SOOS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 30 November 2026

T. Sato
MyAuberge K.K.

30 May 2026

Constitutional AI Protocol -- Regulation Record Specification (CAP-RRS)
draft-sato-soos-cap-rrs-00

Abstract

The Constitutional AI Protocol (CAP) [I-D.sato-soos-cap] defines the enforcement architecture for governed AI agent systems: a three-tier Cedar policy evaluation model that distinguishes absolute prohibitions, jurisdictional legal constraints, operator policies, and resource limits. CAP-01 specifies what the Governance Execution Controller (GEC) does when a Cedar policy fires. It does not specify how Cedar policies are authored, certified, distributed, or maintained as law changes.

This document defines the Regulation Record: the structured representation of a compliance obligation at any CAP tier. A Regulation Record is the human-readable, machine-compilable intermediate form between legal text and Cedar policy. This document specifies the Regulation Record schema (Section 4), the Cedar Compilation Profile that governs how Regulation Records are translated into Cedar policies (Section 5), the conflict declaration model (Section 6), the certification model governing which publishers may certify records at each tier (Section 7), and the versioning and update protocol for the Constitutional Mandate Registry (Section 8).

The core developer experience this document enables: a developer imports certified Regulation Record packages from the Constitutional Mandate Registry, declares their own Tier 2 operator policies and Tier 3 resource policies, calls compile(), and receives a Cedar policy set ready for GEC loading. No Cedar is authored by hand for compliance purposes. Compliance is a package management operation.

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 30 November 2026.

Table of Contents

1. Introduction

1.1. The Compliance Authoring Problem

The Constitutional AI Protocol [I-D.sato-soos-cap] specifies that a GEC evaluates Cedar policies before every agent transition. For high-risk and regulated deployments, those Cedar policies must accurately reflect applicable legal obligations: data protection law, financial crime prevention requirements, healthcare regulations, and so on. The question CAP-01 does not answer is: who writes those Cedar policies, and how?

Writing Cedar policies by hand from legal text is not a viable path to adoption. Legal text is authored in natural language for human interpretation; Cedar is a formal policy language designed for machine evaluation. The translation between them requires both legal expertise and Cedar authoring expertise -- a rare combination. More critically, Cedar policies must be updated whenever the law changes. Regulatory amendment, judicial interpretation, and supervisory guidance can all alter the operative effect of a legal obligation. A compliance architecture that requires manual Cedar updates on every regulatory change will not be maintained correctly in practice.

The Regulation Record resolves this by separating the authoring concern (compliance specialists working in structured JSON with legal vocabulary) from the compilation concern (automated translation from Regulation Record to Cedar per the Cedar Compilation Profile) and the enforcement concern (GEC evaluating Cedar at runtime, fully specified by CAP-01). Each layer is owned by the appropriate expert. No layer requires expertise in all three domains.

1.2. The Compilation Model

Cedar is the compilation target, not the authoring language. The relationship between Regulation Records and Cedar policies is analogous to the relationship between high-level programming languages and machine code: the higher abstraction is where humans work; the lower abstraction is what machines execute; the compiler is the normative bridge between them.

This document specifies the compiler -- the Cedar Compilation Profile -- as a normative mapping. Any two conforming implementations of the Cedar Compilation Profile MUST produce semantically equivalent Cedar from identical Regulation Records. This determinism is essential: it means a Regulation Record certified by a regulatory authority can be compiled by any GEC implementation and produce Cedar that the certifying authority would recognise as an accurate representation of their requirement.

1.3. Relationship to CAP-01

CAP-01 [I-D.sato-soos-cap] specifies runtime enforcement: what the GEC does when a Cedar policy fires. CAP-RRS (this document) specifies the governance of the policy corpus that CAP-01 enforces: how Cedar policies are authored, certified, distributed, and kept current as law changes. The two documents are complementary and form one governance stack. CAP-RRS does not revise or supersede CAP-01; it extends it. A GEC implementing CAP-01 alone has a governed enforcement engine whose policies are manually authored and unverified. A GEC implementing CAP-01 and CAP-RRS has a governed enforcement engine whose policies are registry-sourced, certified, version-managed, and automatically updated.

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.

CAP-01:
: The Constitutional AI Protocol enforcement specification [I-D.sato-soos-cap].

Cedar Compilation Profile:
: The normative mapping from Regulation Record fields to Cedar policy syntax specified in Section 5 of this document.

Constitutional Mandate Registry (CMR):
: The signed, versioned, append-only repository of certified Regulation Record packages. Protocol specified in Section 8.

GEC (Governance Execution Controller):
: The runtime component that enforces Cedar policies produced by the CAP-RRS compiler. Defined in [I-D.sato-soos-cap].

Natural Breakpoint:
: A point in a multi-step agent mission at which stopping produces a coherent, complete deliverable of independent value. Used by HEM_TIER3_ANTICIPATORY to identify scope-reduction options.

Operative Clause:
: The specific prohibition or permission within a legal text that applies at agent decision time and is therefore representable as a Cedar policy. Distinguished from definitional, procedural, and enforcement provisions that do not require Cedar representation.

Regulation Record:
: The structured intermediate representation of a compliance obligation, as defined in Section 4 of this document.

Regulation Record Package:
: A signed, versioned collection of Regulation Records covering a defined legal instrument (e.g., GDPR, BSA, HIPAA).

Resource Policy:
: A Tier 3 Regulation Record governing agent resource consumption (tokens, API calls, time windows, storage).

3. Architecture Overview

3.1. The Three-Layer Stack

The compliance architecture operates as three distinct layers:

Layer 1 -- Law to Regulation Record:
: Compliance specialists extract the operative clause from legal text and represent it as a structured Regulation Record. This layer requires legal expertise. It does not require Cedar knowledge. The output is JSON in the Regulation Record schema (Section 4). Certification is governed by Section 7.

Layer 2 -- Regulation Record to Cedar:
: The CAP-RRS compiler applies the Cedar Compilation Profile

(Section 5) to transform Regulation Records into Cedar policies. This layer is fully automated. No human authoring of Cedar for compliance purposes is required or expected. The output is a Cedar policy set suitable for loading by a CAP-01-conforming GEC.

