privacy regulations including GDPR, CCPA, and HIPAA.

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

Discussion of this document takes place on the vCon 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-lawful-basis.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 1 December 2026.

Copyright Notice

Table of Contents

1. Introduction

Conversations originating from all modes (voice, video, email, fax and messaging) [I-D.draft-ietf-vcon-overview], contain sensitive information that requires a documented lawful basis for processing to comply with privacy regulations and ethical standards. This document defines a lawful basis extension for Virtualized Conversations (vCon) that enables automated lawful basis detection, structured recording, and cryptographic proof mechanisms.

A vCon (Virtualized Conversation) is a standardized container format for storing conversation data, including metadata, participants, and conversation content, as defined in [I-D.draft-ietf-vcon-vcon-core]. The vCon specification supports extensible attachments that can carry additional structured data related to the conversation.

This lawful basis extension provides a Compatible vCon extension (as defined in Section 2.5 of [I-D.draft-ietf-vcon-vcon-core]) that introduces lawful basis management capabilities through a standardized "lawful_basis" attachment (identified by the attachment "purpose" value "lawful_basis"). The extension captures essential metadata including:

* The specific lawful basis being asserted for processing

* Party identification (for consent-based processing)

* Temporal validity periods (where applicable)

* Granular purpose-based permissions

* Documented justifications for non-consent-based lawful bases

* Cryptographic proof mechanisms and external verification

* Integration with SCITT transparency services for audit trails

The lawful basis extension addresses key privacy and compliance challenges while maintaining compatibility with existing vCon implementations. Implementations that do not recognize the lawful basis extension can safely ignore lawful basis attachments while maintaining valid processing of other vCon content.

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.

2.1. Core Terms

Lawful Basis: A valid justification, as defined by applicable law (e.g., GDPR), for the processing of personal data. One of six potential bases must be identified prior to processing.

Data Subject: The identified or identifiable natural person to whom personal data relates [GDPR].

Lawful Basis Attachment: A vCon attachment with the "purpose" value "lawful_basis" that contains structured information documenting the lawful basis for processing conversation data.

Attestation Registry: An external transparency service that maintains an authoritative, verifiable log of attestations about a vCon, which can include attestations of a lawful basis. This document defines integration with registries using the SCITT protocol.

Compatible Extension: A vCon extension that introduces additional data without altering the meaning or structure of existing elements, as defined in [I-D.draft-ietf-vcon-vcon-core].

3. Overview of Lawful Bases

While this document defines an extension for recording any lawful basis for processing, it is important to understand the distinctions between them. Under regulations like the GDPR, there are six lawful bases for processing personal data. Consent is unique in that it is a permission granted by the data subject, while the other five are justifications asserted by the data controller. Understanding this distinction is critical for correctly implementing this extension.

The six lawful bases for processing under GDPR are:

1. *Consent*: The data subject has given clear, unambiguous consent for their personal data to be processed for a specific purpose. This basis is unique because it originates with the data subject.

2. *Contract*: The processing is necessary for a contract that the data subject has with the organization, or because they have asked the organization to take specific steps before entering into a contract. For example, processing a customer’s address to deliver a purchased product.

3. *Legal Obligation*: The processing is necessary for the organization to comply with the law (not including contractual obligations). For example, a financial institution may be legally required to report certain transactions to prevent fraud.

4. *Vital Interests*: The processing is necessary to protect someone’s life. For example, sharing a patient’s medical history with emergency services.

5. *Public Task*: The processing is necessary for the organization to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law. For example, a local authority processing data to provide public services.

6. *Legitimate Interests*: The processing is necessary for the organization's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. For example, a business using customer data for marketing analysis to improve its services, provided it does not infringe on the customer's privacy rights.

This lawful basis extension for vCon provides a standardized way to record and verify any of these lawful bases. The presence and content of a lawful_basis attachment are intended to be the primary mechanism for determining the authorized uses of a vCon's data.

