Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 5 July 2026

A. Hernandez
Varlil Corporation

1 January 2026

The Cosmos Protocol Specification (Trust-Native Semantic Protocol) draft-cosmos-protocol-specification-00

Abstract

The Cosmos Protocol (Trust-Native Semantic Protocol) defines a badge-based identity and communication system intended for deployments that prefer not to rely on external consensus or blockchain infrastructure. Cosmos supports trust-native communication and decentralized identity management through cryptographically signed badges that operate without mandatory external trust systems. The protocol also supports passwordless authentication flows using badge-based credentials and biometric authenticators, reducing reliance on traditional password mechanisms.

The Cosmos Protocol introduces several foundational innovations that together form an integrated identity-native communication substrate. These include: (1) Badge-Based Identity -- cryptographically signed, capability-bearing identifiers designed to operate without requiring blockchain or distributed ledger infrastructure, while allowing deployments to integrate such systems if desired; (2) Trust Scoring -- reputation-anchored trust models (domain-bound for DNS networks, star-bound for Cosmos-native networks) that enable cross-star capability granting and trust-based authorization without requiring new badges; (3) Lumen Encryption -- uses post-quantum candidate cryptographic primitives (see [RFC-XXXX-Lumen]), badge-native encryption designed to support forward secrecy; (4) Echo Grammar -- semantic message structures that provide intent clarity, UI hints, and agent compatibility; (5) Capsule System -- universal, encrypted containers for communication and storage; (6) Slipstream Transport (TNTP) -- a trust-native transport protocol with badge-based sessions, intent-aware routing, and the ability to operate without blockchain or external consensus dependencies; (7) Ramp and SDFF Serialization -- deterministic text and binary formats that provide canonical structure for all Cosmos data; (8) Profile System -- portable, domain-scoped user profiles with badge-based access control; and (9) Productivity Protocols -- standardized scheduling, contacts, and calendaring protocols (Comet, Nebula, Nova) that provide a badge-native model that can serve as an alternative to multiple legacy standards.

Cosmos badges are Ramp (Slope Data Format, SDF) documents with optional DID compatibility, allowing integration with existing decentralized identity systems while preserving the protocol's self-contained architecture within Cosmos deployments. The badge system addresses key limitations in current identity approaches, including the lack of enterprise-grade lifecycle management, star-bound trust establishment, and the ability to operate independently of external infrastructure in constrained or disconnected environments.

The protocol provides a viable alternative to complex identity stacks while maintaining interoperability with existing standards, making it suitable for both greenfield deployments and integration with existing systems.

Note

This document is in draft status and represents a proposed standard for the Cosmos Protocol specification.

Status of This Memo

Copyright Notice

Table of Contents

1. 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."

2. Introduction

This document specifies the Cosmos Protocol, a trust-native, badge-based identity and communication system designed for enterprise deployment without requiring blockchain or distributed ledger infrastructure. The protocol provides a viable alternative to existing decentralized identity solutions by combining identity management, trust scoring, encryption, and communication in a unified, self-contained system within Cosmos deployments.

This document does not obsolete or update any existing RFCs. It defines a new protocol specification intended for use in enterprise identity and communication systems, decentralized applications, and environments that can operate without external consensus or blockchain infrastructure.

2.1. Problem Statement

Current decentralized identity and communication systems face fundamental limitations that prevent widespread adoption and practical deployment:

Infrastructure Dependencies: Most decentralized identity solutions require complex infrastructure dependencies including blockchain networks, distributed ledgers, or specialized consensus mechanisms. These dependencies create barriers to deployment, especially in constrained environments, enterprise settings, or scenarios requiring rapid deployment.

Trust Quantification Challenges: Existing systems lack effective mechanisms for quantifying trustworthiness between entities. Without reliable trust metrics, users cannot make informed decisions about communication partners, leading to either excessive caution or inappropriate trust.

Enterprise Integration Gaps: Current solutions often focus on individual identity management but fail to address enterprise requirements such as lifecycle management, organizational hierarchies, domain-based policies, and integration with existing infrastructure.

Communication Fragmentation: Identity and communication systems are typically separate, requiring complex integration work and creating security gaps between authentication and messaging.

Walled Garden Communication: Modern communication platforms create walled gardens where users on different platforms cannot communicate effectively. This forces users to rely on email systems for cross-platform communication, even when other chat and messaging solutions may be preferred. Users must maintain multiple accounts across different platforms, fragmenting their communication and social graph. Cross-platform interoperability is limited or non-existent, preventing users from choosing preferred communication tools while maintaining universal connectivity.