Layer 3 -- Cedar to Enforcement:
The GEC evaluates the Cedar policy set at every agent transition. This layer is fully specified by CAP-01. The developer observes ALLOW or DENY with a structured reason code referencing the specific Regulation Record that fired.

3.2. Developer Experience

A developer configuring compliance for a regulated agent deployment performs four operations:

(1) Import certified Regulation Record packages from the CMR for all applicable legal frameworks.

(2) Author Tier 2 operator policies in Regulation Record format. No Cedar knowledge required.

(3) Author Tier 3 resource policies in Regulation Record format. No Cedar knowledge required.

(4) Call compile(). The Cedar Compilation Profile generates the full Cedar policy set. The developer does not review or modify Cedar output except for debugging purposes.

Pseudocode example:

```
cap.import("cmr://eu.gdpr.2016/679@2.1.0")   ; Tier 1 -- GDPR
cap.import("cmr://eu.ai_act.2024/art14@1.0.0")
cap.import("cmr://us.bsa.1970/sar@3.2.1")

cap.operator_policy({ record_id: "acme.data_access.v1",
                      tier: "2", ... })

cap.resource_policy({ record_id: "acme.token_budget.v1",
                      tier: "3", ... })

cedar_policy_set = cap.compile()
gec.load_policies(cedar_policy_set)
```

3.3. Registry as Package Ecosystem

The Constitutional Mandate Registry operates as a signed package ecosystem. Each Regulation Record Package is:

* Identified by a URI: cmr://{publisher}.{instrument}@{version}
* Signed by the certified publisher's Ed25519 keypair
* Versioned using Semantic Versioning [SEMVER]
* Accompanied by a changelog declaring which operative clauses changed between versions
* Conflict-declared against known incompatible packages

GEC implementations subscribe to update notifications for imported packages. Update handling is governed by Section 8.4.

The tier architecture determines both the certification requirements (Section 7) and the post-DENY recourse availability:

Tier	Category	Recourse on DENY
0-A	Absolute universal prohib.	None. Ever.

0-B	Qualified absolute prohib.	None within scope.
1	Jurisdictional legal	None within jurisdiction.
2	Operator policy	Operator-defined exception path or HEM escalation.
3	Resource / usage policy	Always exists: commercial, scope reduction, temporal.

This recourse taxonomy is the clearest single articulation of why tiers are structurally distinct: not merely by severity, but by whether a governed path forward exists after DENY.

4. Regulation Record Schema

4.1. Top-Level Fields

A Regulation Record is a JSON object. Fields marked REQUIRED must be present. CONDITIONAL fields are required when the stated condition is met.

record_id (string, REQUIRED):
Unique identifier within the package.
Format: {publisher_id}.{instrument_code}.{article}.
Example: "eu.gdpr.2016_679.art6".
MUST be stable across package versions.

schema_version (string, REQUIRED):
Regulation Record schema version. Current: "cap-rrs-00".

tier (string, REQUIRED):
CAP tier. One of: "0-A", "0-B", "1", "2", "3".

jurisdiction_scope (object, REQUIRED):
territories (array of string): ISO 3166-1 alpha-2 codes, or "GLOBAL" for Tier 0 records.
legal_system (string): "CIVIL", "COMMON", "RELIGIOUS", "HYBRID", or "INTERNATIONAL".
supranational_body (string, OPTIONAL): e.g., "EU", "UN".

legal_source (object, REQUIRED for Tier 0 and 1):
instrument_name (string): Full official instrument name.
instrument_code (string): Short code, e.g., "GDPR".
article (string): Specific article or provision.
official_url (string, OPTIONAL): URL to official text.
treaty_citation (string, REQUIRED for Tier 0-A): Formal international law citation.
parties (integer, OPTIONAL): State party count for treaties.

title (string, REQUIRED):
Short human-readable title. Maximum 200 characters.

operative_clause (string, REQUIRED):
Plain-language statement of the prohibition or permission this record represents. Must be understandable by a compliance professional without Cedar knowledge.
Maximum 500 characters.

full_legal_text_summary (string, OPTIONAL):
Broader legal context. Not compiled into Cedar.

agent_check (object, REQUIRED):
Machine-readable specification of what the GEC evaluates at decision time. Primary input to the Cedar Compilation Profile. Specified in Section 4.2.

resource_policy (object, CONDITIONAL):

REQUIRED when tier is "3". Specified in Section 4.3.

conflict_declarations (array, REQUIRED):
Known conflicts with other records. MAY be empty.
Specified in Section 4.4.

certification (object, REQUIRED):
Certification metadata. Specified in Section 4.5.

effective_date (string, REQUIRED):
ISO 8601 date on which the operative clause is effective.

sunset_date (string, OPTIONAL):
ISO 8601 date on which the operative clause ceases effect.

review_trigger (array of string, REQUIRED, minItems: 1):
Events requiring this record to be reviewed.

record_version (string, REQUIRED):
Semantic version of this record. Pattern: "^[0-9]+\.[0-9]+\.[0-9]+$".

supersedes (string, OPTIONAL):
record_id of the record this record replaces.

4.2. agent_check Object

trigger (object, REQUIRED):
action_scope (array of string): Cedar action namespace
patterns to which this record applies.
"Action::*" applies to all actions.
resource_scope (array of string, OPTIONAL).
principal_scope (array of string, OPTIONAL).

required_context_fields (array of object, REQUIRED):
Each entry specifies an IDP or GEC context field:
field_name (string): Cedar context attribute name.
field_type (string): "boolean", "string", "integer",
"enum", or "array".
field_description (string): Plain-language description.
source (string): "IDP_HEADER", "IDP_CONTEXT",
"GEC_STATE", "RESOURCE_STATE", or "PARTY_REGISTRY".
required (boolean): Whether field must be present.

prohibition_condition (object, CONDITIONAL):
REQUIRED when the record represents a prohibition.
condition_plain (string): Plain-language prohibition
condition.
condition_cedar_hint (string): Cedar expression hint
for compiler implementors. NOT normative.
confidence_threshold (string, OPTIONAL): For Tier 1
observation records. One of: "SUSPICIOUS",
"PROBABLE", "EVIDENT".

permission_condition (object, CONDITIONAL):
REQUIRED when the record represents an explicit permission.
Same structure as prohibition_condition.