4. vCon Lawful Basis Extension Definition

4.1. Extension Classification

The lawful basis extension is a *Compatible Extension* as defined in Section 2.5 of [I-D.draft-ietf-vcon-vcon-core]. This extension:

* Introduces additional lawful basis metadata without altering existing vCon semantics

* Can be safely ignored by implementations that don't support lawful basis processing

* Does not require listing in the critical parameter

* Maintains backward compatibility with existing vCon implementations

4.2. Extension Registration

This document defines the "lawful_basis" extension token for registration in the vCon Extensions Names Registry:

* *Extension Name*: lawful_basis

* *Extension Description*: Lawful basis management for conversation participants with cryptographic proof mechanisms and regulatory compliance support

* *Change Controller*: IESG

* *Specification Document*: This document

4.3. Extension Usage

vCon instances that include lawful basis attachments SHOULD include "lawful_basis" in the extensions array:

```
{
  "vcon": "0.4.0",
  "uuid": "01934b2a-7e2f-8c3d-9a1b-2c3d4e5f6a7b",
  "extensions": ["lawful_basis"],
  "created_at": "2025-01-02T12:00:00Z",
  "parties": [...],
  "dialog": [...],
  "attachments": [
    {
      "purpose": "lawful_basis",
      "start": "2025-01-02T12:15:30Z",
      "party": 0,
      "dialog": 0,
      "encoding": "json",
      "body": {
        // Lawful basis data structure defined below
      }
    }
  ]
}
```

5. Lawful Basis Attachment Structure

5.1. Attachment Container

Lawful basis information MUST be included as vCon attachments using the standard attachment object structure defined in Section 4.4 of [I-D.draft-ietf-vcon-vcon-core].

The lawful basis attachment MUST include:

* *purpose*: MUST be set to "lawful_basis"

* *encoding*: MUST be set to "json" for structured lawful basis data

* *body*: MUST contain the lawful basis data structure as defined below, carried per the "json" encoding defined in Section 2.3.2 of [I-D.draft-ietf-vcon-vcon-core]

* *party*: Index of the party in the vCon parties array (Section 4.4.3 of [I-D.draft-ietf-vcon-vcon-core]); use 0 when no specific party applies

* *dialog*: Index of the associated dialog in the vCon dialog array (Section 4.4.4 of [I-D.draft-ietf-vcon-vcon-core]); use 0 when no specific dialog applies

The lawful basis attachment SHOULD include:

* *start*: ISO 8601 timestamp [RFC3339] when lawful basis was recorded

5.2. Lawful Basis Body Structure

The body field of the lawful basis attachment MUST contain a JSON object with the following structure:

5.2.1. Required Fields

* *lawful_basis*: String enum from consent, contract, legal_obligation, vital_interests, public_task, legitimate_interests

* *expiration*: ISO 8601 timestamp indicating when the lawful basis expires, or null for indefinite

* *purpose_grants*: Array of purpose grant objects specifying permissions

5.2.2. Optional Fields

* *terms_of_service*: URL reference to applicable terms of service document

* *status_interval*: Duration string for revalidation intervals (e.g., "30d")

* *content_hash*: An object containing content integrity information for the lawful basis attachment. The object has the following fields:

  - *algorithm*: (string, required) The hash algorithm used. This document defines initial values of "sha-256", "sha-3-256", and "blake2b-256". Other values may be registered in an IANA registry.

- *canonicalization*: (string, required) The canonicalization method used. This document defines an initial value of "jcs" (JSON Canonicalization Scheme per RFC 8785). Other values may be registered in an IANA registry.

- *value*: (string, required) The hexadecimal-encoded hash value of the canonicalized lawful basis attachment body.

This body-level content_hash integrity object is distinct from the attachment-level content_hash parameter defined in Section 2.4 of [I-D.draft-ietf-vcon-vcon-core], which uses the sha512- Base64url form and applies to externally referenced files.

* *registry*: An object containing information about an external attestation registry for audit trails. The object has the following fields:

  - *type*: (string, required) The type of the attestation registry service. This document defines an initial value of "scitt". Other values may be registered in an IANA registry.

  - *url*: (string, required) The URL endpoint for the attestation registry service.

* *proof_mechanisms*: Array of proof objects supporting the lawful basis

* *metadata*: Additional implementation-specific metadata

5.2.3. Purpose Grant Objects

Each object in the purpose_grants array MUST contain:

* *purpose*: String identifying the processing purpose (e.g., "recording", "transcription", "analysis")

* *granted*: Boolean indicating whether permission is granted (true) or denied (false)

* *granted_at*: ISO 8601 timestamp when this specific permission was granted

* *conditions*: Optional array of strings describing conditions or restrictions

5.2.4. Proof Mechanism Objects

Each object in the proof_mechanisms array MUST contain:

* *proof_type*: String identifying the proof mechanism type
* *timestamp*: ISO 8601 timestamp when proof was created
* *proof_data*: Object containing proof-type-specific data

Supported proof types include:

* *verbal_confirmation*: Lawful basis given verbally within the conversation
* *signed_document*: External signed lawful basis form or agreement
* *cryptographic_signature*: Digital signature using COSE standards [COSE-ALG]
* *external_system*: Lawful basis recorded in external system with API verification

5.3. Example Lawful Basis Attachment

```
{
  "purpose": "lawful_basis",
  "start": "2025-01-02T12:15:30Z",
  "party": 0,
  "dialog": 0,
  "encoding": "json",
  "body": {
    "lawful_basis": "consent",
    "expiration": "2026-01-02T12:00:00Z",
    "purpose_grants": [
      {
        "purpose": "recording",
        "granted": true,
        "granted_at": "2025-01-02T12:15:30Z"
      },
      {
        "purpose": "transcription",
        "granted": true,
        "granted_at": "2025-01-02T12:15:30Z"
      },
      {
        "purpose": "sentiment_analysis",
        "granted": false,
```

```
          "granted_at": "2025-01-02T12:15:30Z"
        }
      ],
      "proof_mechanisms": [
        {
          "proof_type": "verbal_confirmation",
          "timestamp": "2025-01-02T12:15:30Z",
          "proof_data": {
            "dialog_reference": 0,
            "time_offset": "00:01:23",
            "confirmation_text": "Yes, I consent to recording this call"
          }
        }
      ],
      "terms_of_service": "https://example.com/terms/v2024.1",
      "status_interval": "30d",
      "content_hash": {
        "algorithm": "sha-256",
        "canonicalization": "jcs",
        "value": "a1b2c3d4e5f6789abcdef0123456789abcdef0123456789abcdef0123456789ab"
      },
      "registry": {
        "type": "scitt",
        "url": "https://transparency.example.com/lawful_purpose/registry"
      }
    }
  }
```

6. Lawful Basis Processing Requirements

6.1. Content Hash Validation

Implementations MUST validate content hashes when present in lawful basis attachments:

1. *Canonicalization*: Apply the specified canonicalization method to the lawful basis attachment body
    - For "jcs" canonicalization: Use JSON Canonicalization Scheme per RFC 8785
    - Sort object keys lexicographically
    - Remove insignificant whitespace
    - Ensure consistent number representations

2. *Hash Computation*: Compute the hash using the specified algorithm
    * For "sha-256": Use SHA-256 algorithm
    * For "sha-3-256": Use SHA-3-256 algorithm
    * For "blake2b-256": Use BLAKE2b-256 algorithm
3. *Hash Verification*: Compare computed hash with the provided value
    * Reject processing if hashes do not match
    * Log hash validation results for audit purposes
4. *Error Handling*: Provide specific error reporting for hash validation failures
    * *ContentHashMismatchError*: Computed hash does not match provided value
    * *UnsupportedHashAlgorithmError*: Hash algorithm not supported by implementation
    * *UnsupportedCanonicalizationError*: Canonicalization method not supported by implementation

6.2. Temporal Validity

Implementations MUST validate lawful basis expiration before processing:

1. Compare current time against expiration timestamp
2. Account for reasonable clock skew (maximum 5 minutes recommended)
3. Reject processing if lawful basis has expired
4. Support null expiration for indefinite validity subject to revalidation intervals

6.3. Reference Validation

Implementations MUST validate attachment references:

1. Verify party index exists in vCon parties array

2. Verify dialog indices exist in vCon dialog array

6.4. Granular Permission Evaluation

When processing vCon content, implementations MUST:

1. Check for applicable lawful basis attachments for the requested processing purpose
2. Evaluate all relevant purpose grants for the specific purpose
3. Apply most restrictive permission when multiple grants apply
4. Deny processing if no valid permission exists or if it is explicitly denied

6.5. Proof Verification

Implementations SHOULD verify proof mechanisms when present:

1. Validate cryptographic signatures using appropriate algorithms
2. Verify external document integrity using content hashes
3. Check external system lawful basis status via API calls
4. Log proof verification results for audit purposes

7. Transparency Service Integration

7.1. Registry Services

The optional registry field enables integration with external attestation registries for audit trails. The registry object's type field specifies the protocol to be used.

When the registry object is present and its type is "scitt", the url field MUST:

* Reference a SCITT (Supply Chain Integrity, Transparency, and Trust) Transparency Service implementing SCRAPI [I-D.draft-ietf-scitt-scrapi-07]
* Provide cryptographic receipts for state changes
* Support status queries and updates
* Implement appropriate access controls and privacy protections

Other transparency service types may be used if they are registered with IANA. The documentation for each registered type must specify the necessary protocols and interaction models.