Profile Data Fragmentation and Lock-in: User profiles are fragmented across multiple platforms, each with its own data silo. Users must recreate their profiles on each platform, losing their social graph and content when switching providers. Profile data is locked into individual platforms with no portability, preventing users from migrating their profiles, content, and relationships. Users lack control over their profile data and privacy settings across platforms, leading to data silos and vendor lock-in.

Scalability Limitations: Many decentralized systems struggle with scalability, either requiring significant computational resources or failing to handle enterprise-scale deployments effectively.

Password-Based Authentication Weaknesses: Traditional password-based authentication systems suffer from fundamental security weaknesses including password reuse, weak passwords, password theft, phishing attacks, and the burden of password management. Users are forced to create, remember, and manage passwords across multiple services, leading to security vulnerabilities and poor user experience. Password-based systems also lack built-in identity verification and trust establishment mechanisms, requiring external trust systems.

2.2. Solution Overview

The Cosmos Protocol addresses these challenges through a comprehensive badge-based identity and communication system that supports the following capabilities:

Infrastructure Independence: Cosmos can operate without blockchain, distributed ledgers, or external consensus mechanisms. The protocol is self-contained within Cosmos deployments and can be deployed in any environment, including constrained environments and enterprise data centers, without external consensus or blockchain infrastructure.

Star-bound Trust Scoring: A trust algorithm designed to reduce manipulation risks that quantifies trustworthiness using star reputation, network effects, and behavioral patterns, enabling informed trust decisions without centralized authorities.

Enterprise-ready Identity Management: Lifecycle management for badge issuance, renewal, revocation, and organizational hierarchies, designed for enterprise deployment scenarios.

Productivity Protocols: Integrated scheduling, contacts, and calendar protocols (Comet, Nebula, Nova) that interoperate with the badge-based identity system, reducing security gaps between authentication and communication.

Cross-Provider Interoperability: Interlink enables cross-provider interoperability for participating platforms. Users can communicate seamlessly across different providers while each provider maintains their unique features and user experience. This enables users to use preferred chat and messaging solutions for cross-platform communication while maintaining connectivity across participating platforms. Users maintain a single identity and social graph that works across participating providers.

Profile System: The Cosmos Profile System is designed to support portability across participating providers, subject to provider implementation and policy. Cosmos reduces fragmentation by defining a consistent profile format with domain-scoped data spaces. Users maintain a single canonical profile that functions across participating providers, reducing duplication and data silos. Domain spaces allow each service to store its own data within the user’s profile, while users retain full control over privacy settings and migration. Users may migrate their profiles, content, and social graph between participating providers without data loss, subject to provider support. Profiles are private by default and require explicit user action to make public, ensuring user-controlled visibility.

Scalability: The architecture is intended to support deployments ranging from small installations to large multi-service environments, with design considerations for maintaining performance and security across varying scales.

Passwordless Authentication: Cosmos authentication flows are designed to minimize password usage by supporting badge-based credentials and FIDO2/Passkey-compliant biometric authenticators. Badge-based authentication reduces reliance on passwords and mitigates common password-related vulnerabilities such as password reuse, weak passwords, password theft, and phishing attacks. Badge-based authentication also provides built-in identity verification and trust establishment within Cosmos deployments without requiring external trust systems.

2.3. Why Not Existing Solutions?

2.3.1. Why Not Decentralized Identifiers (DIDs)?

DIDs [W3C-DID] provide a flexible decentralized identity model. Cosmos focuses on a different deployment profile by emphasizing self-contained operation and integrated trust scoring. The following differences highlight Cosmos's approach:

Infrastructure Complexity: DIDs require complex resolver infrastructure, method-specific implementations, and often depend on blockchain or distributed ledger technology. This creates deployment barriers and operational complexity that Cosmos avoids through its self-contained design within Cosmos deployments.

Trust Quantification Gap: DIDs provide cryptographic verification but lack built-in trust scoring mechanisms. Cosmos includes star-bound trust scoring that supports informed decisions about communication partners without relying on external trust systems.

Enterprise Lifecycle Management: DIDs focus on individual identity but do not provide enterprise features such as organizational hierarchies, star-based policies, or integrated lifecycle management, which Cosmos is designed to support.