post_deny_protocol (object, REQUIRED):
recourse_available (boolean): MUST be false for Tier 0-A.
MUST be true for Tier 3.
recourse_types (array of string, CONDITIONAL): REQUIRED
when recourse_available is true. One or more of:
"COMMERCIAL_UPGRADE", "SCOPE_REDUCTION",
"TEMPORAL_DEFERRAL", "OPERATOR_EXCEPTION",
"HEM_ESCALATION", "EXTERNAL_REPORTING".
hem_trigger (string, OPTIONAL): HEM trigger class if

DENY should trigger HEM escalation.
reporting_obligation (object, OPTIONAL):
framework (string): e.g., "BSA_SAR", "EU_AMLD_STR".
deadline_hours (integer): Hours to mandatory filing.
auto_escalate_on_timeout (boolean): Whether GEC escalates externally if principal does not respond before deadline.
event_log_entry (string, REQUIRED): GEC Event Log entry type on DENY. e.g., "CAP_TIER1_DENY".

observation_config (object, CONDITIONAL):
REQUIRED when hem_trigger is "HEM_TIER1_OBSERVED" or "HEM_TIER0_OBSERVED". These trigger classes are defined in Sections 5.6 and 5.7 of [I-D.sato-soos-hem] respectively.
observation_type (string): e.g., "AML", "SANCTIONS", "FRAUD", "CSAM".
confidence_grades (object): Configuration for each
grade (SUSPICIOUS, PROBABLE, EVIDENT):
hem_urgency (string): "STANDARD", "ELEVATED", or "CRITICAL".
session_suspension (boolean).
escalation_targets (array of string).
cluster_propagation (boolean): Whether MUST propagate to related execution agent sessions per CONF-MAD-GEC-03.

4.3. resource_policy Object (Tier 3)

resource_type (string, REQUIRED): "TOKEN", "API_CALL", "TIME_WINDOW", "STORAGE", or "COMPUTE_UNIT".

measurement_unit (string, REQUIRED):
e.g., "tokens", "calls/hour", "seconds", "bytes".

budget_field (string, REQUIRED):
Cedar context attribute name for the budget value.

consumed_field (string, REQUIRED):
Cedar context attribute name for consumed value.

estimated_cost_field (string, REQUIRED):
Cedar context attribute name for estimated action cost.

warning_threshold_pct (integer, REQUIRED):
Consumption percentage at which HEM_TIER3_OBSERVED fires. MUST be between 50 and 95. Default: 80.

anticipatory_assessment (boolean, REQUIRED):
Whether GEC MUST perform Mission Viability Assessment before multi-step missions. When true, HEM_TIER3_ANTICIPATORY fires if full mission cost estimate exceeds remaining budget.

natural_breakpoint_required (boolean, REQUIRED):
Whether agents MUST declare Natural Breakpoints at mission start under this constraint.

recourse_types (array of string, REQUIRED):
One or more of: "COMMERCIAL_UPGRADE", "SCOPE_REDUCTION", "TEMPORAL_DEFERRAL".

reset_field (string, OPTIONAL):
Cedar context attribute carrying budget reset datetime.

upgrade_url_field (string, OPTIONAL):
Cedar context attribute carrying upgrade URL.

4.4. conflict_declarations Array

Each entry:

conflicting_record_id (string, REQUIRED):
The record_id of the conflicting record.

conflict_type (string, REQUIRED): One of:
"DIRECT_CONTRADICTION": Mutually exclusive GEC behaviour on the same trigger condition.
"JURISDICTION_OVERLAP": Same territory, different instruments.
"CONFIDENCE_GRADIENT_OVERLAP": Same observation type, overlapping confidence grades.
"PRIORITY_AMBIGUITY": Both apply; neither declares precedence.

conflict_description (string, REQUIRED):
Plain-language description of the specific conflict.

resolution_strategy (string, REQUIRED): One of:
"THIS_RECORD_TAKES_PRIORITY"
"OTHER_RECORD_TAKES_PRIORITY"
"OPERATOR_DECLARES_PRIORITY": Operator MUST declare resolution at compile time. Compiler error if absent.
"HEM_JURISDICTIONAL_CONFLICT": Irresolvable at compile time. Cedar flagged for runtime HEM Class 5 escalation.

resolution_cedar_hint (string, OPTIONAL):
Cedar expression hint for deterministic resolutions.

4.5. certification Object

certification_tier (string, REQUIRED): "FOUNDATION", "REGULATORY_BODY", "LICENSED_PROVIDER", "OPERATOR", or "SELF". MUST be consistent with record tier per Section 7.1.

certified_by (object, REQUIRED):
publisher_id (string): Registered CMR publisher ID.
publisher_name (string): Human-readable publisher name.
publisher_keypair_id (string): Ed25519 keypair identifier.

certification_date (string, REQUIRED): ISO 8601 datetime.

certification_statement (string, REQUIRED):
Plain-language attestation.

record_signature (string, REQUIRED):
Ed25519 signature over canonical JSON of this record (excluding this field), encoded as base64url.

certification_expiry (string, OPTIONAL):
ISO 8601 datetime. GEC MUST refuse to load after expiry without renewal.

4.6. Complete Schema Reference

The normative JSON Schema (Draft 2020-12) is published at:

https://cap.soos.foundation/schema/regulation-record/cap-rrs-00

The prose specification in Sections 4.1 through 4.5 is normative. The JSON Schema is informative and provided for tooling convenience.

4.7. Tier-Specific Requirements

Tier 0-A:
* legal_source REQUIRED. treaty_citation REQUIRED.
* parties SHOULD be present.
* jurisdiction_scope.territories MUST be ["GLOBAL"].
* conflict_declarations MUST be empty.
* certification.certification_tier MUST be "FOUNDATION".
* post_deny_protocol.recourse_available MUST be false.

Tier 0-B:
* legal_source REQUIRED. treaty_citation REQUIRED.
* jurisdiction_scope.territories MUST be ["GLOBAL"] or defined coalition of state parties.
* post_deny_protocol.recourse_available MUST be false within the prohibition scope.
* certification_tier MUST be "FOUNDATION" or "REGULATORY_BODY".