7.2. Registry Integration Requirements

Implementations that support registries MUST:

1. Use HTTPS with TLS 1.2 or higher for all communications
2. Implement appropriate authentication mechanisms
3. Validate SCITT receipts using standard verification procedures
4. Handle service unavailability gracefully
5. Cache lawful basis state within configured intervals

7.3. Privacy Considerations for Registries

Registry services SHOULD:

* Store only lawful basis metadata, not full conversation content
* Implement privacy-preserving query mechanisms
* Maintain audit logs for regulatory compliance
* Support deletion and other personal data compliance responsibilities

8. Error Handling

Implementations SHOULD provide specific error reporting:

* *LawfulBasisExpiredError*: Lawful basis has expired and cannot be used
* *PermissionDeniedError*: Permission explicitly denies the requested processing
* *LawfulBasisMissingError*: No valid lawful basis found for the requested processing
* *ProofVerificationError*: Lawful basis proof mechanisms failed validation

* *ReferenceValidationError*: Attachment references invalid vCon elements

* *ContentHashMismatchError*: Computed hash does not match provided value

* *UnsupportedHashAlgorithmError*: Hash algorithm not supported by implementation

* *UnsupportedCanonicalizationError*: Canonicalization method not supported by implementation

9. Interoperability

To ensure interoperability across implementations:

* Use only standard JSON data types in lawful basis body structures

* Support graceful degradation when advanced features are unavailable

* Implement lawful basis attachment format negotiation for multi-party exchanges

10. Security Considerations

The vcon-core specification provides general-purpose security mechanisms, such as digital signatures, designed to ensure the basic integrity of the vCon container. These mechanisms answer the question, "Has this vCon been tampered with?" However, managing lawful basis requires addressing a more specific and legally significant question: "Did this specific person provide a valid basis for this specific action at a specific time?" Answering this question requires a higher level of security and contextual awareness. The following sections detail the additional security considerations that are critical for a lawful basis mechanism to be considered trustworthy and compliant with privacy regulations.

10.1. Cryptographic Protection and Forgery

Background: Forgery is the act of creating a fake record or altering an existing one -- for instance, by changing the expiration date, expanding the scope of what was agreed to, or faking the identity of the party. The ability to prove that a lawful basis is authentic and unaltered is the bedrock of any privacy compliance framework like GDPR or CCPA. A forged record is equivalent to having no lawful basis at all and carries severe legal and financial penalties under frameworks such as GDPR [GDPR] and CCPA [CCPA].

While vcon-core provides a signature field, this extension adds the necessary business rules to ensure that a signature represents a trusted, verifiable, and legally binding act.

Requirements: Implementations MUST prevent forgery through:

* Cryptographic signature verification for digital proof mechanisms.

* External document integrity validation using content hashes.

* Secure communication channels for external verification.

* Audit logging of all validation activities.

10.2. Replay Attack Prevention

Background: A replay attack involves an attacker copying a valid lawful basis attachment from one vCon and maliciously inserting it into a different vCon that the user never actually provided a basis for. Without replay protection, a user's lawful basis for a non-sensitive inquiry could be "replayed" to appear as if they provided it for the recording and analysis of a highly sensitive conversation. This would be a massive privacy violation and would render the mechanism meaningless.

Requirements: The lawful basis attachment design MUST prevent replay attacks through:

* Cryptographic binding to specific vCon instances.

* Timestamp validation with appropriate clock skew tolerance.

* Nonce inclusion in proof mechanisms where applicable.

* Reference validation to ensure lawful basis applies to correct content.

10.3. Secure Communication Channels

Background: Lawful basis records are themselves sensitive personal data. It is critical that they are protected while in transit between systems. An attacker in a "man-in-the-middle" position could intercept a vCon and alter it before it reaches its destination, potentially stripping or modifying lawful basis information.

Requirements: All lawful basis attachments MUST be integrity protected using vCon signing mechanisms as defined in [I-D.draft-ietf-vcon-vcon-core]. Lawful basis attachments containing

sensitive information SHOULD be encrypted when transmitted outside secure environments, for instance by using TLS 1.2 or higher for all communications.

10.4. Audit Logging

Background: Lawful basis is a matter of legal and regulatory compliance. If a dispute arises, the organization processing the data must be able to _prove_ it had a valid lawful basis at the time of the action. An audit log provides this crucial, non-repudiable evidence for regulators, auditors, and courts. It is a cornerstone of the "accountability" principle in modern privacy law.