Communication Integration: DIDs are primarily identity-focused and require separate integration with communication systems. Cosmos provides unified identity and communication protocols, reducing integration complexity and security gaps between identity and communication systems.

Deployment Flexibility: DIDs often require specific infrastructure choices (blockchain, resolver networks) that limit deployment options. Cosmos can be deployed in any environment without infrastructure dependencies.

Badge-DID Compatibility: Cosmos badges are Ramp (Slope Data Format, SDF) [RFC-XXXX-Ramp] documents with optional DID [W3C-DID] compatibility, allowing integration with existing decentralized identity systems while preserving the protocol's self-contained architecture within Cosmos deployments. This enables Cosmos deployments to interoperate with DID ecosystems without depending on external DID infrastructure.

The Cosmos approach provides an integrated, enterprise-oriented solution that addresses practical deployment needs while maintaining interoperability with existing decentralized identity standards.

2.3.2. Why Not LDAP or Active Directory?

LDAP [RFC4511] and Active Directory provide mature directory services. Cosmos targets scenarios that require integrated trust scoring, badge-based authentication, and unified communication semantics. The following differences highlight Cosmos's approach:

Password-Based Authentication: All LDAP implementations (including Active Directory, OpenLDAP, 389 Directory Server, Apache Directory Server, FreeIPA, eDirectory, and other LDAP-based directory services) rely on password-based authentication, which is vulnerable to password reuse, weak passwords, password theft, and phishing attacks. Cosmos uses badge-based authentication with FIDO2/Passkey-compliant biometric authentication, eliminating the need for passwords within standard Cosmos authentication flows and providing cryptographic proof of identity.

Centralized Architecture: LDAP and Active Directory are centralized systems with single points of failure, domain controller dependencies, and global catalog bottlenecks. Cosmos supports distributed, edge-based deployment models that reduce single-point-of-failure risks, enabling global distribution and automatic scaling.

Trust Establishment Gap: LDAP and Active Directory lack effective mechanisms for establishing and quantifying trust between entities. Cosmos includes star-bound trust scoring that enables informed decisions about communication partners without requiring external trust systems.

Communication Integration: LDAP and Active Directory are primarily identity/directory-focused and require separate integration with communication systems. Cosmos provides unified identity and communication protocols, reducing integration complexity and security gaps between authentication and messaging systems.

Directory Scope Limitation: LDAP is purely a directory query protocol for hierarchical data structures. Cosmos is an integrated identity and communication protocol that includes directory-like query capabilities (Manifest) as one component of a broader system that integrates identity, trust, encryption, messaging, and productivity protocols into a unified, badge-native system.

Key Advantages: Cosmos provides passwordless authentication, trust-based access control, integrated communication, distributed architecture, cryptographic verification, cross-star federation, intended post-quantum resistance, platform-agnostic enforcement, and real-time policy updates. Cosmos implementations can integrate with existing LDAP/Active Directory infrastructure through adapter layers, enabling gradual migration.

3. Scope and Applicability

This specification defines the full Cosmos Protocol, including:

* Badge-based identity system with DID compatibility
* Domain-bound trust scoring algorithm
* Lumen encryption system [RFC-XXXX-Lumen] with intended post-quantum resistance
* Echo grammar [RFC-XXXX-Echo] for semantic messaging
* Capsule system [RFC-XXXX-Capsules] for encrypted communication and storage
* Slipstream Transport Protocol (TNTP) [RFC-XXXX-Slipstream]
* Ramp (Slope Data Format, SDF) [RFC-XXXX-Ramp] and SDFF (Self-Describing Field Format) [RFC-XXXX-SDFF] for data serialization
* Profile system [RFC-XXXX-Profile]
* Productivity suite protocols (Comet [RFC-XXXX-Comet], Nebula [RFC-XXXX-Nebula], Nova [RFC-XXXX-Nova])

The protocol is applicable to:

* Enterprise identity and communication systems
* Decentralized applications requiring trust-native communication

* Constrained environments that can operate without external consensus or blockchain infrastructure

* Systems requiring deployments ranging from small installations to large multi-service environments

* Environments requiring gradual migration from legacy systems

* Complete network replacement scenarios (future work, requires separate transport protocol specification)

4. Requirements Language

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.

5. Terminology

This document defines the following key terms:

Protocol Name vs. Brand Name:

The relationship between "TNSP" (Trust-Native Semantic Protocol) and "Cosmos" follows the same pattern as IEEE 802.11 and WiFi, or IEEE 802.15.1 and Bluetooth:

* *TNSP (Trust-Native Semantic Protocol)*: The technical protocol specification name used in RFCs, technical documentation, and protocol implementations. TNSP is the formal network-layer protocol in the Cosmos stack, providing an identity-native alternative to IP.