Tier 1:
* legal_source REQUIRED.
* treaty_citation OPTIONAL (required for treaty-derived national law).
* certification_tier MUST be "REGULATORY_BODY" or "LICENSED_PROVIDER".
* conflict_declarations SHOULD declare any known conflicts with other Tier 1 records for overlapping jurisdictions.

Tier 2:
* legal_source OPTIONAL.
* certification_tier MUST be "OPERATOR".

Tier 3:
* resource_policy REQUIRED.
* post_deny_protocol.recourse_available MUST be true.
* certification_tier MUST be "SELF".

4.8. Worked Examples

4.8.1. Tier 0-A: Genocide Prohibition (Rome Statute)

```
{
  "record_id":      "int.rome_statute.art6",
  "schema_version": "cap-rrs-00",
  "tier":           "0-A",
  "jurisdiction_scope": {
    "territories":      ["GLOBAL"],
    "legal_system":     "INTERNATIONAL",
    "supranational_body": "ICC"
  },
  "legal_source": {
    "instrument_name":
      "Rome Statute of the International Criminal Court",
    "instrument_code":  "ROME_STATUTE",
    "article":          "Article 6",
    "official_url":     "https://www.icc-cpi.int/sites/
                         default/files/RS-Eng.pdf",
    "treaty_citation":
      "Rome Statute of the International Criminal Court,
       17 July 1998, 2187 UNTS 90, Article 6.",
    "parties":          124
  },
  "title": "Genocide -- Absolute Prohibition",
```

```
    "operative_clause":
      "No agent may perform any action that constitutes,
       facilitates, or contributes to acts committed with
       intent to destroy, in whole or in part, a national,
       ethnical, racial or religious group.",
    "agent_check": {
      "trigger": { "action_scope": ["Action::*"] },
      "required_context_fields": [
        {
          "field_name":
            "genocide_risk_assessment",
          "field_type":        "string",
          "field_description":
            "GEC assessment of whether the action
             contributes to genocide risk.",
          "source":            "GEC_STATE",
          "required":          false
        }
      ],
      "prohibition_condition": {
        "condition_plain":
          "Action contributes to genocide as defined by
           Rome Statute Article 6.",
        "condition_cedar_hint":
          "context.genocide_risk_assessment ==
           \"CONFIRMED\" ||
           context.genocide_risk_assessment ==
           \"PROBABLE\""
      },
      "post_deny_protocol": {
        "recourse_available":  false,
        "hem_trigger":         "HEM_TIER0_OBSERVED",
        "event_log_entry":     "CAP_TIER0A_DENY"
      }
    },
    "conflict_declarations": [],
    "certification": {
      "certification_tier":    "FOUNDATION",
      "certified_by": {
        "publisher_id":        "cap.foundation",
        "publisher_name":      "ATP Foundation",
        "publisher_keypair_id":"cap-foundation-2026-01"
      },
      "certification_date":    "2026-05-01T00:00:00Z",
      "certification_statement":
        "This Regulation Record accurately represents the
         operative clause of Rome Statute Article 6 as
         ratified by 124 state parties.",
      "record_signature": "<Ed25519 sig base64url>"
    },
    "effective_date": "1998-07-17",
    "review_trigger": [
      "Additional state party ratification or withdrawal",
      "ICC Assembly amendment to Article 6",
      "ICC Appeals Chamber ruling on genocide definition"
    ],
    "record_version": "1.0.0"
  }
```

4.8.2. Tier 1: GDPR Article 6 Lawful Basis

```
  {
    "record_id":      "eu.gdpr.2016_679.art6",
    "schema_version": "cap-rrs-00",
    "tier":           "1",
```

```
"jurisdiction_scope": {
  "territories":  ["AT","BE","BG","CY","CZ","DE","DK",
                   "EE","ES","FI","FR","GR","HR","HU",
                   "IE","IT","LT","LU","LV","MT","NL",
                   "PL","PT","RO","SE","SI","SK"],
  "legal_system": "CIVIL",
  "supranational_body": "EU"
},
"legal_source": {
  "instrument_name":
    "Regulation (EU) 2016/679 (GDPR)",
  "instrument_code":  "GDPR",
  "article":
    "Article 6 -- Lawfulness of processing",
  "official_url":
    "https://eur-lex.europa.eu/legal-content/EN/TXT/
     ?uri=CELEX:32016R0679"
},
"title":
  "GDPR Article 6 -- Lawful Basis for Data Processing",
"operative_clause":
  "Processing of personal data is unlawful unless at
   least one lawful basis applies: consent, contract,
   legal obligation, vital interests, public task, or
   legitimate interests.",
"agent_check": {
  "trigger": {
    "action_scope":  ["Action::data_processing::*"],
    "resource_scope":["Resource::personal_data::*"]
  },
  "required_context_fields": [
    {
      "field_name":    "lawful_basis",
      "field_type":    "string",
      "field_description":
        "The lawful basis for processing this data.",
      "source":        "IDP_CONTEXT",
      "required":      true
    },
    {
      "field_name":    "data_category",
      "field_type":    "string",
      "field_description":
        "Category of personal data being processed.",
      "source":        "IDP_CONTEXT",
      "required":      true
    },
    {
      "field_name":    "data_subject_consent",
      "field_type":    "boolean",
      "field_description":
        "Whether valid consent is present.",
      "source":        "IDP_CONTEXT",
      "required":      false
    }
  ],
  "prohibition_condition": {
    "condition_plain":
      "No lawful basis is present, or consent is
       required but absent.",
    "condition_cedar_hint":
      "!context.lawful_basis.has_value() ||
       (context.lawful_basis == \"CONSENT\" &&
        !context.data_subject_consent)"
  },
  "post_deny_protocol": {
```

```
      "recourse_available": true,
      "recourse_types":     ["OPERATOR_EXCEPTION",
                             "HEM_ESCALATION"],
      "hem_trigger":
        "HEM_JURISDICTIONAL_CONFLICT",
      "event_log_entry":    "CAP_TIER1_DENY"
    }
  },
  "conflict_declarations": [
    {
      "conflicting_record_id":
        "eu.medical_act.mandatory_reporting",
      "conflict_type":
        "DIRECT_CONTRADICTION",
      "conflict_description":
        "GDPR consent revocation conflicts with
         mandatory disease reporting in some EU
         member states.",
      "resolution_strategy":
        "HEM_JURISDICTIONAL_CONFLICT"
    }
  ],
  "certification": {
    "certification_tier":    "REGULATORY_BODY",
    "certified_by": {
      "publisher_id":        "eu.edpb",
      "publisher_name":
        "European Data Protection Board",
      "publisher_keypair_id":"edpb-2026-01"
    },
    "certification_date":    "2026-03-15T00:00:00Z",
    "certification_statement":
      "This Regulation Record accurately represents
       the operative clause of GDPR Article 6 as
       interpreted by EDPB Guidelines 01/2020.",
    "record_signature": "<Ed25519 sig base64url>"
  },
  "effective_date": "2018-05-25",
  "review_trigger": [
    "CJEU ruling on Article 6 interpretation",
    "EDPB guideline update on lawful basis",
    "GDPR amendment by European Parliament"
  ],
  "record_version": "2.1.0"
}
```