Requirements: Systems that process or manage lawful basis attachments SHOULD maintain a secure, immutable record of all related activities (e.g., when a lawful basis was given, checked, revoked, or expired). When a registry is used, this requirement may be fulfilled by the registry service.

11. Privacy and Regulatory Compliance

11.1. Data Minimization

Lawful basis attachments MUST implement data minimization principles by:

* Including only information necessary for verification
* Avoiding duplication of personal data already in vCon elements
* Supporting attachment redaction while maintaining verifiability
* Implementing privacy-preserving verification mechanisms

11.2. Regulatory Alignment

The lawful basis extension addresses requirements from major privacy regulations:

* *GDPR Article 7*: Conditions for lawful basis including withdrawal mechanisms
* *CCPA Section 1798.135* [CCPA]: Requirements for personal information processing
* *HIPAA Privacy Rule* [HIPAA]: Requirements for protected health information

Implementers MUST ensure their implementations comply with applicable regulations in their jurisdiction. The NIST Privacy Framework [NIST-PRIVACY] provides additional guidance for organizations implementing privacy controls.

11.3. Data Subject Rights

Implementations MUST support data subject rights including:

* *Right of Access*: Enable data subjects to access their records
* *Right of Rectification*: Allow correction of inaccurate information
* *Right to be Forgotten*: Support deletion and data erasure
* *Right of Portability*: Enable export of data in interoperable formats
* *Withdrawal*: Provide mechanisms for revocation of a lawful basis

12. Conclusion

This document defines a comprehensive lawful basis extension for vCon that balances privacy protection with practical implementation requirements. The extension provides a foundation for lawful basis-aware conversation processing while maintaining compatibility with existing vCon infrastructure.

13. Security and Privacy Considerations Summary

This lawful basis extension addresses several critical security and privacy concerns:

Integrity: Cryptographic protection prevents unauthorized modification of records while maintaining verifiability across system boundaries.

Temporal Security: Expiration controls and revalidation intervals ensure a lawful basis cannot be misused beyond its intended temporal scope.

Audit Transparency: SCITT integration provides cryptographic audit trails for operations while maintaining privacy protections.

Regulatory Compliance: Structured management supports compliance with GDPR, CCPA, HIPAA and other privacy regulations through standardized metadata and processing controls.

Data Minimization: Privacy-preserving design minimizes data collection and supports lawful basis-driven access controls throughout the conversation lifecycle.

Implementers should conduct thorough security reviews and ensure compliance with applicable privacy regulations in their deployment environments.

14. References

14.1. Normative References

[I-D.draft-ietf-scitt-scrapi-07]
Birkholz, H., "SCITT Reference REST API", Work in Progress, Internet-Draft, draft-ietf-scitt-scrapi-07, November 2025, <https://datatracker.ietf.org/doc/draft-ietf-scitt-scrapi/07/>.

[I-D.draft-ietf-vcon-vcon-core]
Petrie, D. G., "The JSON format for vCon - Conversation Data Container", Work in Progress, Internet-Draft, draft-ietf-vcon-vcon-core-02, January 2026, <https://datatracker.ietf.org/doc/draft-ietf-vcon-vcon-core/>.

[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>.

[RFC3339] Klyne, G., "Date and Time on the Internet: Timestamps", July 2002, <https://www.rfc-editor.org/rfc/rfc3339.html>.

[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>.

14.2. Informative References

[CCPA] State of California, "California Consumer Privacy Act", 2018, <https://oag.ca.gov/privacy/ccpa>.

[COSE-ALG] IANA, "COSE Algorithms", May 2026, <https://www.iana.org/assignments/cose/cose.xhtml>.

[FIPS-180-4]
National Institute of Standards and Technology, "Secure Hash Standard (SHS)", August 2015, <https://csrc.nist.gov/publications/detail/fips/180/4/final>.

[FIPS-202] National Institute of Standards and Technology, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", August 2015, <https://csrc.nist.gov/publications/detail/fips/202/final>.

[GDPR] European Union, "General Data Protection Regulation", 2018, <https://gdpr.eu/>.

[HIPAA] U.S. Department of Health and Human Services, "Health Insurance Portability and Accountability Act", 1996, <https://www.hhs.gov/hipaa/index.html>.

[I-D.draft-ietf-vcon-overview]
McCarthy-Howe, T., "The vCon - Conversation Data Container - Overview", Work in Progress, Internet-Draft, draft-ietf-vcon-overview, 2025, <https://datatracker.ietf.org/doc/draft-ietf-vcon-overview/>.