* *Cosmos*: The brand/marketing name used in user-facing documentation, product names, and marketing materials. Cosmos is the user-friendly name for the complete protocol ecosystem.

* *Relationship*: TNSP is the technical protocol specification (like IEEE 802.11), and Cosmos is the brand name (like WiFi). When referring to the technical protocol specification, use "TNSP" or "Trust-Native Semantic Protocol". When referring to the brand, ecosystem, or user-facing aspects, use "Cosmos".

* *Usage Guidelines*:

  - Use "TNSP" in technical contexts: RFCs, protocol specifications, code comments, technical documentation, network layer discussions

  - Use "Cosmos" in brand/marketing contexts: user documentation, product names, marketing materials, ecosystem discussions

  - This document uses "Cosmos Protocol" in the title and abstract for brand recognition, but refers to "TNSP" when discussing the technical network layer protocol specification

* *Badge*: A cryptographically signed identifier that serves as identity, capability, and trust container in the Cosmos Protocol. Badges are self-contained and do not require external infrastructure for validation.

* *Manifest*: The core authority service in the Cosmos ecosystem that consolidates certificate authority, authentication service, and token/authorization service functions into a single unified service.

* *Star*: A Cosmos-native entity identified by a domain name (e.g., "example.com") that serves as the trust anchor and authority boundary in the Cosmos Protocol. Stars are Cosmos-implemented entities with badge-based identity, trust scoring, and Cosmos-native protocols. The term "star" emphasizes the authority and trust anchor role: stars have gravity (authority), and all things around stars naturally gravitate toward them.

* *Domain*: The domain name that a star uses as its primary identifier (e.g., "example.com"). A star is identified by its domain name, which follows familiar TCP/IP domain naming conventions.

* *Accretion*: A bilateral trust relationship between stars where both sides must agree. Accretion is a coordinated event, not automatic, and can be reversed. With enough accretions, a star becomes a constellation (super node).

* *Constellation*: A star that has achieved super node status through sufficient accretion relationships. When a star has enough accretions, it becomes a constellation with high gravity (trust), making it a preferred path in routing decisions. Routing algorithms consider constellation relationships when selecting optimal paths, but routing itself is performed by service layer instances.

* *Trust Score*: A computed metric that quantifies the trustworthiness of a star based on star reputation, network effects, and behavioral patterns. The Cosmos Protocol defines two trust-scoring modes: domain-bound trust scoring, which derives signals from DNS-native sources (e.g., DNS records, TLS history, email reputation) when operating over DNS-addressed networks; and star-bound trust scoring, which uses Cosmos-native signals such as accretions, badge stability, and Manifest behavior when operating within Cosmos-native addressing and federation. The trust-scoring model is extensible: any star MAY implement custom trust-scoring algorithms for its own use cases, and trust scores MAY be applied beyond network routing to authorization decisions, service selection, and other trust-based operations, but MUST NOT be treated as absolute indicators of identity legitimacy.

* *Lumen Encryption*: The badge-based encryption system used in the Cosmos Protocol that uses post-quantum candidate cryptographic primitives (see [RFC-XXXX-Lumen]) and is designed to support forward secrecy.

* *Echo Grammar*: The semantic message structure system in the Cosmos Protocol that provides UI hints and agent compatibility for structured communication.

* *Capsule*: A general-purpose encrypted container in the Cosmos Protocol that provides secure communication and storage capabilities with badge-based access control.

* *Interlink*: Optional social networking protocol that enables cross-provider interoperability for participating platforms. Interlink formalizes how existing Cosmos components work together for social networking, defining standard Echo Grammar structures for posts, comments, and social interactions.

* *Corona*: The star’s outward identity surface and distributed presence layer. Corona provides a minimal, canonical interface to the star without exposing the Manifest directly. Corona instances sit between Wormhole (routing) and Manifest (authority), allowing stars to appear in multiple locations while remaining anchored to a single sovereign Manifest. Corona exposes the star’s basic metadata, trust hints, and canonical service endpoints.

6. Protocol Overview

Implementation Note: Protocol versioning and evolution rules, including deprecation lifecycle, version compatibility, and version negotiation procedures, are defined in [RFC-XXXX-Protocol-Versioning]. This document provides only a high-level overview of the Cosmos Protocol primitives.