4.8.3. Tier 1: AML Suspicious Transaction (BSA / FinCEN)

```
{
  "record_id":      "us.bsa.1970.sar_obligation",
  "schema_version": "cap-rrs-00",
  "tier":           "1",
  "jurisdiction_scope": {
    "territories":  ["US"],
    "legal_system": "COMMON"
  },
  "legal_source": {
    "instrument_name":
      "Bank Secrecy Act (31 U.S.C. 5318(g))",
    "instrument_code":  "BSA",
    "article":
      "31 U.S.C. 5318(g) -- Reporting of suspicious
       transactions"
  },
  "title":
```

```
  "BSA -- Suspicious Activity Report Obligation",
"operative_clause":
  "Financial institutions must report suspicious
   transactions involving possible money laundering
   or financial crimes. Reporting is mandatory when
   evidence confidence reaches PROBABLE or higher.",
"agent_check": {
  "trigger": {
    "action_scope": ["Action::financial::transfer::*",
                     "Action::financial::payment::*"]
  },
  "required_context_fields": [
    {
      "field_name":    "aml_confidence_grade",
      "field_type":    "string",
      "field_description":
        "AML pattern match confidence grade.",
      "source":        "GEC_STATE",
      "required":      false
    },
    {
      "field_name":    "counterparty_risk_level",
      "field_type":    "string",
      "field_description":
        "Risk level of the transaction counterparty.",
      "source":        "IDP_CONTEXT",
      "required":      false
    },
    {
      "field_name":    "typology_match_id",
      "field_type":    "string",
      "field_description":
        "FinCEN typology pattern match identifier.",
      "source":        "GEC_STATE",
      "required":      false
    }
  ],
  "prohibition_condition": {
    "condition_plain":
      "Transaction matches AML typology with EVIDENT
       confidence, or involves a sanctioned
       counterparty.",
    "confidence_threshold": "EVIDENT",
    "condition_cedar_hint":
      "context.aml_confidence_grade == \"EVIDENT\"
       || context.counterparty_risk_level ==
       \"SANCTIONED\""
  },
  "post_deny_protocol": {
    "recourse_available": false,
    "hem_trigger":        "HEM_TIER1_OBSERVED",
    "reporting_obligation": {
      "framework":              "BSA_SAR",
      "deadline_hours":         720,
      "auto_escalate_on_timeout": true
    },
    "event_log_entry":    "CAP_TIER1_DENY"
  },
  "observation_config": {
    "observation_type": "AML",
    "confidence_grades": {
      "SUSPICIOUS": {
        "hem_urgency":        "STANDARD",
        "session_suspension": false,
        "escalation_targets": ["COMPLIANCE_OFFICER"]
      },
```

```
          "PROBABLE": {
            "hem_urgency":        "ELEVATED",
            "session_suspension": false,
            "escalation_targets": ["COMPLIANCE_OFFICER",
                                   "LEGAL_COUNSEL"]
          },
          "EVIDENT": {
            "hem_urgency":        "CRITICAL",
            "session_suspension": true,
            "escalation_targets": ["COMPLIANCE_OFFICER",
                                   "LEGAL_COUNSEL",
                                   "SENIOR_PRINCIPAL"]
          }
        },
        "cluster_propagation": true
      }
    },
    "conflict_declarations": [],
    "certification": {
      "certification_tier":    "REGULATORY_BODY",
      "certified_by": {
        "publisher_id":
          "us.fincen",
        "publisher_name":
          "Financial Crimes Enforcement Network",
        "publisher_keypair_id": "fincen-2026-01"
      },
      "certification_date":    "2026-04-01T00:00:00Z",
      "certification_statement":
        "This Regulation Record accurately represents
         the BSA Section 5318(g) SAR obligation as
         implemented in 31 CFR 1020.320.",
      "record_signature": "<Ed25519 sig base64url>"
    },
    "effective_date": "1992-04-01",
    "review_trigger": [
      "FinCEN rulemaking amending SAR thresholds",
      "BSA amendment by Congress",
      "FATF mutual evaluation recommendation"
    ],
    "record_version": "3.2.1"
  }
```

4.8.4. Tier 2: Operator Data Access Policy

```
  {
    "record_id":      "acme.agent.data_access.v1",
    "schema_version": "cap-rrs-00",
    "tier":           "2",
    "jurisdiction_scope": {
      "territories":  ["US","EU"],
      "legal_system": "HYBRID"
    },
    "title":
      "ACME -- Agent Data Access Restriction",
    "operative_clause":
      "Agents may only access records of principals
       explicitly assigned to the current session.",
    "agent_check": {
      "trigger": {
        "action_scope": ["Action::data_access::*"]
      },
      "required_context_fields": [
        {
          "field_name":    "accessing_principal_id",
```

```
        "field_type":    "string",
        "field_description":
          "Principal whose records agent is accessing.",
        "source":        "IDP_CONTEXT",
        "required":      true
      },
      {
        "field_name":
          "session_assigned_principals",
        "field_type":    "array",
        "field_description":
          "Principal IDs assigned to current session.",
        "source":        "GEC_STATE",
        "required":      true
      }
    ],
    "prohibition_condition": {
      "condition_plain":
        "The accessing principal is not in the
         session's assigned principal list.",
      "condition_cedar_hint":
        "!context.session_assigned_principals
         .contains(context.accessing_principal_id)"
    },
    "post_deny_protocol": {
      "recourse_available": true,
      "recourse_types":     ["HEM_ESCALATION",
                             "OPERATOR_EXCEPTION"],
      "hem_trigger":        "HEM_CEDAR_ROUTED",
      "event_log_entry":    "CAP_TIER2_DENY"
    }
  },
  "conflict_declarations": [],
  "certification": {
    "certification_tier":    "OPERATOR",
    "certified_by": {
      "publisher_id":        "acme.corp",
      "publisher_name":      "ACME Corporation",
      "publisher_keypair_id":"acme-ops-2026-01"
    },
    "certification_date":    "2026-05-01T00:00:00Z",
    "certification_statement":
      "ACME Corporation operator data access policy v1.",
    "record_signature": "<Ed25519 sig base64url>"
  },
  "effective_date": "2026-05-01",
  "review_trigger": [
    "ACME data governance policy update"
  ],
  "record_version": "1.0.0"
}
```