[NIST-PRIVACY]
National Institute of Standards and Technology, "NIST Privacy Framework", 2020, <https://www.nist.gov/privacy-framework>.

[RFC7693] Saarinen, M., "The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)", November 2015, <https://www.rfc-editor.org/rfc/rfc7693.html>.

[RFC8785] Rundgren, A., "JSON Canonicalization Scheme (JCS)", June 2020, <https://www.rfc-editor.org/rfc/rfc8785.html>.

Appendix A. IANA Considerations

A.1. vCon Extensions Names Registry

This document requests IANA to register the following extension in the vCon Extensions Names Registry established by [I-D.draft-ietf-vcon-vcon-core]:

* *Extension Name*: lawful_basis

* *Extension Description*: Lawful basis management for conversation participants with cryptographic proof mechanisms and regulatory compliance support

* *Change Controller*: IESG

* *Specification Document(s)*: RFC XXXX

A.2. Lawful Basis Attachment Type Values Registry

This document requests IANA to establish a new registry for lawful basis attachment type values. A registered value is used as the attachment "purpose" parameter (Section 4.4.1 of [I-D.draft-ietf-vcon-vcon-core]) to identify a lawful basis attachment. The registry has the following initial registration:

* *Type Value*: lawful_basis

* *Description*: Structured lawful purpose records with temporal validity and cryptographic proof mechanisms

* *Change Controller*: IESG

* *Specification Document(s)*: RFC XXXX

Registration Template:

Type Value: The string value used as the attachment "purpose" value identifying this attachment type

Description: Brief description of the attachment type and its purpose

Change Controller: For Standards Track RFCs, list "IESG". For others, give the name of the responsible party.

Specification Document(s): Reference to defining documents with URIs where available ## Lawful Basis Registry Type Values Registry

This document requests IANA to establish a new registry for lawful basis registry type values with the following initial registration:

* *Type Value*: scitt

* *Description*: A transparency service implementing the SCITT (Supply Chain Integrity, Transparency, and Trust) protocol.

* *Change Controller*: IESG

* *Specification Document(s)*: RFC XXXX, [I-D.draft-ietf-scitt-scrapi-07]

Registration Template:

Type Value: The string value used as the registry type identifier

Description: Brief description of the registry type and its purpose

Change Controller: For Standards Track RFCs, list "IESG". For others, give the name of the responsible party.

Specification Document(s): Reference to defining documents with URIs where available

A.3. Lawful Basis Content Hash Algorithm Values Registry

This document requests IANA to establish a new registry for lawful basis content hash algorithm values with the following initial registrations:

* *Algorithm Value*: sha-256

* *Description*: SHA-256 hash algorithm as defined in FIPS 180-4

* *Change Controller*: IESG

* *Specification Document(s)*: RFC XXXX, [FIPS-180-4]

* *Algorithm Value*: sha-3-256

* *Description*: SHA-3-256 hash algorithm as defined in FIPS 202

* *Change Controller*: IESG

* *Specification Document(s)*: RFC XXXX, [FIPS-202]

* *Algorithm Value*: blake2b-256

* *Description*: BLAKE2b-256 hash algorithm as defined in RFC 7693

* *Change Controller*: IESG

* *Specification Document(s)*: RFC XXXX, [RFC7693]

Registration Template:

Algorithm Value: The string value used as the hash algorithm identifier

Description: Brief description of the hash algorithm and its purpose

Change Controller: For Standards Track RFCs, list "IESG". For others, give the name of the responsible party.

Specification Document(s): Reference to defining documents with URIs where available

A.4. Lawful Basis Content Hash Canonicalization Values Registry

This document requests IANA to establish a new registry for lawful basis content hash canonicalization values with the following initial registration:

* *Canonicalization Value*: jcs
* *Description*: JSON Canonicalization Scheme as defined in RFC 8785
* *Change Controller*: IESG
* *Specification Document(s)*: RFC XXXX, [RFC8785]

Registration Template:

Canonicalization Value: The string value used as the canonicalization method identifier

Description: Brief description of the canonicalization method and its purpose

Change Controller: For Standards Track RFCs, list "IESG". For others, give the name of the responsible party.

Specification Document(s): Reference to defining documents with URIs where available

Appendix B. Acknowledgements

* Appreciation to Vinnie Micciche for his unwavering support during the development of this lawful basis attachment in particular, and vCons in general.

Author’s Address

Thomas McCarthy-Howe
VCONIC
United States
Email: ghostofbasho@gmail.com