6.1. Core Principles

The Cosmos Protocol is built on five fundamental principles:

Infrastructure Independence: The protocol operates without requiring blockchain, distributed ledgers, or external consensus mechanisms, enabling deployment in any environment without external consensus or blockchain infrastructure.

Star-bound Trust: Trust is established and managed at the star (domain) level through accretion relationships, providing natural organizational boundaries and policy enforcement.

Badge-centric Identity: All identity, capability, and trust information is contained within cryptographically signed badges that are self-contained and verifiable.

Federated Communication: Identity and communication systems are integrated, enabling cross-provider interoperability for participating platforms while maintaining security and reducing integration complexity.

Enterprise Readiness: The protocol is designed for enterprise-scale deployment with comprehensive lifecycle management and organizational support.

6.2. Architecture Overview

The Cosmos Protocol consists of several integrated components:

* *Badge System*: Cryptographically signed identifiers serving as self-contained identity, capability, and trust containers [RFC-XXXX-Badge]

* *Trust Scoring System*: Manipulation-resistant algorithm for quantifying trustworthiness [RFC-XXXX-Trust-Scoring]

* *Lumen Encryption*: Badge-based encryption using post-quantum candidate primitives [RFC-XXXX-Lumen]

* *Echo Grammar*: Semantic message structures with UI hints [RFC-XXXX-Echo]

* *Capsule System*: General-purpose encrypted communication and storage containers [RFC-XXXX-Capsules]

* *Transport Layer*: Slipstream Transport Protocol (TNTP) [RFC-XXXX-Slipstream] with badge-based sessions

* *Corona*: The star’s outward identity surface and distributed presence layer [RFC-XXXX-Corona], providing a minimal, canonical interface to the star without exposing Manifest directly

* *Profile System*: Universal profiles with domain spaces and privacy controls [RFC-XXXX-Profile]

* *Comet (Scheduling Protocol)*: Unified scheduling protocol that combines iTIP [RFC5546] and iMIP [RFC6047] with badge-based identity and trust scoring [RFC-XXXX-Comet]

* *Nebula (Contact Protocol)*: Unified contact management protocol that combines vCard [RFC6350] and CardDAV [RFC6352] with badge-based identity and trust scoring [RFC-XXXX-Nebula]

* *Nova (Calendar Protocol)*: Unified calendar protocol that combines iCalendar [RFC5545], CalDAV [RFC4791], iTIP [RFC5546], and iMIP [RFC6047] with badge-based identity and trust scoring [RFC-XXXX-Nova]

Implementation Scope Note: While the protocol defines all components, different entities implement different parts based on their role:

* *Manifest Operators*: Implement badge system, trust scoring, and badge lifecycle management

* *Profile Providers*: Implement profile system and (optionally) Interlink

* *Service Providers*: Implement services using badges, profiles, and messaging as needed

* Entities can combine roles (e.g., a manifest operator can also operate as a profile provider)

6.3. Component Relationships

All components work together to provide an integrated identity and communication system:

* Badges provide identity and authentication for all other components
* Trust scoring informs decisions across all communication and access control
* Lumen encryption secures all communication and storage
* Echo grammar structures all messages for semantic processing
* Capsules package all data for secure transmission and storage
* Transport layer provides secure networking consistent with Cosmos transport requirements
* Corona provides the star’s identity surface and distributed presence, sitting between routing (Wormhole) and authority (Manifest) to protect Manifest and enable distributed presence
* Profiles manage user information and privacy
* Manifest-based resolution enables star discovery and capability verification
* Comet (Scheduling Protocol) enables badge-based scheduling with trust-scored permissions, designed for enterprise-scale deployments
* Nebula (Contact Protocol) enables badge-based contact management with trust-scored relationships and cross-star interoperability
* Nova (Calendar Protocol) enables badge-based calendar management with trust-scored access control, designed for enterprise-scale deployments

6.4. Cosmos as Network Stack Evolution

The Cosmos Protocol provides trust-native, identity-aware networking that can operate over existing TCP/IP infrastructure or without IP infrastructure (see Deployment Phases). Cosmos can operate in environments where TCP/IP infrastructure is available and can also operate without IP infrastructure for scenarios that can operate without external consensus or blockchain infrastructure (see Phase 4:

Independent Operation).

These components operate as functional alternatives within Cosmos-native deployments; they do not require or mandate replacement of existing Internet protocols.