4.8.5. Tier 3: Token Budget Resource Policy

```
{
  "record_id":      "acme.resource.token_budget.v1",
  "schema_version": "cap-rrs-00",
  "tier":           "3",
  "jurisdiction_scope": {
    "territories":  ["GLOBAL"],
    "legal_system": "INTERNATIONAL"
  },
  "title":
    "ACME -- Standard Token Budget (100,000 tokens)",
  "operative_clause":
```

```
  "Agent sessions may not consume more than 100,000
   tokens per billing period. Anticipatory assessment
   is required for multi-step missions.",
"agent_check": {
  "trigger": {
    "action_scope": ["Action::*"]
  },
  "required_context_fields": [
    {
      "field_name":    "tokens_remaining",
      "field_type":    "integer",
      "field_description":
        "Tokens remaining in current billing period.",
      "source":        "RESOURCE_STATE",
      "required":      true
    },
    {
      "field_name":    "action_estimated_cost",
      "field_type":    "integer",
      "field_description":
        "Estimated token cost of pending action.",
      "source":        "GEC_STATE",
      "required":      true
    }
  ],
  "prohibition_condition": {
    "condition_plain":
      "Estimated action cost exceeds remaining token
       budget.",
    "condition_cedar_hint":
      "context.tokens_remaining <
       context.action_estimated_cost &&
       !context.upgrade_authorized"
  },
  "post_deny_protocol": {
    "recourse_available": true,
    "recourse_types":     ["COMMERCIAL_UPGRADE",
                           "SCOPE_REDUCTION",
                           "TEMPORAL_DEFERRAL"],
    "hem_trigger":
      "HEM_TIER3_ANTICIPATORY",
    "event_log_entry":    "CAP_TIER3_DENY"
  }
},
"resource_policy": {
  "resource_type":             "TOKEN",
  "measurement_unit":          "tokens",
  "budget_field":              "token_budget",
  "consumed_field":            "tokens_consumed",
  "estimated_cost_field":
    "action_estimated_cost",
  "warning_threshold_pct":     80,
  "anticipatory_assessment":   true,
  "natural_breakpoint_required":true,
  "recourse_types":            ["COMMERCIAL_UPGRADE",
                                "SCOPE_REDUCTION",
                                "TEMPORAL_DEFERRAL"],
  "reset_field":               "budget_reset_at",
  "upgrade_url_field":         "upgrade_url"
},
"conflict_declarations": [],
"certification": {
  "certification_tier":    "SELF",
  "certified_by": {
    "publisher_id":        "acme.corp",
    "publisher_name":      "ACME Corporation",
```

```
      "publisher_keypair_id":"acme-ops-2026-01"
    },
    "certification_date":    "2026-05-01T00:00:00Z",
    "certification_statement":
      "ACME standard token budget resource policy.",
    "record_signature": "<Ed25519 sig base64url>"
  },
  "effective_date": "2026-05-01",
  "review_trigger": [
    "ACME pricing model update"
  ],
  "record_version": "1.0.0"
}
```


5. Cedar Compilation Profile

5.1. Compilation Overview

The Cedar Compilation Profile is the normative specification for translating Regulation Records into Cedar policies. A conforming compiler MUST produce semantically equivalent Cedar from identical Regulation Records. Semantic equivalence means the compiled Cedar produces identical ALLOW/DENY results for all possible Cedar context inputs.

The compiler processes records in tier order: Tier 0-A first, then 0-B, 1, 2, 3. Within each tier, records are processed in record_id lexicographic order.

5.2. Field Mapping: agent_check to Cedar

For each Regulation Record the compiler produces:

(a) A Cedar forbid clause from prohibition_condition. Principal, action, and resource scopes derived from trigger fields.

(b) A Cedar permit clause from permission_condition when present.

(c) Cedar context type annotations for each field in required_context_fields.

(d) An annotation block on each Cedar policy carrying: record_id, tier, jurisdiction_scope.territories, effective_date, and record_version. These annotations enable the GEC to produce structured DENY reason codes referencing the specific Regulation Record that fired.

The condition_cedar_hint field is informative. The compiler MAY use it to guide expression generation but MUST NOT reproduce it verbatim without validation.

5.3. Conflict Surfacing at Compile Time

For each conflict_declaration with resolution_strategy "HEM_JURISDICTIONAL_CONFLICT", the compiler MUST generate a Cedar policy annotation marking the conflicting trigger pattern as a HEM_JURISDICTIONAL_CONFLICT (Class 5) candidate. The GEC MUST check this annotation at runtime and fire HEM_JURISDICTIONAL_CONFLICT when both conflicting policies would fire on the same context.

For deterministic resolutions, the compiler MUST generate Cedar priority annotations using the Cedar priority mechanism.

5.4. Compiler Conformance Requirements

CONF-CAP02-COMP-01: A conforming compiler MUST accept all Regulation Records conforming to the Section 4 schema.

CONF-CAP02-COMP-02: A conforming compiler MUST reject any Regulation Record with an invalid or expired certification signature.

CONF-CAP02-COMP-03: A conforming compiler MUST surface all conflict_declarations with strategy "OPERATOR_DECLARES_PRIORITY" as compile-time errors requiring explicit operator resolution before a Cedar policy set is produced.

CONF-CAP02-COMP-04: A conforming compiler MUST produce Cedar carrying Regulation Record annotations per Section 5.2(d) on every policy clause.

CONF-CAP02-COMP-05: A conforming compiler MUST NOT produce Cedar for a Regulation Record that has reached sunset_date.

6. Conflict Declaration Model

6.1. Conflict Types

See Section 4.4 for conflict type definitions.

6.2. Static vs. Runtime Conflicts

Static conflicts are detectable at compile time because both records apply to the same action_scope and their prohibition conditions are structurally contradictory. The compiler MUST detect and surface all static conflicts.

Runtime conflicts arise only when a specific combination of Cedar context values triggers both policies simultaneously in ways not detectable from schemas alone. The compiler surfaces these as HEM_JURISDICTIONAL_CONFLICT annotations; the GEC detects them at evaluation time.

6.3. Conflict Resolution Protocol

When the compiler surfaces a conflict with strategy "OPERATOR_DECLARES_PRIORITY", the operator MUST provide a signed resolution declaration before compilation proceeds:

```
{
  "resolution_id": "acme.resolution.gdpr_vs_medical",
  "record_a":      "eu.gdpr.2016_679.art6",
  "record_b":      "eu.medical_act.mandatory_reporting",
  "resolution":    "OTHER_RECORD_TAKES_PRIORITY",
  "legal_basis":
    "EU member state medical act takes precedence over
     GDPR under Article 9(2)(i) for mandatory disease
     reporting.",
  "authorized_by": "acme.legal.counsel",
  "authorization_date": "2026-05-15"
}
```

Resolution declarations are signed by the operator keypair and stored in the GAR audit record [I-D.sato-soos-gar].

7. Certification Model

7.1. Publisher Tiers

FOUNDATION: ATP Foundation. Certifies Tier 0-A and 0-B records only. Certification is against treaty text.

REGULATORY_BODY: National or supranational regulatory authority. Certifies Tier 1 records within their statutory jurisdiction.

LICENSED_PROVIDER: Third-party compliance provider licensed by a regulatory body. Certifies Tier 1 records within license scope.

OPERATOR: The deploying organization. Certifies Tier 2. No external approval required.

SELF: Developer or operator. Certifies Tier 3. No external approval required.

7.2. Certification Process

Publisher registration: Publishers register with the CMR by submitting their Ed25519 public key, jurisdiction scope, and certification tier. FOUNDATION and REGULATORY_BODY publishers undergo identity verification before registration.

Record certification: The publisher signs the canonical JSON of the Regulation Record (excluding record_signature) with their registered Ed25519 private key and encodes as base64url.

Package publication: The publisher assembles certified records into a signed package and submits to the CMR.

7.3. Certification Verification

A GEC loading a Regulation Record package MUST:

(a) Verify the publisher's CMR registration is current.
(b) Verify each record_signature against the publisher's registered Ed25519 public key.
(c) Verify certification_expiry has not passed.
(d) Verify certification_tier is consistent with record tier per Section 4.7.

A GEC MUST NOT load a package that fails any verification.

8. Constitutional Mandate Registry Protocol

8.1. Package Structure

```
{
  "package_id":        "eu.gdpr.2016/679",
  "package_version":   "2.1.0",
  "publisher_id":      "eu.edpb",
  "records":           [ ... Regulation Records ... ],
  "changelog":         [ ... version entries ... ],
  "conflicts_with":    [ ... incompatible packages ... ],
  "package_signature": "<Ed25519 over canonical JSON>"
}
```

8.2. Versioning

Packages use Semantic Versioning [SEMVER]:

MAJOR: An operative clause changed such that previously permitted actions may now be denied. GEC operator review REQUIRED before upgrade.

MINOR: New operative clauses added. Previously permitted actions unaffected. GEC operator review RECOMMENDED.

PATCH: Metadata updates only. No change to Cedar output. Automatic upgrade PERMITTED.

8.3. Update Notification

On new package version publication, the CMR sends a signed Update Notification to all registered GEC subscribers:

```
{
  "package_id":     "eu.gdpr.2016/679",
  "new_version":    "2.2.0",
  "change_type":    "MINOR",
  "changed_records":["eu.gdpr.2016_679.art6"],
  "change_summary":
    "Updated to reflect EDPB Guidelines 05/2026",
  "effective_by":   "2026-09-01T00:00:00Z"
}
```

8.4. GEC Update Response Options

ACCEPT: Apply the update automatically. Permitted for PATCH. RECOMMENDED for MINOR with standing regulatory currency policy.

REVIEW_AND_APPROVE: Queue for operator review. Required for MAJOR changes.

PIN: Pin to current version with declared expiry. CMR MUST be notified. GEC MUST refuse the pinned version after expiry.

CONF-CAP02-REG-01: A GEC MUST NOT operate on a Regulation Record package that has reached certification_expiry without renewal or replacement.

CONF-CAP02-REG-02: A GEC MUST surface MAJOR version Update Notifications to the operator within 24 hours of receipt.

9. HEM Integration

9.1. HEM_TIER3_ANTICIPATORY (Class 8)

Trigger: Before beginning a multi-step mission, the GEC determines that total estimated resource cost exceeds remaining budget under any active Tier 3 resource policy with anticipatory_assessment: true.

The GEC MUST:
(a) Halt mission execution before any step begins.
(b) Construct an Execution Options Package (Section 9.3).
(c) Route to the human principal designation chain with urgency STANDARD.
(d) Await human decision before proceeding.

Human decision types for Class 8:
APPROVE_WITH_CONSTRAINTS: Scope reduction -- proceed to a named Natural Breakpoint only.
APPROVE_WITH_PAYMENT: Commercial upgrade -- proceed with full mission after upgrade confirmation.
DEFER: Temporal deferral -- await budget reset.

DENY: Do not begin mission.

9.2. HEM_TIER3_OBSERVED (Class 9)

Trigger: During mission execution, resource consumption reaches warning_threshold_pct in the active Tier 3 policy.

The GEC MUST:
(a) NOT halt execution immediately.
(b) Identify the next Natural Breakpoint.
(c) Construct an Execution Options Package for remaining mission.
(d) Route to the human principal with urgency ELEVATED.
(e) Commit to completing to the next Natural Breakpoint before stopping, regardless of human response timing.