6.4.1. TCP/IP Stack Comparison

Cosmos provides alternative protocols that correspond to layers of the TCP/IP network stack:

Layer 1-2 (Physical/Data Link): Cosmos retains existing physical and data link layers (Ethernet, WiFi, Fiber, MAC addressing). These layers remain unchanged as they provide fundamental hardware communication.

Layer 3 (Network): Cosmos provides the Trust-Native Semantic Protocol (TNSP) as an alternative to IP. Capsules serve as the fundamental unit of TNSP, analogous to IP packets at the network layer. They operate at the application/identity layer with built-in trust, identity, and semantics. In Phase 4 deployments, Badge IDs provide network-layer addressing as an alternative to IP addresses, and intent-based routing (defined in TNSP and service discovery protocols) provides an alternative to IP routing.

Layer 4 (Transport): Cosmos provides Slipstream (Trust-Native Transport Protocol, TNTP) [RFC-XXXX-Slipstream] as an alternative to TCP/UDP. Slipstream provides badge-based sessions, trust-aware flow control, and the ability to operate without external consensus or blockchain infrastructure.

Layer 5+ (Application): Cosmos provides Manifest federation as an identity-native alternative to DNS within Cosmos-native deployments (see Deployment Phases). DNS is still used for bootstrap Manifest discovery in early deployment phases. BEAP (Badge-Enabled API Protocol) [RFC-XXXX-BEAP] with Echo Grammar provides an application protocol model for identity-addressed operations, badge-based authentication, and intent-aware routing, serving the role that HTTP/HTTPS plays in traditional web architectures. Echo Grammar provides structured, semantic message formats in place of HTTP’s unstructured payloads. Badge IDs serve as identity anchors analogous to domain names, but with cryptographic trust semantics.

Implementation Note: The complete Slipstream (Trust-Native Transport Protocol, TNTP) specification is defined in [RFC-XXXX-Slipstream]. Slipstream is the recommended transport protocol for Cosmos deployments and can operate both independently of IP (Layer 2 mode) and over IP networks (via UDP/TCP encapsulation).

Slipstream does not require blockchain or external consensus dependencies, but may require Manifest for badge validation in Cosmos deployments (see [RFC-XXXX-Slipstream] for standalone operation details).

6.4.1.1. Deployment Phases

Cosmos can be deployed in phases, from operation over TCP/IP infrastructure to independent operation:

Phase 1 (TCP/IP Infrastructure): Cosmos runs on TCP/IP infrastructure. Slipstream (TNTP) is the recommended transport protocol and can operate over IP networks via UDP/TCP encapsulation. DNS is used for bootstrap Manifest discovery. This enables immediate deployment without requiring infrastructure changes.

Phase 2 (Application Layer Alternatives): Manifest federation provides an identity-native alternative to DNS resolution within the Cosmos substrate. BEAP (Badge-Enabled API Protocol) [RFC-XXXX-BEAP] with Echo Grammar provides an application protocol model for identity-addressed operations and structured messaging, serving the role that HTTP/HTTPS plays in traditional web architectures. Capsules provide a structured, semantic alternative to HTTP content formats. Slipstream (TNTP) operates over existing IP networks via UDP/TCP encapsulation, and Cosmos continues to use IP for the network layer during this phase.

Phase 3 (Transport Layer Alternatives): Slipstream (Trust-Native Transport Protocol, TNTP) [RFC-XXXX-Slipstream] provides an alternative to TCP/UDP, providing badge-based sessions. Cosmos continues to use IP for network layer.

Phase 4 (Independent Operation): TNSP provides an alternative to IP at the network layer. In Phase 4 deployments, Badge IDs provide an alternative to IP addresses (see [RFC-XXXX-Badge] for Badge ID structure and routing properties), and intent-based routing (defined in TNSP and service discovery protocols) provides an alternative to IP routing. Slipstream (Trust-Native Transport Protocol, TNTP) operates directly over Layer 2 (Ethernet frames) or via TNSP capsules. This enables deployment without external consensus or blockchain infrastructure, including environments where IP infrastructure is not available or desired. Phase 4 deployments still require Manifest for badge validation and trust establishment (see [RFC-XXXX-Manifest]).

7. Badge System

Cosmos implementations MUST use the Badge System as specified in [RFC-XXXX-Badge] for all identity, capability, and trust management operations. Badges are cryptographically signed Ramp (Slope Data Format, SDF) [RFC-XXXX-Ramp] documents that serve as identity, capability, and trust containers without requiring blockchain or external infrastructure.

Implementation Note: The complete Badge System specification, including detailed badge structure, badge types, lifecycle management, DID compatibility, group badges, and security considerations, is defined in [RFC-XXXX-Badge]. This document specifies only the requirement to use badges and the integration points with the Cosmos Protocol.

8. Manifest

Each star participates in the Cosmos Protocol through its Manifest service, which acts as the star's authority for badge issuance, validation, and policy distribution. Deployment models, availability strategies, and operational requirements for Manifest are defined in [RFC-XXXX-Manifest].

Note: Detailed specifications for cross-domain registry hosting, including hosting relationships, federated service model, termination requirements, and high availability requirements, are defined in [RFC-XXXX-Manifest]. This document provides only a high-level overview of Manifest's role in the Cosmos Protocol.

9. Policy Substrate (Governance Substrate)

The Policy Substrate is a network-wide governance layer that defines and enforces policies across all Cosmos components. Unlike traditional policy systems that are component-specific, the Policy Substrate provides a unified governance model for Cosmos deployments where implemented (see [RFC-XXXX-Manifest] for Policy Substrate requirements and deployment models), covering access control, compliance, security, data management, and system configuration.

Implementation Note: Detailed Policy Substrate specifications, including policy categories, network-wide enforcement mechanisms, compliance policies, security policies, data management policies, and Access Control Grammar, are defined in [RFC-XXXX-Manifest] (see Section 9). This document provides only a high-level overview of the Policy Substrate's role in the Cosmos Protocol.

10. Security Considerations

The Cosmos Protocol's security properties derive from cryptographic badge signatures, post-quantum encryption (Lumen; see [RFC-XXXX-Lumen]), domain-bound trust scoring, and the ability to operate without blockchain or external consensus dependencies. Cosmos provides confidentiality through post-quantum candidate primitives (see [RFC-XXXX-Lumen] for algorithm details and security considerations), integrity through cryptographic signatures, authentication through badge-based verification, authorization through badge capabilities and trust scores, and non-repudiation through cryptographically signed operations that include timestamp fields defined in the Badge specification (see [RFC-XXXX-Badge] for signature structure and validation requirements), subject to the security properties of the underlying algorithms.

Key security considerations include: identity spoofing prevention through cryptographic verification, trust manipulation resistance through algorithms designed to reduce manipulation risks, communication interception protection through post-quantum candidate primitives (see [RFC-XXXX-Lumen]), and cross-domain security through domain-bound policies and cryptographic isolation.

Implementation Note: Detailed security considerations, including threat models, attack resistance analysis, privacy protection mechanisms, single-point-of-failure analysis, and implementation security requirements, are defined in component RFCs. See [RFC-XXXX-Badge] for badge security, [RFC-XXXX-Manifest] for Manifest security requirements and SPOF mitigation, [RFC-XXXX-Lumen] for encryption security, and [RFC-XXXX-Slipstream] for transport security. This document provides only a high-level overview of the Cosmos Protocol's security properties.

11. IANA Considerations

This document defines the Cosmos Protocol specification and uses existing DNS record types (TXT, SRV, CNAME). The protocol defines transport-agnostic requirements and internal data structures and algorithms that do not require IANA registration. This document defines no new IANA registries. Transport protocols such as Slipstream define their own IANA considerations in separate documents.

Badge types, trust levels, capabilities, and other protocol-internal elements are defined within this specification and do not require separate IANA registries. Service discovery uses existing SRV record types. Domain authority declaration uses existing TXT record types.

A separate specification document defines the COSMOS DNS record type, which will require IANA registration. That specification contains the necessary IANA considerations for the new DNS record type.

This document has no IANA actions.

12. Acknowledgments

The authors would like to thank the contributors to the Cosmos Protocol specification and the broader decentralized identity community for their insights and feedback.

13. References

13.1. Normative References

[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/info/rfc2119>.

[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/info/rfc8174>.

13.2. Informative References

[RFC-XXXX-Badge]
Hernandez, A., "The Cosmos Badge System", Work in Progress, Internet-Draft, draft-cosmos-badge-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-badge-00>.

[RFC-XXXX-BEAP]
Hernandez, A., "Badge-Enabled API Protocol (BEAP): Identity-Addressed, Intent-Aware API Standard", Work in Progress, Internet-Draft, draft-cosmos-beap-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-beap-00>.