9.3. Execution Options Package

Carried in HEM escalation requests for Class 8 and 9:

```
{
  "full_mission_viable":  boolean,
  "budget_available":     integer,
  "budget_required":      integer,
  "shortfall":            integer,
  "natural_breakpoints": [
    {
      "breakpoint_id":    string,
      "description":      string,
      "cost_to_reach":    integer,
      "viable":           boolean,
      "value_delivered":  string
    }
  ],
  "recourse_options": [
    {
      "option_id":        string,
      "type":             string,
      "description":      string,
      "viable":           boolean,
      "cost":             integer or null,
      "upgrade_url":      string or null,
      "reset_at":         string or null
    }
  ],
  "recommended_option":   string
}
```

Example for "research, write report, send emails to all clients" with 45,000 tokens remaining and 95,000 required:

```
natural_breakpoints:
  BP-1: Research complete. cost: 40,000. viable: true.
        value_delivered: "Research findings."
  BP-2: Report complete.   cost: 60,000. viable: false.
        value_delivered: "Complete report."
  BP-3: Full mission.      cost: 95,000. viable: false.
        value_delivered: "Research + report + emails."

recourse_options:
  RO-1: SCOPE_REDUCTION.  Proceed to BP-1 only.
        viable: true.  cost: 40,000.
  RO-2: COMMERCIAL_UPGRADE.  Upgrade to proceed in full.
        viable: true.  upgrade_url: "..."
  RO-3: TEMPORAL_DEFERRAL.  Budget resets in 6 hours.
        viable: true.  reset_at: "2026-05-30T06:00:00Z"
```

recommended_option: "RO-1"

9.4. Natural Breakpoint Declaration

Agents operating under a resource policy with natural_breakpoint_required: true MUST declare Natural Breakpoints at the PLAN step of the AEP execution loop before beginning multi-step mission execution.

A Natural Breakpoint is a point at which stopping produces a coherent, complete deliverable of independent value.

CONF-CAP02-HEM-01: A GEC implementing Tier 3 resource policies with natural_breakpoint_required: true MUST refuse to begin multi-step mission execution without a Natural Breakpoint declaration from the agent.

CONF-CAP02-HEM-02: A GEC MUST NOT stop a mission mid-task on a Tier 3 resource limit when a Natural Breakpoint declaration is registered. The GEC MUST complete to the next declared Natural Breakpoint before enforcing the limit.

10. Open Issues

10.1. Pattern-Before-Threshold (OQ-CAP-PATTERN)

Detecting a prohibited pattern before any individual observation crosses the confidence threshold -- by reasoning over a trajectory of observations -- is not fully specified. The typology_match_id field provides partial support, but Cedar policy evaluation over event stream trajectories requires formal verification methods not yet specified. Deferred to a successor document.

10.2. Cross-Jurisdiction Tier 1 Compilation (OQ-CAP-XJURIS)

When a single agent session spans multiple jurisdictions, the mechanism for selecting the correct jurisdiction-specific record at Cedar evaluation time is not yet specified. The jurisdiction_scope field provides the metadata; the runtime selection algorithm requires further specification.

11. Security Considerations

Regulation Record integrity depends on publisher Ed25519 keypair security. Keypair compromise would allow injection of fraudulent records. The CMR MUST support keypair rotation with a defined transition period. GEC implementations MUST verify record_signature on every package load.

The Cedar Compilation Profile determinism requirement (Section 5.1) is a security property: it ensures that a certified Regulation Record produces identical Cedar across all conforming compiler implementations.

12. Privacy Considerations

Regulation Records do not contain personal data. The GEC audit records produced on DENY events carry the record_id of the firing Regulation Record as metadata only.

13. IANA Considerations

IANA is requested to register the following media type:
application/cap-regulation-record+json

This media type identifies a Regulation Record conforming to the schema defined in Section 4 of this document.

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

[I-D.sato-soos-cap] Sato, T., "Constitutional AI Protocol (CAP)", Work in Progress, Internet-Draft, draft-sato-soos-cap-01, May 2026, <https://datatracker.ietf.org/doc/draft-sato-soos-cap/>.

[I-D.sato-soos-hem] Sato, T., "Human Escalation Mechanism (HEM)", Work in Progress, Internet-Draft, draft-sato-soos-hem-03, May 2026, <https://datatracker.ietf.org/doc/draft-sato-soos-hem/>.

[I-D.sato-soos-idp] Sato, T., "Intent Declaration Primitive (IDP)", Work in Progress, Internet-Draft, draft-sato-soos-idp-03, May 2026.

[I-D.sato-soos-gar] Sato, T., "Governance Audit Record (GAR)", Work in Progress, Internet-Draft, draft-sato-soos-gar-01, May 2026.

[SEMVER] Preston-Werner, T., "Semantic Versioning 2.0.0", 2013, <https://semver.org/>.

14.2. Informative References

[I-D.sato-soos-mad] Sato, T., "Multi-Agent Delegation (MAD)", Work in Progress, Internet-Draft, draft-sato-soos-mad-01, May 2026.

[I-D.sato-soos-aep] Sato, T., "Agent Execution Protocol (AEP)", Work in Progress, Internet-Draft, draft-sato-soos-aep-00, May 2026.

[ROME_STATUTE] United Nations, "Rome Statute of the International Criminal Court", 17 July 1998, 2187 UNTS 90.

[GDPR] European Parliament and Council, "Regulation (EU) 2016/679", 27 April 2016, OJ L 119/1.

[BSA] United States Congress, "Bank Secrecy Act", 31 U.S.C. 5318(g), 1970.

[CEDAR] Amazon Web Services, "Cedar Policy Language Reference", 2023, <https://docs.cedarpolicy.com/>.

Acknowledgments

The Regulation Record schema, Cedar Compilation Profile, and Constitutional Mandate Registry concept emerged from SOOS KernelSpec V3 development sessions in May 2026. The discussion of tier-specific recourse availability, the compliance-as-package-management model, the Natural Breakpoint Declaration, and the HEM_TIER3 trigger classes originated in those sessions. CAP-RRS is a companion document to CAP-01 [I-D.sato-soos-cap]; it does not revise or supersede it.

Author’s Address

Tom Sato
MyAuberge K.K.
Chino, Nagano
Japan
Email: tomsato@myauberge.jp