[RFC-XXXX-Capsules]
Hernandez, A., "The Cosmos Capsule Protocol", Work in Progress, Internet-Draft, draft-cosmos-capsules-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-capsules-00>.

[RFC-XXXX-Comet]
Hernandez, A., "The Cosmos Comet Scheduling Protocol", Work in Progress, Internet-Draft, draft-cosmos-comet-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-comet-00>.

[RFC-XXXX-Corona]
Hernandez, A., "The Cosmos Corona Protocol", Work in Progress, Internet-Draft, draft-cosmos-corona-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-corona-00>.

[RFC-XXXX-Echo]
Hernandez, A., "The Cosmos Echo Grammar Protocol", Work in Progress, Internet-Draft, draft-cosmos-echo-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-echo-00>.

[RFC-XXXX-Lumen]
Hernandez, A., "The Cosmos Lumen Encryption Protocol", Work in Progress, Internet-Draft, draft-cosmos-lumen-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-lumen-00>.

[RFC-XXXX-Manifest]
Hernandez, A., "The Cosmos Manifest (Badge Registry) Protocol", Work in Progress, Internet-Draft, draft-cosmos-manifest-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-manifest-00>.

[RFC-XXXX-Nebula]
Hernandez, A., "The Cosmos Nebula Contact Protocol", Work in Progress, Internet-Draft, draft-cosmos-nebula-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-nebula-00>.

[RFC-XXXX-Nova]
Hernandez, A., "The Cosmos Nova Calendar Protocol", Work in Progress, Internet-Draft, draft-cosmos-nova-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-nova-00>.

[RFC-XXXX-Profile]
Hernandez, A., "The Cosmos Profile Protocol and Interlink", Work in Progress, Internet-Draft, draft-cosmos-profile-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-profile-00>.

[RFC-XXXX-Protocol-Versioning]
Hernandez, A., "Cosmos Protocol Versioning and Evolution", Work in Progress, Internet-Draft, draft-cosmos-protocol-versioning-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-protocol-versioning-00>.

[RFC-XXXX-Ramp]
Hernandez, A., "Ramp: Slope Data Format (SDF)", Work in Progress, Internet-Draft, draft-ramp-00, <https://datatracker.ietf.org/doc/html/draft-ramp-00>.

[RFC-XXXX-SDFF]
Hernandez, A., "SDFF: Self-Describing Field Format", Work in Progress, Internet-Draft, draft-cosmos-sdff-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-sdff-00>.

[RFC-XXXX-Slipstream]
Hernandez, A., "The Cosmos Slipstream Transport Protocol (TNTP)", Work in Progress, Internet-Draft, draft-cosmos-slipstream-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-slipstream-00>.

[RFC-XXXX-Trust-Scoring]
Hernandez, A., "The Cosmos Trust Scoring Protocol", Work in Progress, Internet-Draft, draft-cosmos-trust-scoring-00, <https://datatracker.ietf.org/doc/html/draft-cosmos-trust-scoring-00>.

[RFC4511] Sermersheim, J., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, DOI 10.17487/RFC4511, June 2006, <https://www.rfc-editor.org/info/rfc4511>.

[RFC4791] Daboo, C. and L. Desruisseaux, "Calendaring Extensions to WebDAV (CalDAV)", RFC 4791, DOI 10.17487/RFC4791, March 2007, <https://www.rfc-editor.org/info/rfc4791>.

[RFC5545] Desruisseaux, B., "Internet Calendaring and Scheduling Core Object Specification (iCalendar)", RFC 5545, DOI 10.17487/RFC5545, September 2009, <https://www.rfc-editor.org/info/rfc5545>.

[RFC5546] Daboo, C., "iCalendar Transport-Independent Interoperability Protocol (iTIP)", RFC 5546, DOI 10.17487/RFC5546, December 2009, <https://www.rfc-editor.org/info/rfc5546>.

[RFC6047] Daboo, C., "iCalendar Message-Based Interoperability Protocol (iMIP)", RFC 6047, DOI 10.17487/RFC6047, December 2010, <https://www.rfc-editor.org/info/rfc6047>.

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

[RFC6352] Daboo, C., "CardDAV: vCard Extensions to WebDAV", RFC 6352, DOI 10.17487/RFC6352, August 2011, <https://www.rfc-editor.org/info/rfc6352>.

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

Author’s Address

Antoine Hernandez
Varlil Corporation
Email: ahernan1@varlil.com